Mathematisches Forschungsinstitut Oberwolfach

Report No. 49/2021

DOI: 10.4171/OWR/2021/49

Geometry and Optimization in Quantum Information (hybrid meeting)

Organized by
Hamza Fawzi, Cambridge UK
Omar Fawzi, Lyon
Aram Harrow, Cambridge MA
Monique Laurent, Amsterdam

3 October – 9 October 2021

Abstract. Quantum information theory seeks to understand the fundamental limits set by quantum mechanics for information processing tasks. The mathematical aspects of quantum information rely on tools from various fields including mathematical optimization, high-dimensional convex geometry, operator algebras and representation theory. The goal of this meeting is to focus on the mathematical aspects connecting geometry, optimization and quantum information theory and develop new tools to solve some of the open problems at the intersection of these fields.

Mathematics Subject Classification (2010): 81P40, 90C22, 14P99, 46L05.

Introduction by the Organizers

The workshop *Geometry and Optimization in Quantum Information*, organized by Hamza Fawzi, Omar Fawzi, Aram Harrow, and Monique Laurent, took place in a hybrid format, with 15 in-person participants and roughly the same number of participants joining remotely. The event brought together a broad spectrum of researchers working on quantum information and mathematical optimization. The workshop aimed at exploring the links between optimization and quantum information, with a focus on the recent developments in the field. The program featured a total of 21 talks, of which 11 were given on-site and 10 remotely via Zoom. The talks were given in different formats: there were 13 regular 45-minute talks, and 8 longer 75-minute talks. Monday evening was partly devoted to several informal 5-minute talks. A stimulating open problem session took place on

Wednesday evening in which several interesting questions were presented by both on-site and remote participants. The program also provided ample time for collaborations and discussions between the participants in Oberwolfach. The expository talks were divided according to the following main themes:

(A) Polynomial optimization, commutative and non-commutative: William Slofstra, Vern Paulsen, Grigoriy Blekherman
(B) Convex geometry and quantum information: Guillaume Aubrun, Andreas Winter
(C) Algorithmic aspects of optimization in quantum information theory: Ryan O'Donnell, Michael Walter, Robert König

We now discuss each section separately.

(A) Polynomial optimization, commutative and non-commutative

One of the recent breakthrough results relating to the topic of this workshop is the $MIP^* = RE$ result by Ji, Natarajan, Vidick, Wright, Yuen, which, in particular, provides a refutation of the Connes' Embedding Problem (CEP) about operator algebras using computer science and quantum information techniques. The result relies at its core on the study of quantum nonlocal games. A key technique in the study of nonlocal games is the noncommutative sum-of-squares hierarchy. In the first expository talk of the workshop, William Slofstra discussed notions of positivity in $*$-algebras, and related computational questions. He focused on problems coming from quantum nonlocal games, and the $MIP^* = RE$ result. He further described some recent undecidability results which imply in particular that on the group algebra of the product of free groups, there are positive elements that are not sums of squares. On Tuesday afternoon, Vern Paulsen talked about a particular class of nonlocal games, called synchronous games. A nice feature of these games is that questions about values of these games connect to questions about traces in operator algebras, which was the original formulation of the Connes' Embedding Problem. On Friday afternoon, Grigoriy Blekherman gave an overview talk about recent exciting applications of the sum of squares method to graph inequalities and extremal combinatorics. Several shorter research talks used tools from polynomial optimization. On Monday morning, Felix Huber presented a new result showing how to use noncommutative optimization to obtain dimension-free entanglement witnesses for multi-partite Werner states. Omar Fawzi presented a new method to obtain lower bounds on the squashed entanglement of a bipartite state, using tools from noncommutative optimization and the sum-of-squares hierarchy. On Tuesday, Stefano Pironio presented methods using noncommutative and trace optimization for a problem in quantum cryptography. Finally, Sander Gribling presented on Wednesday recent progress on the existence of mutually unbiased bases in dimension 6 using the noncommutative sum-of-squares hierarchy, and symmetry reduction.

(B) Convex geometry and quantum information

In his expository talk, Guillaume Aubrun presented the notion of *mean width* of a convex set, and gave an overview of the essential tools that are used to obtain bounds on this quantity. He showed how these tools can be used to compute the mean width of many common convex sets encountered in quantum information, e.g., the set of separable states and the set of states that satisfy the positive partial transpose criterion. Andreas Winter gave an overview talk on the topic of entropy inequalities in the quantum setting, i.e., about valid inequalities on the set $\{(H(\rho_S)_{S\subset[n]} : \rho \text{ density on } n \text{ systems}\} \subset \mathbb{R}^{2^n-1}$ where $H(X) = -\operatorname{tr}[X \log X]$ is the von Neumann entropy function. The closure of this set is a convex cone, and Winter mainly discussed the progress towards finding non-von-Neumann inequalities in the quantum case and commented on the simpler case of Rényi entropies. Research talks featured applications of tools from convex geometry to study particular convex sets in quantum information. Tim Netzer gave a research talk about Quantum Magic Squares and showed that an analogue of the Birkhoff von-Neumann theorem cannot hold for a certain matrix convex set of "quantum doubly-stochastic matrices". David Pérez-García explained how to use techniques from geometry of Banach spaces for analyzing the security of position-based cryptographic protocols. Gemma de las Cuevas presented a new framework to study decompositions of tensors satisfying certain invariance properties. Arne Heimendahl established a negative result about the stabilizer extent, which is a measure of the efficiency of some classical simulation algorithms for quantum computers, using tools from convex optimization theory and probabilistic methods. Cécilia Lancien presented a method to construct entanglement witnesses using projective tensor norms. Nilanjana Datta presented tools from optimization theory to obtain lower bounds on the quantum capacity of quantum channels and analyzed the behavior of their lower bound on random channels. Finally, Debbie Leung talked about a simple family of quantum channels exhibiting surprising non-additivity properties. She also presented a conjecture (the spin alignment conjecture) which generated multiple discussions during the workshop.

(C) Algorithmic aspects of for quantum information

A fundamental problem in quantum information is the problem of quantum tomography: the goal is to efficiently estimate a property about an unknown quantum state ρ using as few samples as possible. Ryan O'Donnell gave an overview of tools and techniques from representation theory that are used to study this problem and highlighted some of the main open problems in this area. On Thursday morning, Michael Walter gave an overview talk about optimization problems that arise from group symmetries, such as the problem of minimizing the norm over a group orbit, which has applications to the quantum marginal problem, and beyond. He described recent tools from geodesic convex optimization to attack these problems. On Friday morning, Robert König presented new limitations on the Quantum Approximate Optimization Algorithms (QAOA) for the combinatorial optimization problem of finding the maximum cut in a graph, and proposed a new recursive

modification that numerically achieves promising results. Several research talks described new classical algorithms for problems in quantum information, as well as quantum algorithms for classical problems. Aram Harrow presented efficient classical algorithms to simulate 2D random quantum circuits of small depth. Harold Nieuwboer presented a new quantum algorithms for the matrix scaling problem, with polynomial speed-up on the best known classical algorithm.

In spite of the challenges imposed by the new hybrid format, the workshop ran smoothly. We would especially like to thank the IT team at the institute for the video conferencing setup which worked surprisingly well and allowed effective interaction between the remote attendees and the participants in the lecture hall. We are grateful to the staff for their efforts in maintaining a high standard of hygiene measures against COVID and creating a relaxed working environment. Finally, our thanks go to the administration of the Mathematisches Forschungsinstitut Oberwolfach for making the conference possible in these difficult times. For some of the participants who were able to be physically present in Oberwolfach, this was an opportunity to discuss in person after a long time due to the pandemic.

Workshop (hybrid meeting): Geometry and Optimization in Quantum Information

Table of Contents

William Slofstra (joint with Arthur Mehta, Yuming Zhao)
Decision problems for positivity and sums of squares 2671

Felix Huber (joint with Igor Klep, Victor Magron, and Jurij Volčič)
Dimension-free entanglement detection in multipartite Werner states . . . 2671

Omar Fawzi (joint with Hamza Fawzi)
Semidefinite programming lower bounds for the squashed entanglement . 2674

Ryan O'Donnell
Estimating quantum states 2675

Guillaume Aubrun
Geometry of high-dimensional entanglement 2678

Tim Netzer (joint with Gemma De las Cuevas, Tom Drescher)
Quantum Magic Squares 2679

Arne Heimendahl (joint with Felipe Montealegre-Mora, Frank Vallentin, David Gross)
Stabilizer extent is not multiplicative 2680

Vern I. Paulsen (joint with J.W. Helton, L. Mancinska, H. Mousavi, S.S. Nezhadi, T. Russell, I.G. Todorov, A. Winter)
Synchronous Values of Games 2682

Stefano Pironio (joint with Armin Tavakoli, Jef Pauwels, and Erik Woodhead)
Correlations in entanglement-assisted prepare-and-measure scenarios . . . 2685

Andreas Winter
Entropy inequalities 2685

Gemma De las Cuevas (joint with Matt Hoogsteder Riera, Andreas Klingler, Tim Netzer)
General decompositions with invariance, positivity and approximations . 2686

Sander Gribling (joint with Sven Polak)
Mutually unbiased bases, polynomial optimization & symmetry 2689

Michael Walter
Noncommutative Group Symmetries and Optimization 2692

David Perez-Garcia (joint with Marius Junge, Aleksander M. Kubicki, C. Palazuelos)
Geometry of Banach spaces: a new route towards Position Based Cryptography 2693

Cécilia Lancien (joint with Maria Anastasia Jivulescu and Ion Nechita)
Multipartite entanglement detection via projective tensor norms 2696

Aram Harrow (joint with John Napp, Rolando La Placa, Alexander Dalzell, Fernando Brandão)
Efficient classical simulation of random shallow 2D quantum circuits . . . 2698

Nilanjana Datta (joint with Satvik Singh)
Detecting positive quantum capacities of quantum channels 2702

Debbie Leung (joint with Felix Leditzky, Vikesh Siddhu, Graeme Smith, John Smolin)
The platypus of the quantum channel zoo 2703

Robert König (joint with Sergey Bravyi, Alexander Kliesch, Eugene Tang)
Hybrid quantum-classical algorithms for approximate graph coloring 2706

Harold Nieuwboer (joint with Joran van Apeldoorn, Sander Gribling, Yinan Li, Michael Walter, Ronald de Wolf)
Quantum algorithms for matrix scaling 2711

Grigoriy Blekherman (joint with Annie Raymond, Mohit Singh, Rekha Thomas)
Graph Homomorphisms and Obstructions to Sums of Squares 2714

Abstracts

Decision problems for positivity and sums of squares

William Slofstra
(joint work with Arthur Mehta, Yuming Zhao)

How do we test if an element of a $*$-algebra is positive? (For this talk, an element of a $*$-algebra is positive if it maps to a positive operator in every $*$-representation on a Hilbert space). One approach we could try is to write the element as a sum of Hermitian squares. On the other hand, if we think the element is not positive, we could try to find a finite-dimensional representation showing that it is not. For the group algebra of the free group, both these approaches give procedures for deciding whether an element is positive. Both approaches also come up in the study of nonlocal games in quantum information. In this case, the underlying $*$-algebra is (closely related to) the product of two free group algebras. Searching over sums of squares can be used to upper bound the commuting-operator value of a nonlocal game, while searching over finite-dimensional representations can be used to lower bound the quantum value. Unfortunately, the recent MIP*=RE result of Ji, Natarajan, Vidick, Wright, and Yuen [1] implies that it is undecidable to determine if elements of this $*$-algebra are positive on all finite-dimensional representations. In addition, there are elements which are not positive, but which are positive in all finite-dimensional representations (so the product of two free group algebras is not RFD). In this talk, I will give an overview of decision problems for positivity and trace-positivity, and the connection with MIP*=RE. Then I will discuss work in progress with Arthur Mehta and Yuming Zhao, where we aim to prove new undecidability results in this area.

References

[1] Z. Ji and A. Natarajan and T. Vidick and J. Wright and H. Yuen. *MIP* = RE,* Commun. ACM 64 (2021), no. 11, pp. 131–138.

Dimension-free entanglement detection in multipartite Werner states

Felix Huber
(joint work with Igor Klep, Victor Magron, and Jurij Volčič)

Our work [1] is concerned with the detection of quantum entanglement. It arose from combining a characterization of Werner state witnesses as non-negative trace polynomials on the positive cone [2] with a recently introduced framework for trace polynomial optimization [3].

A quantum state $\varrho \in L((\mathbb{C}^d)^{\otimes n})$ is said to be *separable*, if it can be written as

$$\varrho = \sum_i p_i \varrho_i^{(1)} \otimes \ldots \otimes \varrho_i^{(n)}$$

for some single-system quantum states $\varrho_i^{(k)} \in L(\mathbb{C}^d)$ and some $p_i \geq 0$ satisfying $\sum_i p_i = 1$. A state is termed *entangled* if it is not separable. It is well known that determining whether a given state is separable or entangled is a computationally hard problem [4, 5]. In particular, the problem scales with the dimension d of the local Hilbert space. In our talk we introduce a method that removes this dependence on d for the class of multipartite Werner states. This allows for the introduction of semidefinite programming hierarchies that scale in the number n of systems only. Our first hierarchy is complete, in the sense that it can detect every entangled Werner state, while the second hierarchy has smaller semidefinite constraints in its first levels.

We consider multipartite Werner states: these are states which are invariant under the adjoint action of unitaries, satisfying $U^{\otimes n} \varrho {U^\dagger}^{\otimes n} = \varrho \,, \forall U \in \mathcal{U}_d$. As a consequence of the Schur-Weyl duality, they can then be expanded in terms of permutation operators $\{\eta_d(\sigma) \,|\, \sigma \in S_n\}$. Here η_d is a unitary representation of the symmetric group on $(\mathbb{C}^d)^{\otimes n}$, permuting individual tensor factors as

$$\eta_d(\sigma) \, |v_1\rangle \otimes \ldots \otimes |v_n\rangle = |v_{\sigma^{-1}(1)}\rangle \otimes \ldots \otimes |v_{\sigma^{-1}(n)}\rangle \ .$$

To detect entanglement, we use the concept of entanglement witnesses. Denote the set of separable and entangled n-partite states with local Hilbert space dimension d as $\mathrm{SEP}(d, n)$ and $\mathrm{ENT}(d, n)$ respectively. Witnesses are operators that satisfy

$$\mathrm{tr}(\mathcal{W}\varrho) \geq 0 \quad \text{for all } \varrho \in \mathrm{SEP}(d, n) \tag{1}$$

$$\mathrm{tr}(\mathcal{W}\varphi) < 0 \quad \text{for some } \varphi \in \mathrm{ENT}(d, n) \tag{2}$$

For Werner states, it is easy to see that one can restrict witnesses to be of the form

$$\mathcal{W} = \eta_d(w) = \sum_{\sigma \in S_n} w_\sigma \eta_d(\sigma) \,, \quad w_\sigma \in \mathbb{C} \,.$$

Again invoking Schur-Weyl duality, we write a Werner state in $L((\mathbb{C}^d)^{\otimes n})$ as

$$\varrho = \bigoplus_{\substack{\lambda \vdash n \\ \mathrm{height}(\lambda) \leq d}} \tilde{\mathbb{1}}_\lambda \otimes \varrho_\lambda \,, \tag{3}$$

Here the unitary group $\mathcal{U}_d$ acts on the first tensor factor while the symmetric group S_n acts on the second; the representations are labeled by partitions λ of n and $\tilde{\mathbb{1}}$ denotes the maximally mixed state. Importantly, in (3) not all irreducible representations of S_n appear if $d < n$. This allows us to show the following.

Theorem 1. *For every entangled Werner state there exists a witness $w \in \mathbb{C}S_n$ satisfying*

$$\mathrm{tr}(\eta_d(w)\varrho) \geq 0 \quad \textit{for all } \varrho \in \mathrm{SEP}(d, n) \,, \forall d \in \mathbb{N} \,.$$

Because the witness has a non-negative expectation value on separable states in all dimensions we term it *dimension-free*. The key idea in the proof is the following: given a Werner state in $\mathrm{ENT}(d, n)$ (for some fixed d) and a witness w detecting it, construct a witness $\tilde{w} = w + u$ where the support of $u \in \mathbb{C}S_n$ lies

exclusively in irreps with height(λ) $> d$. In [1] we show that such u can always be found in order for $\tilde{w}$ to be dimension-free.

Now let us return to the task of finding entanglement witnesses. Given some entangled state φ, (1) is a linear matrix constraint on w. (2) however is not a linear constraint. We deal with this by writing $\mathrm{tr}(\eta_d(w)\varrho)$ as a polynomial that is non-negative on the set of separable states. Recall the following three facts:

a. The minimum of a linear functional on a convex set can always be taken on an extreme point. Thus $\min_{\varrho\in\mathrm{SEP}(d,n)} \mathrm{tr}\left(\eta_d(w)\varrho\right)$ achieves its minimum on some pure product state.

b. Given $X_i \in L(\mathbb{C}^d)$ and $\sigma = (\alpha_1 \dots \alpha_r) \dots (\gamma_1 \dots \gamma_t) \in S_n$ one has [6]:

$$\mathrm{tr}(\eta_d(\sigma) X_1 \otimes \dots \otimes X_n) = \mathrm{tr}(X_{\alpha_r} \cdots X_{\alpha_1}) \cdots \mathrm{tr}(X_{\gamma_t} \cdots X_{\gamma_1}) \,. \tag{4}$$

c. A set of vectors $|v_1\rangle, \dots, |v_n\rangle \in \mathbb{C}^d$ forms a $n \times n$ positive semidefinite Gram matrix Z of rank d with entries $Z_{ij} = \langle v_i | v_j \rangle$.

Our first semidefinite programming hierarchy arises in the following way: from Theorem 1 and Facts *a.* – *c.* it follows that

$$\min_{\varrho\in\mathrm{SEP}(n,n)} \mathrm{tr}(\eta_n(w)\rho) \geq \min_{Z\in\mathcal{Z}} f_w(Z) \,,$$

where f_w is a polynomial in the entries of Z and

$$\mathcal{Z} = \{Z \geq 0 \,|\, Z_{ij} = \overline{Z_{ji}} \,, Z_{ii} = 1 \,, Z \in L(\mathbb{C}^n)\} \,.$$

The set $\mathcal{Z}$ forms a spectrahedron also known as *elliptope*, representing allowed values of inner products $\langle v_i | v_j \rangle$ of normalized vectors from $\mathbb{C}^n$.

A matrix-version of the Putinar Positivstellensatz [7] can now be used to guaranteee non-negativity of $f_w + \epsilon$, $\epsilon > 0$, on $\mathcal{Z}$ in terms of the quadratic module generated by $\mathcal{Z}$; its truncation to monomials of bounded degree yields our first semidefinite programming hierarchy. This hierarchy is complete, in the sense that for every entangled Werner state it finds an entanglement witness at some level of the hierachy.

Our second hierarchy uses Theorem 1 in conjuction with Fact *b.*, and so

$$\min_{\varrho\in\mathrm{SEP}(n,n)} \mathrm{tr}(\eta_n(w)\varrho) \geq \min_{X_i\in L(\mathbb{C}^n),\, X_i^2 = X_i} p(X_1, \dots, X_n) \,,$$

where p is a trace polynomial given by $w \in \mathbb{C}S_n$ through (4) in (non-commutative) matrix variables $X_i = X_i^2$. We now strenghten the domain of non-negativity by asking for non-negativity of p for all projectors from any tracial von Neumann algebra. Again a Putinar-type Positivstellensatz [3] allows for a characterization of non-negative $p + \epsilon$ for all $\epsilon > 0$; its truncation to trace monomials of bounded degree yields our second semidefinite programming hierarchy. While it is presently not known to us whether this hierarchy is also complete or not, it allows for smaller semidefinite constraints in its first levels.

References

[1] F. Huber, I. Klep, V. Magron, and J. Volčič, *Dimension-free entanglement detection in multipartite Werner states,* arXiv:2108.08720

[2] F. Huber, *Positive maps and trace polynomials from the symmetric group,* J. Math. Phys. 62, 022203 (2021).

[3] I. Klep, V. Magron, and J. Volčič, *Optimization over trace polynomials,* Ann. Henri Poincaré, 2021.

[4] L. Gurvits, *Classical complexity and quantum entanglement,* J. Comp. Syst. Sci., 69, 448–484 (2004).

[5] S. Gharibian, *Strong NP-hardness of the Quantum Separability Problem,* Quant. Inf. Comp., 10, 343 (2010).

[6] B. Kostant, *A theorem of Frobenius, a theorem of Amitsur-Levitski and cohomology theory,* J. Math. Mech.7, 237-264, 1958.

[7] C. W. Scherer and C. W. J. Hol, *Matrix Sum-of-Squares Relaxations for Robust Semi-Definite Programs,* Math. Program., 107, 189–211 (2006).

Semidefinite programming lower bounds for the squashed entanglement

Omar Fawzi

(joint work with Hamza Fawzi)

The squashed entanglement is an entanglement measure introduced by Christandl and Winter [1]. It satisfies many desirable properties for an entanglement measure such as monotonicity under local operations and classical communication (LOCC), additivity under tensor products, a monogamy relation and faithfulness. In fact, it is the only known entanglement measure satisfying these properties [3]. These mathematical properties also have operational applications: the squashed entanglement provides an upper bound on the distillable entanglement and the distillable key [2]. For a bipartite state ρ_{AB} on $A \otimes B$, the squashed entanglement is defined as

$$E_{\mathrm{sq}}(A:B)_\rho = \frac{1}{2} \inf_{\rho_{ABE}} I(A:B|E)_\rho \ , \tag{1}$$

where the infimum is taken over all possible finite-dimensional Hilbert spaces E and all extensions ρ_{ABE} of the state ρ_{AB}, i.e., $\mathrm{Tr}_E \rho_{ABE} = \rho_{AB}$. The conditional mutual information is defined in equation (3) below.

To define the conditional mutual information it is useful to start with the quantum relative entropy. For density operators ρ, σ on a finite-dimensional Hilbert space $\mathcal{H}$, the quantum relative entropy is defined by

$$D(\rho\|\sigma) = \begin{cases} \mathrm{Tr}(\rho(\log\rho - \log\sigma)) & \text{if } \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma) \\ +\infty & \text{otherwise.} \end{cases} \tag{2}$$

For a density operator ρ_{AE} on $A \otimes E$ with A finite-dimensional, we define the conditional von Neumann entropy $H(A|E)_\rho = -D(\rho_{AE}\|I_A \otimes \rho_E)$ where $\rho_E = \mathrm{Tr}_A \rho_{AE}$ and I_A denotes the identity operator on A. The conditional mutual

information is then defined by

$$I(A:B|E)_\rho = H(A|E)_\rho - H(A|BE)_\rho \ . \tag{3}$$

Even though $E_{\mathrm{sq}}(A:B)_\rho$ satisfies almost all the properties one might ask of an entanglement measure [3], its main drawback is that it is unclear how to compute it.

In this work, we introduce a hierarchy of lower bounds $E_{\mathrm{sq}}^{(m)}(A:B)_\rho$ on the squashed entanglement satisfying for all positive integers m:

$$E_{\mathrm{sq}}^{(m)}(A:B)_\rho \leq E_{\mathrm{sq}}(A:B)_\rho \leq E_{\mathrm{sq}}^{(m)}(A:B)_\rho + \frac{2d_A - 2}{m^2 \ln 2} \ .$$

The quantity $E_{\mathrm{sq}}^{(m)}(A:B)_\rho$ is defined by using an approximation of the logarithm that appears in Eq. (2) with rational functions obtained via a Gauss-Radau quadrature, as in [4]. These rational functions lead to quantum f-divergences for rational functions f that have variational expressions as determined in [5]. Combining these properties, we find that $E_{\mathrm{sq}}^{(m)}(A:B)_\rho$ can be expressed as a matrix-valued noncommutative polynomial optimization problem over finite dimensional Hilbert spaces. Using standard semidefinite programming hierarchies for noncommutative polynomial optimization problems, this leads to semidefinite programming lower bounds on the squashed entanglement.

References

[1] M. Christandl and A. Winter. *"Squashed entanglement": an additive entanglement measure.* J. Math. Phys. 45(3):829-840, 2004.

[2] M. Christandl. *The structure of bipartite quantum states-insights from group theory and cryptography.* PhD Thesis, Cambridge University, 2006 arXiv:quant-ph/0604183

[3] F. Brandao and M. Christandl and J. Yard. *Faithful squashed entanglement.* Comm. Math. Phys. 306(3):805, 2011

[4] H. Fawzi, J. Saunderson, and P. Parrilo. *Semidefinite approximations of the matrix logarithm.* Found. Comput. Math., Mar 2018.

[5] P. Brown and H. Fawzi,and O. Fawzi. *Device-independent lower bounds on the conditional von Neumann entropy.* arXiv:2106.13692

Estimating quantum states

Ryan O'Donnell

In this talk I surveyed recent results on learning quantum states (tomography) and testing quantum states. A main theme is viewing this task as generalizing known (and in many cases, recently developed) analogous results for learning and testing probability distributions. The goal is to develop quantum algorithms that are not much less than the analogous classical ones.

To develop the analogy, consider the basic, classical problem of *density estimation* (of a discrete distribution). Here there is an unknown probability distribution p on a discrete set of outcomes $\{1, \ldots, d\}$; in other words, we have unknowns $p_1, \ldots, p_d$ with $p_i \geq 0$ and $\sum_i p_i = 1$. We imagine the learning algorithm may "pay for" n samples from p. "Nature" now draws a sample $i_1, \ldots, i_n$ from the

product probability distribution $p^{\otimes n}$, and this sample is revealed to the learner. The learner may now run an algorithm to produce some final output "X". Here "X" may stand for any kind of object; perhaps the learner is trying to estimate all of p, in which case X would be some hypothesis distribution $\hat{p} = (\hat{p}_1, \ldots, \hat{p}_d)$. But the learner might have other goals; for example, X might be an estimate of the *entropy* of p, or an estimate of the distance between p and some other known q. In the particular case of trying to learn all of p, the "obvious" algorithm of letting $\hat{p}$ be the empirical distribution formed by the n samples is almost always the best idea, but for other estimation tasks the right way to go from the samples to the estimate may not be so clear.

In the quantum analogue of these tasks, we have an unknown quantum mixed state ρ of d dimensions; i.e., $\rho \in \mathbb{C}^{d \times d}$ is a positive semidefinite matrix ($\rho \geq 0$) with trace 1 ($\sum_i \rho_{ii} = 1$). It can be very helpful also to view ρ as an unknown probability distribution p on the unknown orthonormal basis of eigenvectors $|1\rangle, \ldots, |d\rangle$ of ρ. (The slight ambiguity that occurs if ρ has eigenvalues with multiplicity causes no difficulties.) Now n "samples" consist of n copies $\rho^{\otimes n}$ of ρ, and this in turn can be thought of as n independent draws from p, resulting in a vector $|i_1\rangle \otimes \cdots \otimes |i_n\rangle \in (\mathbb{C}^d)^{\otimes n}$. We may think of this sample vector as being presented to the quantum learner, who must now make a quantum measurement and produce an appropriate output "X" based on the measurement outcome. Again, "X" could be an estimate $\hat{\rho}$ of all of ρ, or something else: e.g., an estimate $\hat{p}$ of ρ's eigenvalues p, an estimate of the von Neumann entropy of ρ, etc.

In the talk, several learning/testing goals and results were reviewed, comparing the classical and quantum cases. For example:

- The naive algorithm can with high probability learn an unknown p, with a hypothesis $\hat{p}$ having total variation error at most ε (i.e., $\frac{1}{2}\|p - \hat{p}\|_1 \leq \varepsilon$), using $n = O(d/\varepsilon^2)$ samples, and this is known to be sharp (up to constants). Analogously, one can learn ρ to trace distance ε using $O(d^2/\varepsilon^2)$ samples [3], and again this is sharp [1]. However the known algorithms in the quantum case are quite sophisticated, relying on *representation theory*.
- The classical result above extends to stricter distance measures such as Hellinger distance. The same improvement is also known for the quantum analogue (using quantum fidelity in place of trace distance), up to logarithmic factors [1]. Extensions of the quantum result to even stronger distances measures (e.g., Bures χ^2-distance) remain open.
- For the quantum task of just learning the *eigenvalues* p of ρ, this can be done (again, via representation theory) with sorted-total-variation distance ε using $n = O(d^2/\varepsilon^2)$ samples. The classical analogue of this task is learning the *multiset* $\{p_1, \ldots, p_d\}$ to sorted-total-variation distance ε, and interestingly it is known [5] that this can be done with $n = o(d)$ samples (more precisely, $\Theta(d/\log d)/\varepsilon^2$). As the only known quantum lower bound for this problem is $\Omega(d/\varepsilon^2)$, it is an interesting open problem as to whether the quantum eigenvalue estimation task can be done with $n = o(d^2)$ samples.

- The classical problem of testing whether an unknown distribution is the uniform distribution $p \equiv 1/d$, or else ε-far (in total variation distance) from uniform can be done with $\Theta(\sqrt{d}/\varepsilon^2)$ samples [4], and it is known a natural algorithm for empirically estimating $\sum_i p_i^2$ can be used for this. Regarding the analogous quantum problem, testing if ρ is the maximally mixed state $\mathbb{1}/d$ (or else ε-far in trace distance), this can be done with $\Theta(d/\varepsilon^2)$ samples [2], and also via a natural algorithm that estimates the *purity* $\mathrm{tr}(\rho^2)$ of ρ.

The latter portion of the talk was devoted to giving some introduction to the representation-theoretic ideas that go into some of the quantum algorithms. For example, the algorithm for estimating the purity of ρ (and hence testing whether ρ is the maximally mixed state) is via a generalization of the "SWAP test", wherein given $\rho^{\otimes n}$, one estimates the average, over all pairs $\{i,j\} \subset \{1,\ldots,n\}$, of the expectation value under ρ of the SWAP_{ij} operator (which swaps the ith and jth tensor components). This estimate has the correct expectation, and computing its variance relies on the analysis of $(\mathrm{avg}_{\{i,j\}}\mathrm{SWAP}_{ij})^2$. In turn, this latter operator can best be understood by expressing it as a linear combination of the more general operators

$$A_\kappa = \mathrm{avg}\{R(\pi) : \pi \in S_n,\ \mathrm{cycleType}(\pi) = \kappa\},$$

where $R(\pi)$ is the operator on $(\mathbb{C}^d)^{\otimes n}$ that acts by permuting tensor components according to pi. Note that

$$R : S_n \to \{\text{linear operators acting on } (\mathbb{C}^d)^{\otimes n}\}$$

is a *group representation*, which is one way in which group representation theory enters the picture.

Indeed, thanks to notion of *Schur–Weyl duality* from representation theory, one can show that the optimal estimator for *any* symmetric polynomial of the eigenvalues of ρ (not just $\mathrm{tr}(\rho^2)$) is the expectation value of some linear combination of operators A_κ. This implies that for quantum learning/testing algorithms that are only concerned with properties of the eigenvalues p, it is optimal for them to measure $\rho^{\otimes n}$ in the *Schur–Weyl basis*, the result of which is a random *Young diagram* with a certain probability distribution depending on p. This distribution can alternatively be understood in terms of the probabilistic combinatorics of *longest increasing subsequences in random words*, and in this way one can fruitfully use a variety of tools from combinatorics to study quantum state eigenvalue learning/testing. For more general learning/testing tasks involving the whole of ρ (i.e., also its eigen*vectors*), further tools from the representation theory of the unitary group may be used, but this was beyond the scope of the talk.

References

[1] J. Haah, A. Harrow, Z. Ji, X. Wu, and N. Yu. *Sample-optimal tomography of quantum states.* In Proceedings of the 48th Annual ACM Symposium on Theory of Computing, pages 913–925, 2016.

[2] R. O'Donnell and J. Wright. *Quantum spectrum testing.* In Proceedings of the 47th Annual ACM Symposium on Theory of Computing, pages 529–538, 2015.

[3] R. O'Donnell and J. Wright. *Efficient quantum tomography.* In Proceedings of the 48th Annual ACM Symposium on Theory of Computing, pages 899–912, 2016.
[4] L. Paninski. *A coincidence-based test for uniformity given very sparsely sampled discrete data.* IEEE Transactions on Information Theory, 54(10):4750–4755, 2008.
[5] G. Valiant and P. Valiant. *Estimating the unseen: an $n/\log(n)$-sample estimator for entropy and support size, shown optimal via new CLTs.* In Proceedings of the 43rd Annual ACM Symposium on Theory of Computing, pages 685–694, 2011.

Geometry of high-dimensional entanglement

Guillaume Aubrun

We compare, in terms of geomety, the relative sizes of different sets which appear in quantum information theory, connected to the notion of entanglement. The talk, of introductory nature, is based on material from [1].

To this end, we introduce the *mean width* of a convex subset K or a Euclidean finite-dimensional vector space V as

$$w(K) = \mathbf{E} \sup_{x \in K} \langle x, G \rangle$$

where the expectation is taken with respect to a standard Gaussian vector G in V. The mean width can be used to quantify the size of a set. As opposed to volume, it is intrinsic: if W is a subspace of V and $K \subset W$, the mean width of K is the same, computer in either W or V.

Two basic estimates are

(1) the *union bound*: if $K \subset V$ is convex hull of N vectors of norm ≤ 1, then $w(K) \lesssim \sqrt{\log N}$,
(2) the *Sudakov minoration*: if K contains an ε-separated subset of cardinal N, then $w(K) \gtrsim \varepsilon\sqrt{\log N}$.

Elaborating on these two estimates, we derive the following information.

(1) The set D_n of mixed quantum states on $\mathbf{C}^n$ satisfies $w(D_n) \simeq \sqrt{n}$,
(2) The inscribed Euclidean ball $B \subset D_n$, which has Hilbert–Schmidt radius $1/\sqrt{n(n-1)}$, satisfies $w(B) \simeq 1$.
(3) The set $Sep_{d\otimes d} \subset D_{d\otimes d}$ of separable states satisfies $w(Sep_{d\otimes d}) \simeq \sqrt{d}$, so it is much smaller than $D_{d\otimes d}$.
(4) By duality, the set $BP_{d\otimes d}$ of block-positive matrices of trace 1 satisfies $d^{3/2} \lesssim w(BP_{d\otimes d}) \lesssim d^{3/2}\log(d)$. Here, the logarithmic loss comes from a application of the "$MM*$ estimate" from local theory of Banach spaces.
(5) The set $MME_{d\otimes d}$ of states which are mixtures of maximally entangled states satisfies $w(MME_{d\otimes d}) \sim d$.
(6) The set $k{-}Ext_{d\otimes d}$ of states that are k-extendible satifsies $w(k{-}Ext_{d\otimes d}) \gtrsim d/k$ because it contains a $1/k$-homothetic copy of $MME_{d\otimes d}$. This shows that when stopped at a level $k \ll \sqrt{d}$, the extendibility hierarchy is asymptotically a poor approximation to separability.

(7) The set $PPT_{d\otimes d} \subset D_{d\otimes d}$ of states with a positive partial transpose satisfies $w(PPT_{d\otimes d}) \sim d$. As above, the PPT criterion is asymptotically a poor approximation to separability.

References

[1] G. Aubrun and S. J. Szarek, *Alice and Bob meet Banach,* American Mathematical Soc., 223 (2017).

Quantum Magic Squares

Tim Netzer
(joint work with Gemma De las Cuevas, Tom Drescher)

The notion of a magic square is familiar to many people, the similar notion of a doubly stochastic matrix at least to many mathematicians. A doubly stochastic matrix can be defined as a square matrix of size n, that contains a probability measure in each row and each column. The famous theorem of Birkhoff-von Neumann states that these matrices are all convex combinations of permutation matrices, i.e. matrices arising from permuting rows and columns of the identity matrix I_n.

In quantum theory, the notion of a probability measure is replaced by a so-called positive operator valued measure (POVM), a collection of positive semidefinite matrices $P_1, \dots, P_n \in \mathrm{Mat}_s(\mathbb{C})$, that sum to the identity matrix:

$$P_1 + \cdots + P_n = I_s.$$

So a *quantum magic square* is an $n \times n$ matrix that contains a POVM (of arbitrary size s) in each row and column. There also exists the well-studied notion of a *quantum permutation matrix*, which is a quantum magic square whose entries are all idempotents, i.e. orthogonal projections.

Now a quantum version of the Birkhoff-von Neumann Theorem would ask whether each quantum magic square is a convex combination of quantum permutation matrices. Taking classical convex combinations does clearly not suffice here, but there exists a much more suitable notion, that of a *free convex hull*. Here the single matrix entries of a quantum permutation matrix are compressed with a matrix, which might even result in a change of size. In formulas, the quantum permutation matrix $(P_{ij})_{i,j=1,\dots,n}$, whose entries P_{ij} are projectors of size s, is changed to

$$(V^* P_{ij} V)_{i,j=1,\dots,n}$$

where $V \in \mathrm{Mat}_{s,t}(\mathbb{C})$. One also allows for sums of such compressions, with the normalization constraint that $\sum_j V_j^* V_j = I_t$ for the respective compression matrices. Reading this backwards, one says that the resulting quantum magic square *dilates* to a quantum permutation matrix. For example, given just one POVM, it always dilates to a so-called *projective measurement*, a POVM that consists of only projectors. This is known as Naimark's Dilation Theorem, and we thus ask for a *magic* version thereof, applying to quantum magic squares instead of a single POVM only.

We prove that this result is true when restricted to special quantum magic squares, which we call semi-classical. They arise from classical magic squares by tensoring them with positive semidefinite matrices (related to the minimal operator system over the classical magic squares). But we also prove that the general version of a Quantum Birkhoff-von Neumann Theorem / Magic Naimark Theorem fails even under the very general notion of free convexity. The result is constructive, we produce a quantum magic square of any size $n \geqslant 3$ that does not dilate to a quantum permutation matrix.

Stabilizer extent is not multiplicative

Arne Heimendahl

(joint work with Felipe Montealegre-Mora, Frank Vallentin, David Gross)

The Gottesman-Knill theorem states that a Clifford circuit acting on stabilizer states can be simulated efficiently on a classical computer. Recently, this result has been generalized to cover inputs that are close to a coherent superposition of polynomially many stabilizer states. The runtime of the classical simulation is governed by the *stabilizer extent*, which roughly measures how many stabilizer states are needed to approximate the state. An important open problem is to decide whether the extent is multiplicative under tensor products. An affirmative answer would yield an efficient algorithm for computing the extent of product inputs, while a negative result implies the existence of more efficient classical algorithms for simulating large-scale quantum circuits. Here, we answer this question in the negative. Our result follows from very general properties of the set of stabilizer states, such as having a size that scales subexponentially in the dimension, and can thus be readily adapted to similar constructions for other resource theories. This work has been published here [1].

The problem

The stabilizer extent of an n-qubit state ψ is the following minimization problem

$$\xi(\psi) = \min\left\{ \Big(\sum_{s \in \mathrm{Stab}_n} |c_s| \Big)^2 \,:\, \psi = \sum_{s \in \mathrm{Stab}_n} c_s s \right\},$$

where Stab_n is the set of n-qubit stabilizer states. The extent ξ is the outcome of an ℓ_1-minimization problem whose complexity scales polynomially in the number of n-qubit stabilizer states.

In particular, the complexity of determining the stabilizer extent of an arbitrary vector $\psi \in (\mathbb{C}^2)^{\otimes n}$, scales superexponentially with the number of qubits n. Thus, the question arises whether it is possible to simplify the computation of ξ for certain inputs, e.g. product states of the form $\psi = \otimes_j \psi_j$.

Since the set of stabilizer states is closed under taking tensor products, one can easily see that the stabilizer extent is submultiplicative, that is $\xi(\otimes_j \psi_j) \leq \prod_j \xi(\psi_j)$ for any input state $\otimes_j \psi_j$. Bravyi *et al.* proved that it is actually multiplicative if the factors are composed of 1-, 2- or 3-qubit states.

As a result the stabilizer extent of product states is computationally tractable if the factors are composed of at most three qubits. This raises the question whether this property holds for arbitrary product states.

Main result

Our main result is that stabilizer extent is *not* multiplicative in general. In fact our proof does not depend on the detailed structure of stabilizer states and holds in much greater generality. Specifically only rather simple properties of Stab_n enter into the proof, prime among the properties used is that the number of the stabilizer states scales subexponentially with the Hilbert space dimension. We present our theorem in its full generality in the technical version of the abstract.

Theorem 1. *Let n be large enough and ψ be a Haar-random n-qubit pure state. Then,*

$$\Pr[\xi(\psi \otimes \psi^*) < \xi(\psi)\xi(\psi^*)] \geq 1 - o(1).$$

In particular, the stabilizer extent is not multiplicative.

Additionally, we prove a conceptually simple necessary condition that is satisfied by optimal decompositions. Recall that Stab_n can be partitioned into stabilizer orthonormal bases (e.g. $\mathrm{Stab}_1 = \{|0\rangle, |1\rangle\} \cup \{|+\rangle, |-\rangle\} \cup \{|+, Y\rangle, |-, Y\rangle\}$ where the last term is the eigenbasis of the Pauli Y matrix).

Theorem 2. *Let ψ be an n-qubit state. Suppose that $\psi = \sum c_s s$ is an optimal stabilizer extent decomposition, that is $\xi(\psi) = \left(\sum_{s \in \mathrm{Stab}_n} |c_s|\right)^2$. Then, for any orthonormal basis $B \subset \mathrm{Stab}_n$, there is* at most *one $s \in B$ for which $c_s \neq 0$.*

Implications

Theorem 1 indicates that computing the extent is not only hard for general inputs but also for product states of the form $\otimes_j \psi_j$.

It has also implications for classical simulation algorithms of quantum computation that are based on the stabilizer extent. These methods are usually called *Stabilizer rank methods* [2, 3, 4]. Within the framework of quantum computing with magic states, the idea is to expand initial magic state as a coherent superposition of stabilizer states. The smallest number of stabilizer states required to express a given vector in this way is its *stabilizer rank*. No efficient methods are known for computing the stabilizer rank analytically or numerically. To address this issue, Bravyi *et al.* [5] originally introduced the stabilizer extent as a computationally better-behaved convex relaxation. The central *sparsification lemma* of [5] states that a stabilizer decomposition with small extent can be transformed into a sparse decomposition that is close to the original state.

Our result implies that if the magic state $\psi \otimes \phi$ is a product state, then decompositions involving only product stabilizer states $s \otimes s'$ will generally be suboptimal.

That is, even if

$$\psi = \sum_{s \in \mathrm{Stab}_n} c_s s, \quad \phi = \sum_{s \in \mathrm{Stab}_n} d_s s,$$

are optimal (i.e. such that $\sqrt{\xi(\psi)} = \sum_s |c_s|$ and $\sqrt{\xi(\phi)} = \sum_s |d_s|$), it can happen that the decomposition $\psi \otimes \phi = \sum_{s,s' \in \mathrm{Stab}_n} c_s d_{s'} s \otimes s'$ is not optimal, i.e. $\sqrt{\xi(\psi \otimes \phi)} < \sum_{s,s'} |c_s d_{s'}|$. Therefore, the commonly used approach of using product stabilizer state decompositions for stabilizer rank simulations could in principle be improved upon.

Our main theorem also proves that other *magic monotones* recently defined in [3] are not multiplicative since they all coincide with the stabilizer extent on pure states [6].

Open questions

An interesting open question is how large the gap can get between $\xi(\phi \otimes \psi)$ and $\xi(\phi)\xi(\phi)$ for states $|\phi\rangle$ and $|\psi\rangle$.

Furthermore, it might be interesting to see whether this technique can also be applied to other conic optimization techniques.

References

[1] A. Heimendahl, F. Montealegre-Mora, F. Vallentin, and D. Gross, *Stabilizer extent is not multiplicative,* Quantum, vol. 5, page 400 (2021)

[2] S. Bravyi, G. Smith, and J. Smolin, *Trading classical and quantum computational resources,* Phys. Rev. X 6, 021043 (2016).

[3] J. R. Seddon, B. Regula, H. Pashayan, Y. Ouyang, and E. T. Campbell, *Quantifying quantum speedups: improved classical simulation from tighter magic monotones,* (2020), arXiv:2002.06181 [quant-ph].

[4] S. Bravyi and D. Gosset, *Improved classical simulation of quantum circuits dominated by Clifford gates,* Phys. Rev. Lett. 116, 250501 (2016).

[5] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, *Simulation of quantum circuits by low-rank stabilizer decompositions,* Quantum, vol. 3, page 181 (2019).

[6] B. Regula, *Convex geometry of quantum resource quantification,* J. Phys. A: Math. Theor. 51,045303 (2018).

Synchronous Values of Games

Vern I. Paulsen

(joint work with J.W. Helton, L. Mancinska, H. Mousavi, S.S. Nezhadi, T. Russell, I.G. Todorov, A. Winter)

Entanglement assisted cooperative games, often called non-local games, are an important object of study in many areas of computer science and quantum information. Such games were vital to the recent resolution of the Connes' Embedding Problem [9] and to answering the Tsirelson Problems [15, 9] about the relationships between the different mathematical models for entanglement.

The *value* of a nonlocal game is the supremum of the probability of winning the game over all allowed strategies. The value of a game can vary depending

on the types of strategies or probability densities that are allowed, and there has been considerable interest in how the value of a game can change when one is allowed to use quantum assisted strategies versus classically defined distributions [1, 12, 2, 14, 4, 3].

However, the Tsirelson problems are concerned with the fact that there are several different mathematical models for describing the probability densities that can arise from using entanglement and we now know that each of these models give rise to different sets of densities. Thus, for each mathematical model of entanglement, there is a corresponding value of a game and, in fact, showing that the value of a game can vary depending on the model has been the most effective tool for proving that these models are indeed different.

In this talk we focus on how the values of games behave when we insist that the allowed densities are *synchronous*. A game is *synchronous* if the two cooperating players, Alice and Bob, each have the same input(question) set and output(answer) set and the rules of the game include the rule that if in a round of the game, they are both asked the same question, then they must both give the same answer.

If we let $p(a, b|x, y)$ denote the conditional probability that they return answers a and b, respectively, given respective inputs x and y, then a density is called synchronous if $p(a, b|x, x) = 0, \forall a \neq b$, i.e., if the probability that they give different outputs given the same input is 0.

Each of the mathematical models for entanglement produces different sets of synchronous densities and our goal is to try and compute these various values for some special families of games.

The first type of game that we focus on are graph colouring games. Given a graph with no loops $G = (V, E)$ described by a vertex and edge set and a set of k-colours, the goal of this game is for Alice and Bob to come as close as possible to convincing a Referee that they have coloured the graph with k-colours.

At each round of the game Alice and Bob are given a pair of vertices and they must return a pair of colours. They win the round if whenever the vertices were adjacent, they returned different colours and whenever they are given the same vertex, they returned the same colour. The value of the game measures the optimal probability of winning this game over many rounds.

A deterministic strategy for this game, just means that Alice and Bob each have a function $f, g : V \to \{1, ..., k\}$ such that upon receiving inputs x, y they reply with outputs $f(x), g(y)$.

However, when we restrict to synchronous deterministic strategies, then we need $f(x) = g(x)$ for all x, and so Alice and Bob must both use the same "colouring" function. From this it follows that the synchronous deterministic value of this game is directly related to the max k-cut problem for the graph.

It is well known that quantum densities can out perform any deterministic strategy for this game. We show that similarly, synchronous quantum strategies and out perform any synchronous deterministic strategy. Some what surprisingly, even though this game is synchronous, we show that there are graphs for which a non-synchronous quantum strategy can out perform synchronous quantum strategies.

Another important topic in the theory of games is how their values behave under parallel repetition of the game. It is known that the deterministic value of a game can be supermultiplicative. But it is also known that if the value is less than one, then the value of n parallel copies of the game will tend to 0 as n grows.

In sharp contrast, we give an example of a game for which the synchronous value(both classical and quantum) is monotone increasing under repetition.

The XOR games are a family of games for which the classical and quantum values have been widely studied. We find parallel results for their synchronous values. In particular, the synchronous value is obtained as the solution to a semidefinite program, i.e., by maximizing a linear functional over a spectrahedron.

Synchronous densities of the various quantum types have been shown to correspond to traces of various types on a universal C*-algebra [13, 10] and for this reason computing the value of a game can be seen as computing the supremum over all traces of a certain positive element of the algebra defined by the game. This fact connects questions about synchronous values of games with problems about traces, which was the original content of Connes' Embedding Problem.

The new results in this talk are based on two papers, [6] and [11].

References

[1] J. F.Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed Experiment to Test Local Hidden-Variable Theories*, Phys. Rev. Lett., 23(1969), No.15, 880–884.

[2] R. Cleve, P. Hoyer, B. Toner, J. Watrous, "Consequences and limits of nonlocal strategies," *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.*, 2004, pp. 236-249.

[3] R. Cleve, L. Liu, and W. Slofstra, *Perfect commuting-operator strategies for linear system games*, Journal of Mathematical Physics, 58(2017), No.1, 1089-7658.

[4] R. Cleve and R. Mittal, *Characterization of Binary Constraint System Games*, International Colloquium on Automata, Languages and Programming(2014).

[5] R. Cleve, W. Slofstra, F. Unger, S. Upadhyay, *Perfect Parallel Repetition Theorem for Quantum Xor Proof Systems*, *Comput. Complex.* 17, 2 (2008), pp. 282–299.

[6] W. Heltoon, H. Mousavi, S.S. Nezhadi, V.I. Paulsen, T. Russell, *Synchronous values of games*, preprint, arixv.

[7] W. Helton, K. P. Meyer, V. I. Paulsen, M. Satriano, *Algebras, Synchronous Games and Chromatic Numbers of Graphs*, New York Journal of Mathematics, Vol. 25(2019), pp. 328-361.

[8] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, and R. F. Werner, *Connes' embedding problem and Tsirelson's problem*, Journal of Mathematical Physics, 52(2011).

[9] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen, *MIP*=RE*, arXiv:2001.04383(2020).

[10] S. J. Kim, V. I. Paulsen, and C. P. Schafhauser, *A synchronous game for binary constraint systems*, Journal of Mathematical Physics 59(2018), 032201.

[11] L. Mancinska, V. I. Paulsen, I. G. Todorov, and A. M. Winter, *Products of synchronous games*, preprint.

[12] N. D. Mermin, *Simple unified form for the major no-hidden-variables theorems*, Phys. Rev. Lett., 65(1990), No.27.

[13] V. I. Paulsen, S. Severini, D. Stahlke, I. G. Todorov, and A. Winter, *Estimating quantum chromatic numbers*, Journal of Functional Analysis, vol. 270, No. 6, pp. 2188-2222, 2016.

[14] O. Regev and T. Vidick, *Quantum XOR Games*, ACM Transactions on Computation Theory, 7(2015), No.15, 1-43.
[15] W. Slofstra, *The set of quantum correlations is not closed*, Forum of Mathematics, Pi, 7(2019), e1.
[16] W. Slofstra, *Tsirelson's problem and an embedding theorem for groups arising from non-local games*, Journal of the American Mathematical Society, 33(2019), no. 1, 1–56.
[17] B. Tsirelson, *Some results and problems on quantum bell-type inequalities* Hadronic Journal Supplement, 8(1993), no. 4, 329–345.

Correlations in entanglement-assisted prepare-and-measure scenarios

Stefano Pironio
(joint work with Armin Tavakoli, Jef Pauwels, and Erik Woodhead)

Entanglement and quantum communication are paradigmatic resources in quantum information science leading to correlations that have no classical analogue. Correlations due to entanglement when communication is absent have for long been studied in Bell scenarios. Correlations due to quantum communication when entanglement is absent have been studied extensively in prepare-and-measure scenarios in the last decade. Here, we will present some results about correlations in scenarios that involve both entanglement and communication, focusing on entanglement-assisted prepare-and-measure scenarios. The paradigmatic example of such a scenario is the quantum dense coding protocol, where the communication capacity of a qudit can be doubled if a two-qudit entangled state is shared between Alice and Bob. We provide examples of correlations that actually require more general protocols based on higher-dimensional entangled states. This motivates us to investigate the set of correlations that can be obtained from communicating either a classical or a quantum d-dimensional system in the presence of an unlimited amount of entanglement. We show how such correlations can be characterized by a hierarchy of semidefinite programming relaxations by reducing the problem to a non-commutative polynomial optimization problem. We also introduce an alternative relaxation hierarchy based on the notion of informationally-restricted quantum correlations, which, though it represents a strict (non-converging) relaxation scheme, is less computationally demanding. As an application, we introduce device-independent tests of the dimension of classical and quantum systems that, in contrast to previous results, do not make the implicit assumption that Alice and Bob share no entanglement.

Entropy inequalities

Andreas Winter

What are the constraints that the von Neumann entropies of the 2^n possible marginals of an n-party quantum state have to obey? Similarly for the Shannon entropy of n random variables? Pippenger called these "the laws of (quantum) information theory", among them subadditivity and strong subadditivity, and while we know a few of them, we seem to be missing many. In fact, it is known that both

classically and quantumly, the set of entropy vectors is essentially a convex cone, so the laws in question naturally take the form of homogeneous convex inequalities, More specifically, we can describe the classical and entropy cones for n parties by linear information inequalities. Starting with Zhang and Yeung [1], Dougherty et al. [2] and finally Matus [3] have shown that 4-partite Shannon entropies satisfy infinitely many inequalities beyond the standard ones, the "Shannon inequalities", which define a polyhedral cone. Matus's result implies that the entropy cone of 4 random variables is not polyhedral. In this talk I will review progress towards finding non-von-Neumann inequalities in the quantum case, commenting briefly on the case of Rényi entropies as well.

References

[1] Z. Zhang and R. W. Yeung, *On characterization of entropy function via information inequalities,* IEEE Transactions on Information Theory, vol. 44, no. 4, pp. 1440–1452, (1998).
[2] R. Dougherty, C. F. Freiling, and K. Zeger, *Non-Shannon Information Inequalities in Four Random Variables,* arXiv preprint arXiv:1104.3602, (2011).
[3] F. Matus, *Infinitely Many Information Inequalities,* IEEE International Symposium on Information Theory, 2007, pp. 41–44.

General decompositions with invariance, positivity and approximations

Gemma De las Cuevas
(joint work with Matt Hoogsteder Riera, Andreas Klingler, Tim Netzer)

To specify a theory or framework, one need not only to describe its basic components but also how they *compose*, i.e. how they can be combined to give rise to other elements. For example, the postulates of quantum mechanics specify how to describe individual systems (as a ray in a Hilbert space), and how to describe composed systems (with the tensor product of Hilbert spaces). Composition is thus a fundamental and essential part of a theory.

Decomposition, i.e. expressing an object in the composed space in terms of its elementary constituents, is the inverse problem, and it appears in any theory relying on a composition rule—notably, in quantum many-body systems, but also multivariate polynomials or probabilistic graphical models. Decomposing an element is often hard, as the decomposition can reveal whether it has some notion of positivity (e.g. it is positive semidefinite or separable when considering matrix tensor product spaces), or of invariance (i.e. it is invariant under permutations of the local spaces given by an action of a group G). This applies to objects of very different nature within mathematics, physics and beyond, which can all be studied from the common umbrella of *general decompositions with invariance and positivity*.

Recently, such a unifying framework was proposed [4], which applies to spaces where the composition rule is given by the tensor product. In such a space, every

object can be expressed as a sum of elementary constituents

$$v = \sum_{\alpha=1}^{r} a_\alpha \otimes b_\alpha \otimes \cdots \otimes z_\alpha, \tag{1}$$

called a *tensor rank* decomposition. Whereas this is the natural decomposition from the perspective of mathematics, in (quantum) physics the following linear structure is considered in order to describe systems in one spatial dimension,

$$v = \sum_{\alpha_1,\ldots,\alpha_{n-1}=1}^{r} a_{\alpha_1,\alpha_2} \otimes b_{\alpha_2,\alpha_3} \otimes \cdots \otimes z_{\alpha_{n-1},\alpha_1}, \tag{2}$$

called a *Matrix Product State* representation of v [12]. But there are many other possibilities to arrange these indices (a combinatorial number depending on n). Our framework described all such decompositions by means of a *weighted simplicial complex* Ω: *The summation indices are associated with the facets of a weighted simplicial complex, and elementary constituents are associated with their vertices.* In addition, for invariant objects under a group of permutations G, this invariance can be made explicit in the elementary tensors, resulting in a so-called (Ω, G)-*decomposition*. For example, choosing the local vectors in a elementary tensor to be the same

$$v = \sum_{\alpha=1}^{r} a_\alpha \otimes a_\alpha \otimes \cdots \otimes a_\alpha \tag{3}$$

results in a *symmetric tensor rank* decomposition. Similarly, a *translational invariant Matrix Product State* is given by

$$v = \sum_{\alpha_1,\ldots,\alpha_{n-1}=1}^{r} a_{\alpha_1,\alpha_2} \otimes a_{\alpha_2,\alpha_3} \otimes \cdots \otimes a_{\alpha_{n-1},\alpha_1}. \tag{4}$$

By construction, if an object admits an (Ω, G)-decomposition, then it is G-invariant. The main question considered in [4] was the converse: If an object is G-invariant, when does it admit an invariant decomposition? A sufficient condition for the existence of an invariant decomposition was given, and it was shown that the multiplicity of the facets of Ω (or equivalently the number of summation indices) can always be increased to satisfy this condition.

This framework contains as very special cases the tensor rank and symmetric tensor rank decomposition, as well as various notions of inherently positive decompositions that apply to positive semidefinite matrices or entrywise nonnegative tensors. Particular examples are the nonnegative [2], positive semidefinite [9], completely positive [1] and completely positive semidefinite transposed decompositions [5] of matrices. In addition, it includes the local purification form [7] and the Matrix Product Density Operator form [14, 15]. This framework thus unifies decompositions with and without positivity or symmetry which are well-studied in algebraic geometry, convex optimisation, quantum information and quantum many-body systems. Moreover, every (Ω, G)-decomposition has an associated rank, defined as the minimal number of terms in the sum, and we study how

these ranks are modified when varying Ω or G. In this way, we can compare ranks, and we find that the largest one is the tensor rank (the minimal r in Eq. (1)).

While this framework is inspired by quantum many-body systems [4], we have also applied it to multivariate polynomials [6], and have thus transferred results about separations of ranks [7], the lack of local certificates of positivity in unconstrained decompositions [3], and the existence of explicitly invariant and inherently positive decompositions among the two.

In addition, we have extended this framework to the *approximate* case, where the notion of approximation is given by ε-balls around the elements (in some norm). We have shown that essentially all separations among ranks disappear in the approximate case. To prove this result, we have leveraged a recent version of the *approximate Carathéodory Theorem* [10], showing that every element in a convex hull can be approximately represented with a number of extremal points, and only depending on the error, independent of the system dimension.

There are several open questions for further research. Concerning the error analysis, what is the *border rank* of an (Ω, G)-decomposition? In particular, what is the minimal rank of descriptions with an error going to 0. While the border rank coincides with the rank of an exact description for many cases (including the matrix rank [8] or positive factorisations [9]), this is in general not true for multipartite tensors and tensor (network) decompositions thereof [11]. The existence of non-trivial border ranks of locally positive decompositions remains open.

Another perspective would be a generalised version of Comon's conjecture which states that the tensor rank and its symmetric analogue always coincide for symmetric tensors. Recently, this conjecture has been disproven, i.e. there exist tensors whose standard tensor rank is strictly smaller than its symmetric tensor rank [13]. Studying other decomposition geometries, the W-state is a representative example for a separation between the operator Schmidt rank and the translational invariant operator Schmidt rank, as shown in [5, 12]. The framework of (Ω, G)-decompositions provides the means to generalise this statement, namely characterising decomposition geometries Ω and symmetries G where the Ω-rank is different from the (Ω, G)-rank.

References

[1] A. Berman and N. Shaked-Monderer. *Completely Positive Matrices*. World Scientific, 2003.

[2] J. E. Cohen and U. G. Rothblum. *Nonnegative ranks, decompositions, and factorizations of nonnegative matrices*. Linear Algebra Appl., 190(C):149–168, 1993.

[3] G. De las Cuevas, T. S. Cubitt, J. I. Cirac, M. M. Wolf, and D. Pérez-García. *Fundamental limitations in the purifications of tensor networks*. J. Math. Phys., 57(7):071902, 2016.

[4] G. De las Cuevas, M. Hoogsteder Riera, and T. Netzer. *Tensor decompositions on simplicial complexes with invariance*. 2019. arXiv:1909.01737

[5] G. De las Cuevas, A. Klingler, and T. Netzer. *Approximate tensor decompositions: disappearance of many separations*. J. Math. Phys., 62(9):093502, 2021.

[6] G. De las Cuevas, A. Klingler, and T. Netzer. *Polynomial decompositions with invariance and positivity inspired by tensors*. 2021. arXiv:2109.06680

[7] G. De las Cuevas, N. Schuch, D. Pérez-García, and J. I. Cirac. *Purifications of multipartite states: Limitations and constructive methods*. New J. Phys., 15, 2013.

[8] C. Eckart and G. Young. *The approximation of one matrix by another of lower rank.* Psychometrika, 1(3):211–218, 1936.
[9] H. Fawzi, J. Gouveia, P. A. Parrilo, R. Z. Robinson, and R. R. Thomas. *Positive semidefinite rank.* Math. Program., 153(1):133–177, 2015.
[10] G. Ivanov. *Approximate Carathéodory's Theorem in Uniformly Smooth Banach Spaces.* Discrete Comput. Geom. 66:273–280, 2021.
[11] J. M. Landsberg, Y. Qi, and K. Ye. *On the geometry of tensor network states.* Quantum Inf. Comput., 12(3-4):346–354, 2012.
[12] D. Perez-Garcia, F. Verstraete, M. M. Wolf, and J. I. Cirac. *Matrix product state representations.* Quantum Inf. Comput., 7(5-6):401–430, 2007.
[13] Y. Shitov. *A Counterexample to Comon's Conjecture.* SIAM J. Appl. Algebra Geom., 2(3):428–443, 2018.
[14] F. Verstraete, J. J. García-Ripoll, and J. I. Cirac. *Matrix product density operators: Simulation of finite-temperature and dissipative systems.* Phys. Rev. Lett., 93(20):12–15, 2004.
[15] M. Zwolak and G. Vidal. *Mixed-state dynamics in one-dimensional quantum lattice systems: A time-dependent superoperator renormalization algorithm.* Phys. Rev. Lett., 93(20):1–5, 2004.

Mutually unbiased bases, polynomial optimization & symmetry

Sander Gribling
(joint work with Sven Polak)

Let $d \in \mathbb{N}_{\geq 2}$. A set of k orthonormal bases of $\mathbb{C}^d$ is called *mutually unbiased* if

$$(*) \qquad |\langle e, f\rangle|^2 = \frac{1}{d}$$

whenever e and f are basis vectors in *distinct* bases. A natural question is for which pairs (d, k) there exist k mutually unbiased bases in dimension d. A dimension counting argument shows that there can be at most $d+1$ mutually unbiased bases (MUBs) in dimension d. No other general upper bounds are known. When d is a power of a prime number it is known that there exists a set of $d+1$ MUBs [10, 16]. However, for all d that are not a power of a prime the question is wide open. Even for the first such number, dimension 6, it is not known whether there exist more than 3 such bases, despite extensive numerical search [4]. It is known however that certain sets of 3 MUBs are *maximal*, i.e., they can not be extended, see [8]. Zauner conjectured that there do not exist 4 MUBs in dimension 6 [18]. This conjecture is widely believed, but there is no formal proof. We refer to [3] for an excellent survey on mutually unbiased bases. MUBs have many applications in quantum information theory, for example in tomography algorithms, cryptographic protocols, and entanglement detection.

Navascués, Pironio, and Acín [13] gave a C^*-algebraic formulation of the above problem: k MUBs exist in dimension d if and only if a certain C^*-algebra has a representation with $I \neq 0$. This formulation naturally gives rise to a (tracial) noncommutative polynomial optimization approach and thus to semidefinite programming relaxations. Proving infeasibility of such a relaxation would prove non-existence of k MUBs in dimension d. We follow this approach and exploit the symmetries in the resulting semidefinite programming hierarchy.

Symmetry is widely used in semidefinite programming and polynomial optimization with applications in many areas including coding theory, combinatorics, and geometry; for an overview see [2] and references therein. Symmetry in semidefinite programs can be used to reduce the size of the involved matrices. Indeed, it is a consequence of Schur's lemma that a complex matrix $*$-algebra $\mathcal{A}$ is $*$-isomorphic to a direct sum of full matrix algebras. That is, there exists a $*$-isomorphism ϕ such that

$$\phi(\mathcal{A}) = \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i}. \tag{1}$$

Constructing this $*$-isomorphism is often challenging. There exist numerical methods to do so, or can use the regular $*$-representation to obtain a representation of $\mathcal{A}$ in an (often) smaller matrix algebra. We focus on the setting where the algebra consists of matrices that are invariant under a permutation action of a (finite) group. That is, we consider the matrix $*$-algebra $\mathcal{A} = (\mathbb{C}^{Z\times Z})^G$ of G-invariant $Z \times Z$ matrices where the group G acts on the finite set Z. In this setting one can construct the $*$-isomorphism from (1) explicitly. To do so, one needs to decompose the G-module $\mathbb{C}^Z$ into a direct sum of irreducible G-modules. Group invariance has been used previously in (commutative) polynomial optimization, see for example [6, 14]. Finding the $*$-isomorphism (i.e., the decomposition of $\mathbb{C}^Z$) remains challenging even in the group-invariance setting.

What is the symmetry in the MUB problem? Let S_n be the symmetric group on n elements. The MUB property $(*)$ of a set of k MUBs in dimension d is naturally invariant under relabeling the bases (an S_k action) and, for each basis, relabeling the basis elements (S_d actions). These actions together precisely define an action of the wreath product $S_d \wr S_k$. One can show that the C^*-algebraic formulation and the related semidefinite programming (SDP) relaxations are invariant under this action. Our main contribution is a decomposition of the ring of homogeneous degree-t polynomials in variables $x_{i,j}$ $(i \in [d], j \in [k])$ into irreducible $S_d \wr S_k$-modules. In other words, we decompose the $S_d \wr S_k$-module $\mathbb{C}^Z$ where $Z = ([d] \times [k])^t$. The irreducible modules for wreath products of finite groups are well known, see, e.g., [11]. However, in general there is no explicit description of the homomorphisms from the irreducible modules to other $S_d \wr S_k$-modules. See [9] for a partial description. Our decomposition of $\mathbb{C}^{([d]\times[k])^t}$ involves constructing novel explicit homomorphisms for certain "L-shaped permutation modules".[1]

There are two canonical actions of the wreath product of $S_d \wr S_k$: a primitive action on $[d]^k$ and an imprimitive action on $[d] \times [k]$. We have studied the imprimitive action. The primitive action is the one used extensively in coding theory related SDPs: see the fundamental work of Schrijver [15] and subsequent works that rely on representation theory [7, 12].

Using our symmetry reduction we obtain numerical sum-of-squares certificates for the non-existence of $d + 2$ MUBs in dimensions $d = 2, 3, 4, 5$, see Table 1. We used the SDP-solvers SDPA-GMP, SDPA-DD or SDPA [17].

[1]For $t = 1$ the separate actions of S_d on $\mathbb{C}^{[d]^t}$ and S_k on $\mathbb{C}^{[k]^t}$ are transitive and the analytic decomposition can be obtained for example from [5, Thrm. 3.1.1].

d	k	t	size $= (dk)^{\lfloor t \rfloor}$	#variables	(sum,max) block sizes	result
2	4	4.5	4096	7	(1776, 380)	**infeasible**
3	5	4.5	50625	7	(4529, 587)	**infeasible**
4	6	5	7962624	43	(22225,1775)	**infeasible**
5	7	5.5	52521875	75	(89385, 5495)	**infeasible**
6	4	5.5	7962624	54	(67224, 5361)	feasible
6	7	5.5	130691232	75	(92371, 5496)	feasible

TABLE 1. We give the number of rows of the original t-th level SDP, and for the symmetry reduced SDP the number of variables, the sum and max of the block sizes, and the solver status.

Finally, we mention some directions for future work. A reformulation of the MUB problem in terms of a nonlocal game based on quantum random access codes is given in [1]. This gives gives rise to another SDP hierarchy that can be used to prove non-existence of certain sets of MUBs and in [1] they numerically exploit the symmetry in the corresponding SDPs (and rule out the existence of $d + 2$ MUBs in dimensions $d = 3, 4$). We leave it for future work to combine our analytical symmetry reduction with their approach. A second, more open problem is whether it is possible to further exploit the small number of variables in the symmetry reduced SDPs.

REFERENCES

[1] E.A. Aguilar, J.J. Borkała, P. Mironowicz, and M. Pawłowski. *Connections between mutually unbiased bases and quantum random access codes.* Phys. Rev. Lett., 121:050501, Jul 2018.

[2] C. Bachoc, D.C. Gijswijt, A. Schrijver, and F. Vallentin. *Invariant semidefinite programs.* Handbook on Semidefinite, Conic and Polynomial Optimization, pages 219–269. Springer, 2012.

[3] I. Bengtsson, W. Bruzda, A. Ericsson, J-A. Larsson, W. Tadej, and K. Życzkowski. *Mutually unbiased bases and Hadamard matrices of order six.* Journal of Mathematical Physics, 48(5):052106, 2007.

[4] S. Brierley and S. Weigert. *Constructing mutually unbiased bases in dimension six.* Phys. Rev. A, 79:052316, May 2009.

[5] T. Ceccherini-Silberstein, F. Scarabotti, and F. Tolli. *Representation Theory and Harmonic Analysis of Wreath Products of Finite Groups.* London Mathematical Society Lecture Note Series (410). Cambridge University Press, 2013.

[6] K. Gatermann and P.A. Parrilo. *Symmetry groups, semidefinite programs, and sums of squares.* Journal of Pure and Applied Algebra, 192(1–3):9–128, 2004.

[7] D.C. Gijswijt. *Block diagonalization for algebra's associated with block codes.* arXiv:0910.4515, 2009.

[8] M. Grassl. *On SIC-POVMs and MUBs in Dimension 6.* In Proceedings ERATO Conference on Quantum Information Science 2004 (EQIS 2004), pages 60–61, 2004. quant-ph/0406175.

[9] R. Green. *Some properties of Specht modules for the wreath product of symmetric groups.* PhD thesis, University of Kent, 2019.

[10] I.D. Ivanović. *Geometrical description of quantal state determination.* Journal of Physics A: Mathematical and General, 14(12):3241–3245, 1981.

[11] A. Kerber. *Representations of Permutation Groups I.* Lecture Notes in Mathematics. Springer-Verlag, 1971.

[12] B. Litjens, S. Polak, and A. Schrijver. *Semidefinite bounds for nonbinary codes based on quadruples.* Designs, Codes and Cryptography, 84:87–100, 2017.
[13] M. Navascués, S. Pironio, and A. Acín. *SDP relaxations for non-commutative polynomial optimization.* In Handbook on Semidefinite, Conic and Polynomial Optimization, pages 601–634. Springer, 2012.
[14] C. Riener, T. Theobald, L. Jansson Andrén, and J.B. Lasserre. *Exploiting symmetry in sdp-relaxations for polynomial optimization.* Mathematics of Operations Research, 38:122–141, 2013.
[15] A. Schrijver. *New code upper bounds from the terwilliger algebra and semidefinite programming.* IEEE Transactions on Information Theory, 51(8):2859–2866, 2005.
[16] W.K. Wootters and B.D. Fields. *Optimal state-determination by mutually unbiased measurements.* Annals of Physics, 191(2):363 – 381, 1989.
[17] M. Yamashita, K. Fujisawa, M. Fukuda, K. Kobayashi, K. Nakata, and M. Nakata. *Latest developments in the SDPA Family for solving large-scale SDPs.* In Handbook on Semidefinite, Conic and Polynomial Optimization, pages 687–714. Springer, 2012.
[18] G. Zauner. *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie.* PhD thesis, University of Vienna, 1999.

Noncommutative Group Symmetries and Optimization

Michael Walter

We report on a recent work initiating the systematic development of a theory of geodesically convex optimization on Riemannian manifolds that arise from the symmetries of noncommutative groups [1]. This builds on and generalizes a growing body of work from the past few years which gave algorithmic solutions in important special cases. A fundamental algorithmic problem in this setting is the following. Consider a complex reductive group G acting linearly on a finite-dimensional Hilbert space V, with a maximal compact subgroup K acting unitarily. Given a vector $v \in V$, we wish to minimize the norm over its orbit:

$$\operatorname{cap}(v) := \inf \{\|w\| : w \in G \cdot v\}.$$

This problem is geodesically convex when formulated on the symmetric space G/K. Remarkably, for different group actions it captures natural important problems in algebra (null cone), computational complexity (noncommutative polynomial identity testing), analysis (Brascamp-Lieb inequalities), statistics (maximum likelihood estimation), and quantum information (marginal problems). Even when restricted to commutative groups, it already captures all of linear programming – a well-known and powerful paradigm in mathematical optimization. Related algorithmic questions are to minimize moment maps (a noncommutative notion of the usual gradient) and to test membership in moment polytopes (convex polytopes, typically of exponential vertex and facet complexity, which arise from this a priori nonconvex setting). The above captures a diverse set of problems in different areas of computer science, mathematics, and physics. Several of them were solved efficiently for the first time using optimization methods; the corresponding algorithms also lead to solutions of purely structural problems and to many new connections between disparate fields.

In the spirit of standard convex optimization, we develop two general methods in the geodesic setting, a first order and a second order method, which receive first and second order information, respectively, on the "derivatives" of the function to be optimized. These methods in particular subsume all past results. The main technical work goes into identifying the key parameters of the underlying group actions which control convergence to the optimum in each of these methods. These noncommutative analogues of "smoothness" are far more complex and require significant algebraic and analytic machinery. Despite this complexity, the way in which these parameters control convergence in both methods is quite simple and elegant. We show how to bound these parameters and obtain efficient algorithms for null cone membership in several concrete situations. Finally, we discuss intriguing open problems and further research directions.

References

[1] P. Bürgisser, C. Franks, A. Garg, R. Oliveira, M. Walter, A. Wigderson, *Towards a theory of non-commutative optimization: geodesic first and second order methods for moment maps and polytopes*, Proceedings of the 60th IEEE Symposium on Foundations of Computer Science (FOCS 2019), 845–861.

Geometry of Banach spaces: a new route towards Position Based Cryptography

David Perez-Garcia

(joint work with Marius Junge, Aleksander M. Kubicki, C. Palazuelos)

In the field of Position Based Cryptography (PBC) one aims to develop cryptographic tasks using the geographical position of a third party as its only credential. Once the party proves to the verifier that it is in fact located at the claimed position, they interact considering the identity of the third party as granted. This may result very appealing in practical applications and, notably, it presents the only known proposal to prevent man-in-the-middle attacks without the need of a secure private channel. Furthermore, since the study of PBC entered into the quantum domain approximately a decade ago, beautiful and striking connections were established with topics ranging from classical complexity theory to AdS/CFT holographic correspondence. All this endow the study of PBC with a remarkable interest also from a fundamental point of view, perspective that we take as our main motivation in this work. In particular, here we build a new deep connection with geometric functional analysis that is at the heart of our main results. This also allows us to introduce new ideas and techniques in a field whose development has slowed down due to the unexpected difficulty of the most fundamental questions about it. We hope this work sparkles a renewed interest on the community on these far reaching problems.

The main task in PBC is called *Position Verification* (PV). In PV a prover has to convince a verifier (usually composed by several agents spatially distributed) that he is located at a claimed position. In purely classical scenarios, PV is easily

proven to be insecure against a team of colluding adversaries surrounding the honest location. That motivates the study of *quantum* PV schemes. Nonetheless, it turns out that quantum PV can be also attacked and therefore, informationally secure PV is not possible. Intriguingly, known general attacks build on the delicate manipulation of quantum entanglement being this, in fact, a necessary resource to compromise the security of general PV quantum protocols. The main question regarding this setting is then the optimal amount of entanglement necessary to break *any* PV protocol. Known upper bounds for that quantity are exponential in the size of the quantum systems manipulated in the honest implementation of the protocol while best lower bounds are only linear. This leaves the previous question widely open. Proving that the correct scaling is indeed exponential would lead to protocols that can be regarded as *secure for all practical purposes*. On the contrary, finding general attacks to PV using only polynomially sized entanglement would dramatically restrict the security guarantees in PBC. Our central goal is making progress on the understanding of this dichotomy.

Main results. For that, we propose a PV protocol in the simplest one-dimensional case (1-D PV) and find lower bounds on the resources needed to break it. We denote G_{Rad} the proposed protocol that, as customary, makes reference to a family $\{G_{Rad}^{(n)}\}_{n\in\mathbb{N}}$ rather than to a single task. The index n represents the security parameter and it determines the *quantum size* of the protocol. More concretely, in $G_{Rad}^{(n)}$ the honest prover is required to manipulate an n^2 dimensional quantum system. In this work we are interested just on entanglement consumption and hence we will assume that both classical communication and computational power are not limited.

In 1-D PV, two verifiers in a line surrounding a point x aim to verify that the prover they communicate with is located at x. The general structure of a PV protocol in this setting proceeds in three basic steps: first, the verifiers prepare a bipartite system and communicate it to x: one part of the system is communicated to this point from the left, and the other, from the right. Secondly, when a honest prover located at x receives both registers, he has to immediately apply a required computation resulting in another bipartite system that has to be returned to the verifiers. One register should be sent to the verifier at the left of x, and the other, to its right. Finally, the verifiers check whether prover's answer arrives on time and whether the computation was performed correctly. Based on this information they declare the verification correct or not.

In the dishonest scenario, two cheaters surrounding the location x, intercept the communication between verifiers and honest prover and try to emulate the ideal action in the honest protocol avoiding any delay in their response. This restricts the cheater's action, called strategy from now on, to consist of two rounds of local operations mediated by a step of *simulatenous two-way communication* – see Section 2.2 in the main text of this submission for a detailed discussion on that.

Once we have fixed the basic setting we study, let us describe the protocol G_{Rad} involved in our main results. The honest implementation is as follows: given $n \in \mathbb{N}$, in $G_{Rad}^{(n)}$ the verifiers start uniformly sampling a vector of n^2 signs $\varepsilon =$

$(\varepsilon_{ij})_{i,j=1}^{n}$, where $\varepsilon_{ij} = \pm 1$ for each $i, j = 1, \ldots, n$, and preparing the state $|\psi\rangle := \frac{1}{n}\sum_{i,j} |i\rangle_A \otimes |j\rangle_B \otimes |ij\rangle_C$ in a tripartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. Registers $\mathcal{H}_A \otimes \mathcal{H}_B$ are both forwarded to the verifying location x from one of the verifiers, let us say from the left of x. This verifier keeps register $\mathcal{H}_C$ private during the execution of the protocol. From the right, the classical information about the choice of ε is communicated. A honest prover located at x, upon receiving both pieces of information, has to apply the diagonal unitary determined by ε on the received state. Immediately, registers $\mathcal{H}_A \otimes \mathcal{H}_B$ must be returned, but this time only $\mathcal{H}_A$ should travel to the verifier at the left. $\mathcal{H}_B$ should be sent to the verifier at the right. After receiving those registers, the verifiers check answer's timing and, at some later time, they perform the measurement $\{|\psi_\varepsilon\rangle\langle\psi_\varepsilon|, \mathrm{Id} - |\psi_\varepsilon\rangle\langle\psi_\varepsilon|\}$ on the whole system $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, where $|\psi_\varepsilon\rangle := \frac{1}{n}\sum_{i,j} \varepsilon_{ij}|i\rangle_A \otimes |j\rangle_B \otimes |ij\rangle_C$. They accept the verification only if the arriving time was correct and the outcome of the measurement was the one associated to $|\psi_\varepsilon\rangle\langle\psi_\varepsilon|$.

Coming back to the dishonest scenario, specialized in this case for G_{Rad}, we can informally state our main result as follows:

If the cheating strategy depends on the value of $\varepsilon \in \{\pm 1\}^{n^2}$ in a sufficiently regular way, then the entanglement needed to pass $G_{Rad}^{(n)}$ is exponential in n.

In order to formalize this result, we need to quantify the *regularity of a strategy*. We do this following two complementary approaches that lead to the definition of two regularity parameters, $\sigma_{\mathcal{S}}^{i}$ and $\sigma_{\mathcal{S}}^{ii}$. These parameters can be in fact understood as vector-valued measures of the *total influence* of a strategy regarded as a function on the Boolean cube. Complementing this analytic understanding of $\sigma_{\mathcal{S}}^{i}$ and $\sigma_{\mathcal{S}}^{ii}$, we can also give a more operational interpretation for these regularity parameters. More concretely, a given cheating strategy is determined by a family of quantum operations $\{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon\}_{\varepsilon\in\{\pm1\}^{n^2}}$ and an entangled state they share in advance, $|\varphi\rangle$. In their strategy, depending on the value ε sampled by the verifiers in a given instance of the challenge, the cheaters first apply operators $V \otimes W_\varepsilon$ and, after communicating, they apply $\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon$. With this, $\sigma_{\mathcal{S}}^{i(ii)}$ can be upper bounded, up to multiplicative logarithmic factors, by the following expressions:

$$\sigma_{\mathcal{S}}^{i} \lesssim_{\log} \mathbb{E}_\varepsilon \left(\sum_{i,j} \frac{1}{2} \left\| \tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon - \tilde{V}_{\overline{\varepsilon}^{ij}} \otimes \tilde{W}_{\overline{\varepsilon}^{ij}} \right\|^2 \right)^{1/2} + \mathcal{O}\left(\frac{1}{n}\right),$$

$$\sigma_{\mathcal{S}}^{ii} \lesssim_{\log} \mathbb{E}_\varepsilon \left(\sum_{i,j} \frac{1}{2} \left\| V \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}})\, |\varphi\rangle \right\|_{\ell_2}^2 \right)^{1/2} + \mathcal{O}\left(\frac{1}{n}\right),$$

where $\overline{\varepsilon}^{ij}$ denotes the sign vector $(\varepsilon_{11}, \ldots, -\varepsilon_{ij}, \ldots, \varepsilon_{nn})$. These expressions measure how strongly the first (resp. second) round of local operations implemented by the cheaters in their strategy depend on ε. We note that current attacks to PV based on teleportation or port-based teleportation are *sufficiently regular*, that is, they fulfil $\sigma_{\mathcal{S}}^{i} = \mathcal{O}(\log(n)/n)$.

We can now state our main theorem in a more rigorous way:

Theorem 1. *Consider a cheating strategy for $G^{(n)}_{Rad}$, $\mathcal{S}$, attaining acceptance probability of at least $1-\epsilon$ for some $0 \leq \epsilon \leq \frac{1}{8}$. Denote by k the local dimension of the quantum resources used in $\mathcal{S}$. If $\sigma^{i}_{\mathcal{S}} = \mathcal{O}(\mathrm{polylog}(n)/n^{\alpha})$ or $\sigma^{ii}_{\mathcal{S}} = \mathcal{O}(\mathrm{polylog}(n)/n^{3/4+\alpha})$ for some $\alpha > 0$, then:*

$$k = \Omega\Big(\exp\left(n^{\alpha'}\right)\Big) \quad \textit{for some } \alpha' > 0.$$

Even when known constructions verify the smoothness assumption above, we do not know how generic this behaviour is. Moreover, we connect the possibility of dropping out this assumption and obtaining unconditional bounds with a collection of open problems in the area of geometric functional analysis. These open problems are concerned with the estimation of type constants for the tensor product of finite dimensional Hilbert spaces, endowed with some tensor norms, and the relation between the cotype of these spaces and their volume ratio.

Multipartite entanglement detection via projective tensor norms

Cécilia Lancien

(joint work with Maria Anastasia Jivulescu and Ion Nechita)

Determining whether a multipartite quantum system is in a *separable* or an *entangled* state is of prime importance in quantum information theory. Indeed, if such a quantum system is in a separable state, it means that there are no intrinsically quantum correlations between its subsystems, so that it is not providing any advantage compared to a classical system in information processing tasks. However, the problem of deciding if a multipartite quantum state is separable or entangled (and even only approximate versions of it) is known to be computationally hard [2]. Standard solutions to overcome this practical difficulty consist in looking for necessary conditions to separability that would be easier to check than separability itself. These are usually dubbed *entanglement criteria*, and various families of such criteria have already been extensively studied in the past. From a mathematical point of view, a quantum state is described by a positive semidefinite operator on a complex Hilbert space having unit Schatten 1-norm. And for a quantum state on a multipartite system (i.e. on a tensor product Hilbert space), being entangled is characterized by having a so-called *projective Schatten* 1*-norm* which is strictly larger than 1 [5]. But there is no efficient way of estimating such tensor norm in general [4]. An alternative consists in looking at other tensor norms, whose values are easier to compute and always smaller than the tensor norm characterizing entanglement (so that if they are strictly larger than 1, then the state is guaranteed to be entangled).

This is the approach that we take in this work. We define and study a class of entanglement criteria based on the idea of applying local contractions to an input multipartite state, and then computing the projective tensor norm of the output. More precisely, the local contractions that we consider are from the Schatten 1-norm to the ℓ_2 norm, i.e. from a non-commutative space to a commutative one. This is what makes such entanglement criteria interesting in practice: they can

be seen as reducing the study of mixed state entanglement to that of pure state entanglement, which is an easier task.

Another advantage of our entanglement criteria is that their definition is independent from the number of subsystems. Several aspects are, admittedly, simpler to understand in the bipartite case, but they remain equally well-suited to the case where more than two parties are involved. In fact, one of the main issues with most well-known entanglement criteria is that they are specifically designed for bipartite systems, and generalizations to systems with more parties are not fully satisfying. Indeed, they usually consist in applying the bipartite criterion across all bipartitions, which certifies entanglement across bipartitions of the subsystems, but not genuinely multipartite entanglement [3].

Well studied entanglement criteria, such as the realignment criterion [1, 6] and the SIC POVM criterion [7], are important examples in the framework we consider. Our work provides natural generalizations of these criteria to the multipartite setting, going beyond the biseparable case already discussed in the literature. Moreover, we establish an exact relation between the performance of the realignment and the SIC POVM criteria, solving in the positive two conjectures from [7]. We are in fact able to quantify more generally how all *symmetric testers* perform in detecting the entanglement of several classes of bipartite states: pure states, Werner states, isotropic states, pure states with white noise. Another natural question that we ask is whether our family of entanglement criteria is complete, i.e. in other words, whether any entangled state can be detected by a tester. We show that, in the bipartite case, the answer is yes, when allowing for a permutation of indices of the considered state before applying the testers. Finally, we take a closer look at the multipartite case. We show that our extension of the realignment criterion to this setting detects all entangled pure states, as in the bipartite case.

To summarize, we introduce in this work a new paradigm for entanglement detection in bipartite and multipartite quantum systems, based on entanglement testers. It consists in reducing the entanglement problem of mixed quantum states (i.e. computing a projective Schatten 1-norm) to that of pure quantum states (i.e. computing a projective ℓ_2 norm). The latter is know to be much simpler, but this is at the cost of obtaining only a sufficient criterion for entanglement.

The main question that remains unanswered at this point is whether our family of entanglement criteria is complete, without allowing for a preliminary reshuffling of indices. In the bipartite case, this problem can be seen as a *factorization through* ℓ_2 problem. In a different direction, it would be worth investigating further the performance of our entanglement criteria in the multipartite setting. Indeed, the only quantitative results that we establish in this work when more then two parties are involved are for pure states. But what about the case of mixed states? Are there interesting classes of multipartite mixed states whose entanglement can be detected by the realignment or SIC POVM testers? And can we, in general, compare the respective performances of these two testers? Finally, it could be interesting to probe the efficiency of entanglement testers in the case where the output dimension is (much) smaller than the dimension of the input space. Although

such testers cannot be *perfect* (i.e. detect all entangled pure states), computing the projective norm of the output tensor is easier when the dimension is smaller, so the trade-off between the computational efficiency and the performance of these testers needs to be assessed.

References

[1] K. Chen and L. Wu. *A matrix realignment method for recognizing entanglement.* Quantum Information and Computation 3:193–202, 2003.

[2] S. Gharibian. *Strong NP-hardness of the quantum separability problem.* Quantum Information and Computation 3:343–360, 2010.

[3] M. Horodecki, P. Horodecki and R. Horodecki. *Separability of mixed quantum states: linear contractions and permutation criteria.* Open Systems & Information Dynamics 13(1):103–111, 2006.

[4] D. Pérez-García. *Deciding separability with a fixed error.* Physics Letters A 330(3-4):149–154, 2004.

[5] O. Rudolph. *A separability criterion for density operators.* Journal of Physics A: Mathematical and General 33(21):3951, 2000.

[6] O. Rudolph. *Computable cross-norm criterion for separability.* Letters in Mathematical Physics 70:57–64, 2004.

[7] J. Shang , A. Asadian, H. Zhu and O. Gühne. *Enhanced entanglement criterion via symmetric informationally complete measurements.* Physical Review A 98(2):022309, 2018.

Efficient classical simulation of random shallow 2D quantum circuits

Aram Harrow

(joint work with John Napp, Rolando La Placa, Alexander Dalzell, Fernando Brandão)

Overview. One of the most basic questions in quantum computing is whether a given class of quantum computations admits an efficient classical simulation. Due to the exponential blowup in Hilbert space dimension associated with an extensive quantum system, brute-force simulation quickly becomes intractable. However, this does not preclude the existence of clever classical simulation algorithms which exploit extra structure of the problem at hand to obtain efficiency: classic examples include 1D quantum circuits with low entanglement (simulatable via MPS) and Clifford circuits (simulatable via the Gottesman-Knill theorem).

In this work, we add another class of quantum circuits to this list: namely, random, sufficiently shallow, 2D quantum circuits. Besides the fact that delineating the boundary between classically simulatable and classically hard-to-simulate processes is a basic question in computational complexity theory, random circuits are of use in physics due to their being models of chaotic quantum dynamics, and in quantum computation due to (among other applications) the fact that Random Circuit Sampling (RCS) — that is, sampling from the output distribution produced by a random circuit — is a leading candidate for demonstrating so-called "quantum computational supremacy", and in fact was the basis for Google's recent claim of achieving this [1]. In this context, it becomes crucial to understand the asymptotic hardness of the RCS problem. Unfortunately, while there are some

hardness results for RCS under additional conjectures which have not received widespread scrutiny, strong theoretical evidence remains sparse. A major advance was made by Bouland, Fefferman, Nirkhe, and Vazirani [2], who proved that the alternative problem of computing output probabilities of random circuits admits a certain worst-to-average case reduction; since computing output probabilities of generic instances is intractable under widely believed assumptions, this work essentially showed that computing output probabilities of random circuits is intractable. Subsequently, Movassagh made a technical improvement to this result [3].

Despite these strong hardness results for computing output probabilities, we describe an efficient classical algorithm for the RCS problem in the setting of sufficiently shallow 2D circuits. This algorithm is only efficient for *shallow* circuits, and therefore does not refute Google's quantum computational supremacy claims which are based on *deep* circuits. Nonetheless, the existence of such an algorithm has some bearing on the line of work attempting to establish the hardness of RCS. The conventional wisdom, partially informed by [2, 3], has been that for a given architecture, random gates should be almost the hardest possible. Our work challenges this intuition and cautions against making bold average-case hardness conjectures by showing that there is a natural setting where simulation is exponentially easier for typical instances than for the worst case.

As a more concrete implication, our work demonstrates limitations of the hardness results of [2, 3] in providing evidence for the hardness of RCS. In particular, these hardness results do apply to the shallow random circuit families we study, showing that near-exactly computing output probabilities is average-case hard. Yet, we find that it is classically tractable to solve the RCS problem, and even to compute typical output probabilities when some small additive error is allowed. While the hardness results of [2, 3] apply to computing output probabilities, they have been widely cited as evidence for the hardness of RCS; however, our work implies that there are natural settings in which classically solving the RCS problem is far easier than precisely computing output probabilities in the average case. Therefore, hardness results for the latter task should not in isolation be viewed as evidence for hardness of the former.

Interestingly, we also find evidence that our algorithms experience computational phase transitions from polynomial-time to exponential-time when the circuit depth or local dimension exceeds some critical, constant value. As elaborated upon below, we relate these computational phase transitions to (1) measurement-driven entanglement phase transitions in 1D chaotic quantum dynamics, and (2) phase transitions in classical statistical mechanical models.

Simulation algorithms. We propose two classical simulation algorithms for (noiseless) random shallow 2D quantum circuits. To the best of our knowledge, these algorithms represent the first simulation algorithms for 2D random circuits which go beyond (exponential-time) methods based on tensor network contraction. The first algorithm, which is also the algorithm we study in greatest depth, is based on a reduction of the 2D simulation problem to the problem of simulating a certain 1D

dynamics evolving in time. In turn, this effective 1D dynamics is simulated via Matrix Product State (MPS) methods. More precisely, the effective 1D dynamics is simulated using the Time Evolving Block Decimation (TEBD) algorithm of Vidal [4], which involves periodically truncating (i.e. compressing) the MPS; we therefore refer to this algorithm as Space Evolving Block Decimation (`SEBD`). While MPS are used to simulate the effective 1D dynamics, we note that `SEBD` is not merely a tensor network contraction scheme, but crucially exploits the unitarity of the circuit for its effectiveness. This differentiates it from simulation proposals for random circuits based on truncated tensor network contractions (e.g. [5]). Also unlike such truncated tensor network contraction approaches, the algorithm is *self-certifying* in the sense that it can bound the sampling error it's making as a function of the Schmidt coefficients discarded in the MPS compression steps, even though exact simulation is hard and therefore the exact solution is unknown. This self-certification feature allows us to numerically study the performance of the algorithm. Our second proposed algorithm, which we call `Patching`, is based on first exactly sampling from the marginal distributions of small causally disconnected regions, before "stitching" these patches together via recovery maps to obtain a global sample. The efficiency of the first algorithm hinges on the effective 1D process having low entanglement, while the second hinges on the classical output distribution being approximately Markovian in the sense that the conditional mutual information (CMI) decays exponentially quickly with respect to shielded regions.

Results and techniques. We give two classes of results: first, a rigorous proof that `SEBD` is efficient in a specific situation that is hard in the worst case (Theorem 1), and second, numerical and analytical evidence that the runtime of our algorithms is efficient more generally when the circuits are sufficiently shallow, transitioning to inefficient when the qudit local dimension or circuit depth becomes too large.

`SEBD` involves a reduction of the 2D simulation problem to a 1D simulation problem evolving over time. We find that, after performing this reduction, the effective 1D dynamics are highly similar to those of "unitary-and-measurement" processes, which have seen an explosion in interest within the condensed matter physics community in the past few years [6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]. This line of work has found strong evidence that, when random unitary dynamics are interspersed with weak measurements, the 1D dynamics experiences an entanglement phase transition from an area-law to volume-law phase as measurement strength is tuned. We find that, roughly, increasing the depth or the local dimension corresponds to decreasing the measurement strength in this picture, hence the phase transition from an efficient to inefficient regime.

Unfortunately, so far the aforementioned measurement-driven entanglement phase transition has eluded formal proof, and it is similarly hard to formally prove that `SEBD` is generally efficient for random shallow 2D circuits, as the efficiency of `SEBD` hinges on its associated effective 1D dynamics lying in an entanglement

area-law phase. Nonetheless, we are able to formally prove that `SEBD` runs in polynomial time for some special-case 2D architectures for which exact simulation is known (from prior works) to be hard.

Theorem 1 (Informal)**.** *There exists a 2D circuit architecture A defined on n qubits such that, if C_A is the Haar-random circuit family associated with A, under standard hardness conjectures there does not exist a polynomial-time classical algorithm for sampling from the output distribution of arbitrary instances of C_A, or for near-exactly (i.e. up to $e^{-\Omega(n^2)}$ precision) computing output probabilities of typical instances of C_A. However, `SEBD` runs in time $O(n)$ and, with probability $1-2^{-n^{0.99}}$ over choice of circuit instance, samples from the output distribution of C_A up to error at most $2^{-n^{0.99}}$ in total variation distance, and estimates a fixed output probability of C_A with additive error $2^{-n}/2^{n^{0.99}}$.*

While the architecture used to prove this result is contrived, it suffices to demonstrate a formal separation between the hardness of approximately simulating average-case circuits and worst-case simulation. The proof of the above theorem lies partly on a technical lemma on the typical behavior of entanglement after measurement; namely, we show that if a contiguous block of m qubits are measured after applying a random shallow 1D circuit, the expected entanglement entropy of the induced bipartite pure state is exponentially small in m. While this theorem applies for a contrived architecture for which a formal proof is feasible, it is desirable to understand the performance of these simulation algorithms for more general and more natural 2D circuit architectures. To this end, we make conjectures on the general performance of the algorithms, which are summarized informally below.

Conjecture 1 (Informal)**.** *`SEBD` and `Patching` are asymptotically efficient for any family of 2D quantum circuits with Haar-random gates of sufficiently low depth, but experience a computational phase transition to an inefficient (exponential runtime) regime when the depth or local Hilbert space dimension exceeds some (constant) critical value. The critical values are architecture-dependent.*

We collect numerical and heuristic, analytical evidence for these conjectures.

References

[1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. GSL Brandao, D. A. Buell, et al. *Quantum supremacy using a programmable superconducting processor.* Nature, 574(7779):505–510, 2019.

[2] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani. *On the complexity and verification of quantum random circuit sampling.* Nature Physics, 15(2):159, 2019.

[3] R. Movassagh. *Cayley path and quantum computational supremacy: A proof of average-case #p–hardness of random circuit sampling with quantified robustness, 2019.*

[4] G. Vidal. *Efficient simulation of one-dimensional quantum many-body systems.* Physical review letters, 93(4):040502, 2004.

[5] F. Pan, P. Zhou, S. Li, and P. Zhang. *Contracting arbitrary tensor networks: general approximate algorithm and applications in graphical models and quantum circuit simulations,* 2019.

[6] Y. Li, X. Chen, and M. PA Fisher. *Quantum zeno effect and the many-body entanglement transition.* Physical Review B, 98(20):205136, 2018.
[7] A. Chan, R. M. Nandkishore, M. Pretko, and G. Smith. *Weak measurements limit entanglement to area law*, 2018.
[8] B. Skinner, J. Ruhman, and A. Nahum. *Measurement-induced phase transitions in the dynamics of entanglement.* Physical Review X, 9(3):031009, 2019.
[9] Y. Li, X. Chen, and M. Fisher. *Measurement-driven entanglement transition in hybrid quantum circuits*, 2019.
[10] M. Szyniszewski, A. Romito, and H. Schomerus. *Entanglement transition from variable-strength weak measurements,* 2019.
[11] S. Choi, Y. Bao, X.-L. Qi, and E. Altman. *Quantum error correction and entanglement phase transition in random unitary circuits with projective measurements,* 2019.
[12] M. J. Gullans and D. A. Huse. *Dynamical purification phase transition induced by quantum measurements,* 2019.
[13] Y. Bao, S. Choi, and E. Altman. *Theory of the phase transition in random unitary circuits with measurements,* 2019.
[14] C.-M. Jian, Y.-Z. You, R. Vasseur, and A. WW Ludwig. *Measurement-induced criticality in random quantum circuits*, 2019.
[15] M. J. Gullans and D. A. Huse. *Scalable probes of measurement-induced criticality,* 2019.
[16] A. Zabalo, M. J. Gullans, J. H. Wilson, S. Gopalakrishnan, D. A. Huse, and J. H. Pixley. *Critical properties of the measurement-induced transition in random quantum circuits,* 2019.
[17] A. Nahum, S. Vijay, and J. Haah. *Operator spreading in random unitary circuits.* Physical Review X, 8(2):021014, 2018.
[18] CW V. Keyserlingk, T. Rakovszky, F. Pollmann, and S. L. Sondhi. *Operator hydrodynamics, otocs, and entanglement growth in systems without conservation laws.* Physical Review X, 8(2):021013, 2018.
[19] T. Zhou and A. Nahum. *Emergent statistical mechanics of entanglement in random unitary circuits.* Physical Review B, 99(17):174205, 2019.
[20] N. Hunter-Jones. *Unitary designs from statistical mechanics in random quantum circuits,* 2019.

Detecting positive quantum capacities of quantum channels

Nilanjana Datta
(joint work with Satvik Singh)

Using elementary techniques from analytic perturbation theory of Hermitian matrices, we devise a simple strategy to detect positive quantum capacities of quantum channels and their complements. Several noteworthy examples, such as the depolarizing and transpose-depolarizing channels (including the Werner-Holevo channel), dephasing channels, generalized Pauli channels, multi-level amplitude damping channels, and (conjugate) diagonal unitary covariant channels, serve to aptly exhibit the utility of our method. Our main result leads to simplified proofs of certain existing structure theorems for the class of degradable quantum channels, and an extension of their applicability to the larger class of more capable quantum channels.

The platypus of the quantum channel zoo

Debbie Leung
(joint work with Felix Leditzky, Vikesh Siddhu, Graeme Smith, John Smolin)

Quantum channels are astonishing. They are like animals in a zoo each exhibiting some exotic behaviors and unusual interactions with each other. This includes a variety of synergies: super-additivity of coherent information, private information, and Holevo information, superactivation of quantum capacity, and private communication at a rate above the quantum capacity. Over the past two decades, significant effort has been dedicated to elucidating these phenomena with numerous exciting findings, but a full understanding remains elusive. Without such understanding, we lack a theory on how to best communicate with quantum channels, and fail to answer the kinds of questions classical information theory does. Random codes can be suboptimal; we cannot evaluate capacities beyond special examples; our capacities may not capture the communication potential of a noisy channel; our understanding of error correction in the quantum setting is incomplete, whether the data is classical, private, or quantum.

We think the best path towards a deeper understanding of super-additivities in quantum information—really, a better understanding of quantum information itself—is to better understand and develop the menagerie of phenomena. Clean and clear examples of channels that isolate different aspects of nonadditivity are in short supply. This paper presents such an example which is novel in several ways.

Key results. We study a remarkably simple, low-dimensional, single-parameter family of channels $\mathcal{N}_s$ (defined in (1) below). This family exhibits many strange behaviors for quantum communication while having uncomplicated classical and private classical capacities: (i) The classical and private classical capacities can be calculated explicitly because the underlying information quantities (Holevo and private information, respectively) are additive, even though the channel does not belong to any of the known additivity classes. (ii) The same holds true for the quantum capacity: the coherent information of this family is additive, provided that a certain entropy minimization conjecture is true. We state this "spin alignment conjecture" below and give evidence for its validity in the main text. (iii) The coherent information, and also the quantum capacity (assuming the spin alignment conjecture) of $\mathcal{N}_s$ tensored with an assisting channel is super-additive. The phenomenon is exhibited even on simple assisting channels, including the qubit amplitude damping channel, the qubit erasure channel, and the qubit depolarizing channel. Moreover, super-additivity persists even if the assisting channel has positive quantum capacity by itself, which has not been observed before. (iv) The mechanism of super-additivity is novel and in particular differs from the known explanation [1] of super-activation [3]. The vanilla mechanism from prior activation results does not give super-additivity.

Channel definition. This family of quantum channels is first introduced in [2], and is defined by the isometry $F : \mathcal{H}_a \to \mathcal{H}_b \otimes \mathcal{H}_c$ with $\mathcal{H}_a = \mathcal{H}_b = \mathbb{C}^3$ and $\mathcal{H}_c = \mathbb{C}^2$,

$$\begin{aligned} F|0\rangle &= \sqrt{s}\,|0\rangle \otimes |0\rangle + \sqrt{1-s}\,|1\rangle \otimes |1\rangle\,, \\ F|1\rangle &= |2\rangle \otimes |0\rangle\,, \\ F|2\rangle &= |2\rangle \otimes |1\rangle\,, \quad 0 \le s \le 1/2. \end{aligned} \tag{1}$$

This gives rise to a pair of channels $\mathcal{N}_s(\rho) = \mathrm{tr}_c F\rho F^\dagger$, and $\mathcal{N}_s^c(\rho) = \mathrm{tr}_b F\rho F^\dagger$. If one restricts the input to the span of $\{|0\rangle, |1\rangle\}$ or the span of $\{|0\rangle, |2\rangle\}$, one obtains a degradable sub-channel of $\mathcal{N}_s$. Likewise, the span of $\{|1\rangle, |2\rangle\}$ maps perfectly to the output of $\mathcal{N}_s^c$. These two simple modes of transmission are intertwined in F, giving rise to the following long list of exotic properties, some of which are summarized in Figures 1A and 1B below.

- $\mathcal{N}_s$ is neither degradable nor antidegradable, yet its private information is additive and the private capacity can be computed exactly: $\mathcal{P}(\mathcal{N}_s) = 1$.
- Subject to the spin-alignment conjecture, the coherent information is additive and the quantum capacity can be computed exactly.
- The quantum capacity of $\mathcal{N}_s$ can be upper-bounded (unconditionally) as $\mathcal{Q}(\mathcal{N}_s) \le \log(1 + \sqrt{1-s})$. Thus the quantum and private capacity of $\mathcal{N}_s$ are provably separated; see also Fig. 1 below), yet both capacities are additive (modulo the spin alignment conjecture for quantum capacity).
- $\mathcal{N}_s$ does not belong to any of the known additivity classes for Holevo information (unital qubit channels, entanglement-breaking channels, Hadamard channels, depolarizing channels, direct sum of partial trace channels), yet its Holevo information is additive and the classical capacity can be computed exactly: $\mathcal{C}(\mathcal{N}_s) = 1$.
- In summary, the private and classical capacity of $\mathcal{N}_s$ coincide, while the quantum capacity of $\mathcal{N}_s$ is different. Furthermore, the complementary channel $\mathcal{N}_s^c$ has all capacities equal to 1.
- Both the private and classical capacity of $\mathcal{N}_s$ have the strong converse property, establishing the respective capacity as a sharp threshold beyond which any private or classical information transmission fails with certainty. The channel is not a member of any of the known classes of channels for which strong converses (for either private capacity or classical capacity) are known.
- The coherent information of $\mathcal{N}_s$ is strictly super-additive when used with many familiar simple channels such as the qubit amplitude damping channel, $\mathcal{A}_p$, the qubit erasure channel, $\mathcal{E}_\lambda$, and the qubit depolarizing channel, $\mathcal{D}_p$. See Fig. 1 for an overview.

- Subject to the spin-alignment conjecture, the strict super-additivity of $\mathcal{Q}^{(1)}(\mathcal{N}_s \otimes \mathcal{M})$ for $\mathcal{M} = \mathcal{A}_p, \mathcal{E}_\lambda$ is lifted to the quantum capacities, and here, both constituent channels have large, positive quantum capacities. The super-additivity of coherent information for all three assisting channels (and superadditivity of quantum capacity for $\mathcal{M} = \mathcal{A}_p, \mathcal{E}_\lambda$) is achieved on a joint input state having the same form. Thus, in all three cases the same mechanism lies at the heart of the observed super-additivity effects.
- This "mechanism" of super-additivity is distinct from those in prior (super-) activation of quantum capacities. Smith and Yard [2] showed that a 50% erasure channel can transform private capacity into quantum capacity at the cost of a factor of 1/2, via an attempted conversion of a p-bit (state with secret key) into entanglement, which succeeds with probability 1/2. This superactivates the quantum capacity of any channel with no quantum capacity but positive private capacity. But for the channel $\mathcal{N}_s$, even though the private capacity is much bigger than the quantum capacity, we have $\mathcal{Q}(\mathcal{N}_s) > \frac{1}{2}\mathcal{P}(\mathcal{N}_s)$. Therefore, the Smith-Yard protocol cannot increase the capacity. We may expect that the coherent information is optimized on an input that is independent across the erasure channel and $\mathcal{N}_s$, giving additive coherent information. Instead, superposing the Smith and Yard strategy with the product strategy while retaining a coherent memory of which strategy was used provides the observed super-additivity!

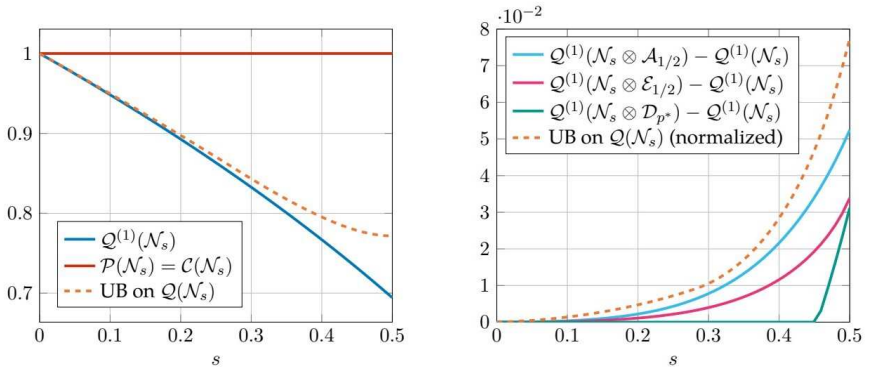
Spin alignment conjecture. We now provide a short description of a conjecture about the entropy of spins. Subject to this conjecture, $\mathcal{Q}^{(1)}(\mathcal{N}_s) = \mathcal{Q}(\mathcal{N}_s)$. First, consider a single spin-1/2 particle whose density operator ρ is a convex combination of a given mixed state Q and some variable state ω. The minimum entropy of ρ can be shown to occur at $\omega = |\phi\rangle\langle\phi|$, where $|\phi\rangle$ is an eigenvector of Q corresponding to the largest eigenvalue. The spin-alignment conjecture generalizes the aforementioned setup: ρ is now allowed to be an n-spin density operator that is formed by a convex combination of several distinct states. In each distinct n-spin state, a subset of the spins are fixed to be products of the mixed state Q, and the rest of the spins are in some variable joint state. The spin-alignment conjecture posits that ρ has minimum entropy when spins in all these variable states align with each other making each variable state a product over the same spin state $|\phi\rangle$. We prove this conjecture in certain special cases with $n = 2$ and 3. For modest values of n we find numerical evidence supporting this conjecture.

References

[1] J. Oppenheim. *For quantum information, two wrongs can make a right.* Science 321.5897 (2008), 1783–1784. arXiv: 1004.0052.

[2] G. Smith and J. Yard. *Quantum communication with zero-capacity channels.* Science 321.5897 (2008), pp. 1812–1815. arXiv: 0807.4935.

[3] V. Siddhu. *Leaking information to gain entanglement.* arXiv: 2011.15116.



(A) (B)

FIGURE 1. (A) Capacities of the qutrit channel $\mathcal{N}_s$. (B) Superadditivity of coherent information of $\mathcal{N}_s$

Hybrid quantum-classical algorithms for approximate graph coloring

ROBERT KÖNIG

(joint work with Sergey Bravyi, Alexander Kliesch, Eugene Tang)

There is a growing demand for practical algorithms solving combinatorial optimization problems which are challenging for classical computers. An example of such a problem is the graph coloring problem, which tends to be NP-complete even when restricted to special sub-classes of graphs. An approximate version of the graph coloring problem is the MAX-k-CUT problem, which seeks to find an approximate vertex coloring of a graph using k colors such that the number of miscolored edges is minimized. This problem generalizes the standard MAX-CUT problem (which is equivalent to MAX-2-CUT). A well-studied quantum algorithm for MAX-CUT is the Quantum Approximate Optimization Algorithm (QAOA) [1].

In this work, we first formulate a variation of QAOA using (k-dimensional) qudits which is applicable to the MAX-k-CUT problem. Given a graph $G = (V, E)$, define the (classical) 2-local cost Hamiltonian on $n = |V|$ k-dimensional qudits as follows:

$$(1) \qquad H = \sum_{(i,j)\in E} \sum_{b\in\mathbb{Z}_k\setminus\{0\}} \Pi_{i,j}(b) \qquad \text{where} \qquad \Pi(b) = \sum_{a\in\mathbb{Z}_k} |a, a+b\rangle\langle a, a+b| \ .$$

Maximum energy states of H have support on computational basis states associated with optimal approximate k-colorings. The level-p QAOA (denoted QAOA_p) uses variational states of the form

$$(2) \quad |\psi(\beta,\gamma)\rangle = \prod_{t=1}^{p} B(\beta_t)^{\otimes n} e^{i\gamma_t H} |+\rangle^{\otimes n} \qquad \text{with angles} \qquad (\beta,\gamma) \in (\mathbb{R}^k)^p \times \mathbb{R}^p$$

where $|+\rangle = k^{-1/2} \sum_{b\in\mathbb{Z}_k} |k\rangle$, $B(\boldsymbol{\beta}) = \sum_{\alpha\in\mathbb{Z}_k} e^{i\boldsymbol{\beta}_a} |\phi_a\rangle\langle\phi_a|$, and where $|\phi_a\rangle = Z^a |+\rangle$, $Z = \sum_{b\in\mathbb{Z}_k} e^{2\pi i b/k} |b\rangle\langle b|$ are the eigenvectors of the generalized Pauli operator X. As usual, angles (β, γ) maximizing $\langle\psi(\beta,\gamma)| H |\psi(\beta,\gamma)\rangle$ are found using some (classical) iterative procedure such as gradient descent (by querying the quantum device); a corresponding state $|\psi(\beta,\gamma)\rangle$ is subsequently measured in the computational basis to obtain an approximate k-coloring $z \in \mathbb{Z}_k^n$. The approximation ratio achieved by QAOA$_p$ (i.e., the expected number of properly colored edges divided by the maximal number $\mathrm{MC}_k(G)$ of properly colored edges in an k-coloring) is then given by $\alpha_p^{\mathrm{MC}_k}(G) = \max_{\beta,\gamma} \langle\psi(\beta,\gamma)| H |\psi(\beta,\gamma)\rangle / \mathrm{MC}_k(G)$.

Main findings. Here we seek to study the power of this modified QAOA applied to MAX-k-CUT as compared to the best known efficient classical algorithms. We first establish analytical bounds pinpointing limitations of QAOA as described here: similar to earlier observations about QAOA for MAX-CUT, the proposed algorithm suffers from locality constraints and its uniformity. Prompted by this, we introduce a modification of QAOA which supplements the basic energy minimization routine by efficient classical processing. The latter sidesteps the locality constraints inherent in near-term quantum hardware. We find numerically that this modification which we call recursive QAOA (RQAOA), substantially improves upon the results of standard QAOA. In fact, it is shown to outperform the best known classical algorithms for the MAX-k-CUT problems on generic random instances.

Limitations of QAOA$_p$ for MAX-k-CUT. While it is known that QAOA asymptotically provides optimal solutions, it is important for the imminent NISQ era to understand its behavior for low levels p (corresponding to few variational parameters). In [2], we showed that for levels $p = O(\log n)$, one can always find examples for which QAOA for the MAX-CUT problem is outperformed by the best known classical algorithm, the Goemans-Williamson algorithm [3]. This result was further improved by Farhi et al. [4], where they demonstrate a class of graphs for which constant-level QAOA is incapable of beating the most trivial algorithm which randomly assigns each vertex to one of the two sets in the desired bipartition. We show that a similar kind of restriction also holds for the MAX-k-CUT problem:

Theorem 1. *Let $\mathcal{G}_{n,d}^{bi}$ denote the uniform distribution over all d-regular bipartite graphs on n vertices. Let $\alpha_p^{\mathrm{MC}_k}(G)$ denote the approximation ratio achieved by QAOA$_p$ for MAX-k-CUT on the graph G. There is a constant $\zeta > 0$ such that*

$$\Pr_{G\sim\mathcal{G}_{n,d}^{bi}} \left[\alpha_p^{\mathrm{MC}_k}(G) \geq (1 - 1/k) + o_d(1) + o_n(1)\right] \leq o(1) \tag{3}$$

for all degrees d satisfying $d \geq \zeta$ and $d = o(\sqrt{n})$ and all levels $p < \frac{1}{2}\log_d n$.

Theorem 1 states that, roughly speaking, for random d-regular bipartite graphs of sufficiently large degree d, the performance of constant (or even logarithmic) depth QAOA$_p$ is asymptotically equivalent to the naive algorithm of assigning

each vertex to a random partition. This result therefore generalizes the corresponding bound for MAX-CUT derived in [4]. The proof of Theorem 1 relies on two key characteristics of QAOA, namely its locality and uniformity. The QAOA unitary is a local quantum circuit: for a constant level p, each interaction term $\langle\psi(\beta,\gamma)|\Pi_{i,j}|\psi(\beta,\gamma)\rangle$ involves only a neighborhood of radius p around each given edge (i,j). Moreover, the algorithm is spatially uniform: reduced density operators for isomorphic neighborhoods are identical and thus contribute the same amount of energy. A random d-regular graph has the property that almost all of its local neighborhoods are isomorphic, which implies strong concentration properties for the resulting QAOA expectation values.

Sidestepping locality constraints: RQAOA. To sidestep the locality constraints facing QAOA, we consider a recursive modification of the algorithm which we call *recursive QAOA* (RQAOA). RQAOA utilizes additional classical processing in the form of correlation rounding. The correlation rounding step amplifies the results of low-level QAOA, taking full advantage of both the budding quantum hardware and the powerful existing classical architecture. RQAOA mitigates the problematic limitations of QAOA by allowing the coupling of non-local degrees of freedom through the correlation rounding step.

Formally, RQAOA (which we previously discussed for MAX-CUT in [2]) proceeds as follows. First, run the standard QAOA to maximize the expected value of the cost function Hamiltonian H defined in equation (1). For $i,j \in [n]$, define $M_{i,j}(b)$ as the expectation value of $\Pi_{i,j}(b)$ on the optimal state. Next, find a pair (i^*,j^*) of vertices and a color $b^* \in \mathbb{Z}_k$ such that the value of $M_{i^*,j^*}(b^*)$ is maximal (breaking ties arbitrarily). Then impose the constraint $x_{j^*} = x_{i^*} + b^* \pmod k$, restricting the search space to the span of computational basis vectors $|x\rangle$ which satisfy the constraint. Now, we eliminate the variable x_{i^*} by inserting the constraint into the cost function Hamiltonian. To do so, we use the identity $\Pi_{i,j}(b)\Pi_{j,h}(a-b) = \Pi_{i,j}(b)\Pi_{i,h}(a)$ which holds for all $h \notin \{i,j\}$ and all $a \in \mathbb{Z}_k$. Thus we have $\Pi_{i^*,h}(a) = \Pi_{j^*,h}(a-b^*)$ on the subspace satisfying the constraint. Replacing $\Pi_{i^*,h}(a)$ by $\Pi_{j^*,h}(a-b^*)$ in the cost function Hamiltonian for all $h \notin \{i^*,j^*\}$, we get a new Hamiltonian H' of the form (1) (possibly with additional edge weights) which acts on $n-1$ variables. We can now run standard QAOA again on the reduced Hamiltonian H', iterating the process above until we reduce the problem to a size which is amenable to a straightforward computation (such as a brute-force search).

Efficient classical simulation of $\mathbf{QAOA_1}$ and $\mathbf{RQAOA_1}$. To numerically assess the performance of RQAOA, we require classical simulation algorithms. For MAX-CUT, an analytic expression for QAOA_1 expectation values is known, permitting efficient classical evaluation [5, 2]. We show that for MAX-k-CUT, QAOA_1 expectation values can also be efficiently computed:

Theorem 2 (Classical Simulation of level-1 QAOA for MAX-k-CUT)**.** *For any $i,j \in [n]$, $b \in \mathbb{Z}_k$ and $(\beta,\gamma) \in \mathbb{R}^k \times \mathbb{R}$, the $QAOA_1$-correlation function*

$$\langle\psi(\beta,\gamma)|\,\Pi_{i,j}(b)\,|\psi(\beta,\gamma)\rangle$$

can be classically computed in time $O(k^6(d_i+d_j))$, where d_i and d_j are the degrees of vertices i and j, respectively.

For a constant number of colors k, this scales at most linearly with n. For constant-degree graphs, the computation requires a constant amount of time. Our simulation algorithm works more generally for Hamiltonians $H = \sum_{i,j} H_{i,j}$ with pairwise commuting 2-local interaction terms $\{H_{i,j}\}_{i<j}$ and QAOA_1-type ansatz states defined using any tensor product operator as the driving term. The algorithm relies on the fact that by commutativity of the interaction terms, the evaluation of expectation values can be reduced to the iterative application of superoperators $\mathcal{E}_w$ for every $w \in V \setminus \{i,j\}$ to the density matrix $\eta = e^{i\gamma H_{i,j}}|+\rangle\langle+|^{\otimes n}e^{-i\gamma H_{i,j}}$. For MAX-$k$-CUT, $\mathcal{E}_w$ admits diagonal Kraus operators which allows for an efficient evaluation. This results in the stated complexity for QAOA_1.

Through the efficient evaluation of correlation functions, Theorem 2 also immediately implies an efficient simulation method for RQAOA_1. Therefore, RQAOA at level 1 is itself an instance of an efficient classical algorithm for MAX-k-CUT. Conversely, the efficient classical simulation of RQAOA_1 allows a crucial window into the algorithm's performance, allowing key comparisons to well known classical algorithms. Corresponding simulation results are indicative for the potential performance of RQAOA at larger ("genuinely quantum") levels p.

Numerical performance of RQAOA for MAX-3-CUT. Here we present numerical results comparing the performance of QAOA_1, RQAOA_1, and the best known, very recently discovered classical algorithm by Newman [6] for MAX-3-CUT. The latter is a simplification of the previous algorithms by Klerk et al. [7] and Goemans and Williamson [8] based on randomized rounding of SDP solutions.

To this end, we randomly generated d-regular, 3-colorable graphs with n vertices for several values of d and n. For QAOA_1 and RQAOA_1, we employ a suitable parametrization allowing to find optimal angles using a 1-dimensional grid search instead of the notoriously problematic gradient descent. Since Newman's algorithm is randomized, we run the algorithm 100 (i.e., a constant number of) times and take the best result over these samples as the benchmark for our comparisons.

A selection of our numerical results is illustrated in Fig. 1. We observe that RQAOA_1 significantly outperforms QAOA_1 for MAX-3-CUT in all considered cases. We also note that RQAOA_1 is highly competitive with Newman's algorithm, although this statement needs to be qualified.

For certain parameter values of (n,d) (e.g., for small graphs), we observe that Newman's algorithm produces a distribution of approximation ratios with large variance. This in turn implies that the optimal solution (over 100 samples) returned by Newman's algorithm tends to provide a good coloring. For such graphs, RQAOA_1 is outperformed by this best solution, yet still provides a coloring better than what Newman's algorithm produces on average. For other parameter values (including cases where the size of the graphs is larger), the variance of Newman's algorithm is smaller, and the empirical average is close to theoretically guaranteed worst-case approximation ratio. For these instances, we observe that RQAOA_1 outperforms all solutions returned by Newman's algorithm. This suggests that

RQAOA may be a promising algorithm for problem sizes of real practical relevance.

Outlook. Our quantum-classical hybrid algorithm studied here provides concrete evidence that limitations of near-term quantum devices can be overcome by the inclusion of classical processing. Especially in the resource limited NISQ era, further analytical understanding of both QAOA and RQAOA is an important open problem.

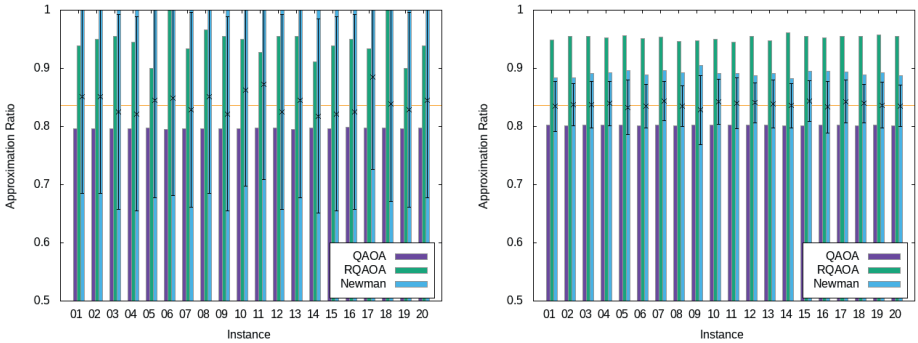


FIGURE 1. Approximation ratios for $(n, d) = (60, 6)$ (left) and $(300, 6)$ (right), respectively. The guaranteed worst-case approximation ratio of Newman's algorithm is indicated by the horizontal line at $\alpha = 0.836008$. For each graph, the empirical mean and standard deviation of Newman's algorithm are indicated through the error bars.

REFERENCES

[1] E. Farhi, J. Goldstone, and S. Gutmann. *A Quantum Approximate Optimization Algorithm,* arXiv:1411.4028.

[2] S. Bravyi, A. Kliesch, R. König, and E. Tang. *Obstacles to Variational Quantum Optimization from Symmetry Protection.* Phys. Rev. Lett., 125:260505, Dec 2020.

[3] M. X. Goemans and D. P. Williamson. *Improved Approximation Algorithms for Maximum Cut and Satisfiability Problems Using Semidefinite Programming.* J. ACM, 42(6):1115–1145, 1995.

[4] E. Farhi, D. Gamarnik, and S. Gutmann. *The Quantum Approximate Optimization Algorithm Needs to See the Whole Graph: Worst Case Examples,* arXiv:2005.08747.

[5] Z. Wang, Stuart Hadfield, Z. Jiang, and E. G. Rieffel. *Quantum approximate optimization algorithm for MaxCut: A fermionic view.* Phys. Rev. A, 97:022304, Feb 2018.

[6] A. Newman. *Complex Semidefinite Programming and Max-k-Cut.* In 1st Symposium on Simplicity in Algorithms (SOSA 2018), volume 61 of OpenAccess Series in Informatics (OASIcs), pages 13:1–13:11, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[7] E. Klerk, D. Pasechnik, and J.P. Warners. *On Approximate Graph Colouring and MAX-k-CUT algorithms based on the ϑ-function.* Journal of Combinatorial Optimization, 8:267–294, 09 2004.

[8] M. X. Goemans and D. P. Williamson. Approximation Algorithms for MAX-3-CUT and Other Problems via Complex Semidefinite Programming. *Journal of Computer and System Sciences*, 68(2):442–470, 2004. Special Issue on STOC 2001.

Quantum algorithms for matrix scaling

Harold Nieuwboer
(joint work with Joran van Apeldoorn, Sander Gribling, Yinan Li, Michael Walter, Ronald de Wolf)

Matrix scaling is an easily stated computational task: given a matrix with non-negative entries, rescale its rows and columns with positive numbers such that the new matrix has prescribed row and column sums. Despite its simple statement, it has applications in many different contexts, such as approximation of the permanent [14], fast approximation of optimal transport distances in machine learning [11], and finding maximum-likelihood estimators for log-linear models [6]. A related problem with similar structure is that of matrix balancing, which is used in practice for numerical preconditioning, and can be used to approximate min-mean-cycles in weighted graphs [3]. Furthermore, there has been a lot of recent interest in (non-commutative) generalizations of matrix scaling, such as operator and tensor scaling [12, 8]. The matrix scaling and balancing problems are well-understood and efficiently solvable with classical algorithms. In this talk, we discuss two recent works [4, 13] on both quantum algorithms and quantum lower bounds for matrix scaling and balancing.

For $\boldsymbol{A} \in \mathbb{R}_{\geq 0}^{n\times n}$, let $\vec{r}(\boldsymbol{A}) := \boldsymbol{A}\vec{1}_n$ and $\vec{c}(\boldsymbol{A}) := \boldsymbol{A}^T\vec{1}_n$ be its vectors of row and column sums, respectively. The matrix scaling problem is then defined as follows for the ℓ_p-norm ($p \geq 1$): given $\varepsilon > 0$, and $\vec{r}, \vec{c} \in \mathbb{R}_{\geq 0}^n$ with $\|\vec{r}\|_1 = \|\vec{c}\|_1 = 1$, find positive diagonal matrices $\boldsymbol{X}, \boldsymbol{Y}$ such that $\boldsymbol{B} = \boldsymbol{X}\boldsymbol{A}\boldsymbol{Y}$ satisfies $\|\vec{r}(\boldsymbol{B}) - \vec{r}\|_p \leq \varepsilon$ and $\|\vec{c}(\boldsymbol{B}) - \vec{c}\|_p \leq \varepsilon$. We refer to such a $\boldsymbol{B}$ as being ε-$(\vec{r}, \vec{c})$-scaled. A common choice for $\vec{r}, \vec{c}$ is $\vec{1}_n/n$, i.e., the uniform distribution, and we refer to these as the uniform target marginals. We assume henceforth that the smallest non-zero entry of each of $\boldsymbol{A}$, $\vec{r}$ and $\vec{c}$ is at least $1/\mathrm{poly}(n)$, and we write m for the number of (possibly) non-zero entries of $\boldsymbol{A}$.

While achieving both $\vec{r}(\boldsymbol{X}\boldsymbol{A}\boldsymbol{Y}) \approx_\varepsilon \vec{r}$ and $\vec{c}(\boldsymbol{X}\boldsymbol{A}\boldsymbol{Y}) \approx_\varepsilon \vec{c}$ simultaneously is difficult, satisfying one of the constraints at a time is easy; if $\boldsymbol{X}\boldsymbol{A}\boldsymbol{Y}$ is the current matrix, then to satisfy the row-marginal constraint, one can update $\boldsymbol{X}$ to $\boldsymbol{X}'$ by setting $X_i' = X_i \cdot r_i/r_i(\boldsymbol{X}\boldsymbol{A}\boldsymbol{Y})$. Alternating between updating $\boldsymbol{X}$ and $\boldsymbol{Y}$ is known as Sinkhorn's algorithm, and surprisingly, this algorithm converges whenever $\boldsymbol{A}$ is *asymptotically* $(\vec{r}, \vec{c})$*-scalable*, that is, for every $\varepsilon > 0$ there exist $\boldsymbol{X}, \boldsymbol{Y}$ such that $\boldsymbol{X}\boldsymbol{A}\boldsymbol{Y}$ is ε-$(\vec{r}, \vec{c})$-scaled. We assume that this holds from here onwards.

It is known that if one computes the $r_i(\boldsymbol{X}\boldsymbol{A}\boldsymbol{Y})$ exactly, then Sinkhorn's algorithm outputs an ε-ℓ_1-scaling of $\boldsymbol{A}$ in $\widetilde{O}\big(1/\varepsilon^2\big)$ iterations (cf. [2, 9, 4]). This can

be proven by considering the (convex) potential function

$$f(\vec{x},\vec{y}) = \sum_{i,j=1}^{n} A_{ij} e^{x_i+y_j} - \langle \vec{r},\vec{x}\rangle - \langle \vec{c},\vec{y}\rangle$$

where $\vec{x} = \log(\boldsymbol{X})$ and $\vec{y} = \log(\boldsymbol{Y})$, showing that it decreases by roughly ε^2 as long as $\boldsymbol{XAY}$ is not ε-ℓ_1-scaled, and showing that the potential gap $f(\vec{0},\vec{0}) - \inf_{\vec{x},\vec{y}} f(\vec{x},\vec{y})$ is not too large. The cost of every iteration is given by the cost of computing the row (or column) sums of the current matrix, which can be done in time $\widetilde{O}(m)$; hence a classical implementation of Sinkhorn's algorithm finds an ε-ℓ_1 scaling in time $\widetilde{O}\big(m/\varepsilon^2\big)$. When $\boldsymbol{A}$ is entrywise positive, one can show $\widetilde{O}(1/\varepsilon)$ iterations suffice, thus finding scalings in time $\widetilde{O}\big(n^2/\varepsilon\big)$.

However, if one has quantum (binary) oracle access to $\boldsymbol{A}$, then we show that one can use quantum amplitude estimation [7] to compute $(1\pm\delta)$-multiplicative approximations to the $r_i(\boldsymbol{XAY})$ in time $\widetilde{O}(\sqrt{n}/\delta)$ per row, and use these approximations for updating the $\boldsymbol{X},\boldsymbol{Y}$. The choice $\delta = O(\varepsilon^2)$ only increases the number of required iterations by a constant factor (compared to the classical setting), leading to a quantum algorithm finding ε-ℓ_1-scalings of $\boldsymbol{A}$ in quantum time $\widetilde{O}\big(\sqrt{mn}/\varepsilon^4\big)$ when $\boldsymbol{A}$ has at most m non-zero entries. If $\boldsymbol{A}$ is entrywise positive, one can reduce this to $\widetilde{O}\big(n^{1.5}/\varepsilon^3\big)$, in analogy with the classical setting. Furthermore, the quantum Sinkhorn method can be shown to be optimal (up to logarithmic factors) for constant ε, in the following sense: there exists an $\varepsilon_0 > 0$ such that any quantum algorithm that ε_0-ℓ_1-scales dense matrices to uniform marginals with probability $\geq 2/3$ must make $\Omega(n^{1.5})$ queries.

Among the classical state-of-the-art are second-order methods which have a polylogarithmic $1/\varepsilon$ dependence, namely box-constrained Newton methods [10, 1] and interior-point methods [10]. These rely on efficient graph sparsification algorithms, for which a quantum speedup was recently obtained [5]. We use this to obtain a quantum speedup for the second-order methods in terms of n, m, but the resulting algorithm still has a polynomial $1/\varepsilon$ dependence; see [13] for details.

This leads to the question as to whether a polylogarithmic $1/\varepsilon$ dependence can be preserved while obtaining a sublinear dependence on the input size m. We show that this is impossible: we prove that for $\varepsilon = \widetilde{\Theta}(1/m)$, any quantum algorithm which ε-ℓ_2-scales matrices with at most m non-zero entries to uniform marginals must make $\widetilde{\Omega}(m)$ queries to the matrix entries, even when the success probability is only assumed to be $\geq \frac{3}{2}\exp(-n/100)$. This lower bound is proven by a reduction from determining the Hamming weight of bit strings of length n, each of which is assumed to have Hamming weight $n/2\pm 1$, for which a $\Omega(n^2)$ quantum query lower bound holds. From (random permutations of) the bit strings one then creates a matrix $\boldsymbol{A}$ such that the row sums are determined by the Hamming weights; hence the scaling factors $\boldsymbol{X}$ obtained from a single row-rescaling step encode the Hamming weight of each bit string. Using a concentration argument, one can show that $\boldsymbol{XA}$ is $\widetilde{\Theta}(1/m)$-scaled with probability $\geq 2/3$ (over the random permutations), and strong convexity properties of the potential f discussed earlier

imply that any other scaling factors which ε-ℓ_2-scale the matrix for $\varepsilon = \widetilde{\Theta}(1/m)$ also encode the Hamming weights of the bit strings.

However, some open problems remain. For general matrices, the interior-point method of [10] has the best guarantees in the high-precision regime, finding an ε-ℓ_1-scaling in time $\widetilde{O}\big(m^{1.5}\big)$; a natural question is whether this can be reduced with a quantum algorithm while retaining the polylogarithmic $1/\varepsilon$-dependence. Another interesting problem is determining the complexity of the following task: given a dense non-negative matrix $\boldsymbol{A}$ whose entries sum to at most 1, find an ε-ℓ_1-approximation of $\vec{r}(\boldsymbol{A})$. An upper bound of $\widetilde{O}\big(n^{1.5}/\varepsilon\big)$ can be given using amplitude estimation. One can also prove lower bounds of $\Omega(n^{1.5})$ when ε is a small enough constant, and $\Omega(n/\varepsilon)$ when $\varepsilon = \Omega(1/n)$ [13], so there remains a gap between the lower and upper bounds.

References

[1] Z. Allen-Zhu, Y. Li, R. Oliveira, and A. Wigderson. *Much faster algorithms for matrix scaling.* In Proceedings of IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS'17), pages 890–901, 2017. arXiv:1704.02315.

[2] J. Altschuler, J. Niles-Weed, and P. Rigollet. *Near-linear time approximation algorithms for optimal transport via Sinkhorn iteration.* In Advances in Neural Information Processing Systems, volume 30, pages 1964–1974, 2017.

[3] J. M. Altschuler and P. A. Parrilo. *Approximating Min-Mean-Cycle for low-diameter graphs in near-optimal time and memory,* arXiv:2004.03114.

[4] J. van Apeldoorn, S. Gribling, Y. Li, H. Nieuwboer, M. Walter, and R. de Wolf. *Quantum Algorithms for Matrix Scaling and Matrix Balancing.* In 48th International Colloquium on Automata, Languages, and Programming (ICALP 2021), volume 198, pages 110:1–110:17, 2021. arXiv:2011.12823.

[5] S. Apers and R. de Wolf. *Quantum speedup for graph sparsification, cut approximation and laplacian solving.* Proceedings of IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS'20), pages 637–648, 2020. arXiv:1911.07306.

[6] Y. M. M. Bishop, S. E. Fienberg, and P. W. Holland. *Discrete Multivariate Analysis: Theory and Practice.* MIT Press, 1975.

[7] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. *Quantum amplitude amplification and estimation.* In Quantum Computation and Quantum Information: A Millennium Volume, volume 305 of Contemporary Mathematics, pages 53–74. American Mathematical Society, 2002. arXiv:quant-ph/0005055.

[8] P. Bürgisser, C. Franks, A. Garg, R. Oliveira, M. Walter, and A. Wigderson. *Towards a theory of non-commutative optimization: geodesic 1st and 2nd order methods for moment maps and polytopes.* In Proceedings of 60th IEEE Annual Symposium on Foundations of Computer Science (FOCS'19), pages 845–861. IEEE, 2019. arXiv:1910.12375.

[9] D. Chakrabarty and S. Khanna. *Better and simpler error analysis of the Sinkhorn–Knopp algorithm for matrix scaling.* Mathematical Programming, pages 1–13, 2020.

[10] M. B. Cohen, A. Madry, D. Tsipras, and A. Vladu. *Matrix scaling and balancing via box constrained Newton's method and interior point methods.* In Proceedings of IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS'17), pages 902–913, 2017.

[11] M. Cuturi. *Sinkhorn distances: Lightspeed computation of optimal transport.* In Advances in Neural Information Processing Systems, volume 26, pages 2292–2300, 2013.

[12] A. Garg, L. Gurvits, R. Oliveira, and A. Wigderson. *Operator scaling: theory and applications.* Foundations of Computational Mathematics, pages 1–68, 2019. Earlier version in FOCS'16.

[13] S. Gribling and H. Nieuwboer. *Improved quantum lower and upper bounds for matrix scaling,* arXiv:2109.15282.
[14] N. Linial, A. Samorodnitsky, and A. Wigderson. *A deterministic strongly polynomial algorithm for matrix scaling and approximate permanents.* Combinatorica, 20(4):545–568, 2000.

Graph Homomorphisms and Obstructions to Sums of Squares

Grigoriy Blekherman
(joint work with Annie Raymond, Mohit Singh, Rekha Thomas)

A graph G has vertex set $V(G)$ and edge set $E(G)$. All graphs are assumed to be simple, without loops or multiple edges. The *homomorphism density* of a graph H in a graph G, denoted by $t(H;G)$, is the probability that a random map from $V(H)$ to $V(G)$ is a graph homomorphism, i.e., it maps every edge of H to an edge of G. An inequality between homomorphism densities refers to an inequality between $t(H_i;G)$, for some finite graphs H_i, that is valid for all graphs G.

The *graph profile* of a collection of connected graphs $\mathcal{U} = \{C_1, \dots, C_s\}$, denoted as $\mathcal{G}_\mathcal{U}$, is the closure of the set of all vectors $(t(C_1;G), t(C_2;G), \dots, t(C_s;G))$ as G varies over all graphs. For example, the graph profile of $\mathcal{U} = \{\text{edge, triangle}\}$ is the well-known set in $[0,1]^2$ shown in Figure 1 [17].

Figure 1. The graph profile of edge and triangle.

Graph profiles are extremely complicated sets and they have been fully understood in very few cases. The study of graph profiles was initiated in [7], where it was shown that a graph profile is a closed full-dimensional subset of $[0,1]^s$ for an arbitrary s-tuple of connected graphs. However to this day, there is no triple of connected graphs for which the graph profile is fully known. For pairs of graphs, the profile $\mathcal{G}_\mathcal{U}$ for $\mathcal{U} = \{\text{edge}, K_n\}$ where K_n denotes the complete graph on n vertices was determined first for $n = 3$ in [17], for $n = 4$ in [15], and for a general n in [19]. Determining the profile of $\{\text{edge}, H\}$ where H is an arbitrary bipartite graph would involve resolving the famous *Sidorenko conjecture* which says

$t(H;G) \geq t(\text{edge};G)^{|E(H)|}$. Despite considerable attention, this conjecture is only known for some classes of bipartite graphs [5, 11, 20, 6].

Completely understanding a graph profile is equivalent to understanding polynomial inequalities valid on it. Many results and problems in extremal graph theory can be restated as polynomial inequalities between homomorphism densities [12, 16]. The Cauchy-Schwarz inequality has been one of the powerful tools used to verify density inequalities for graphs and hypergraphs [8, 12, 18, 9]. This proof method is equivalent to the general sum of squares (sos) proof method that has been widely used in optimization [1]. Moreover, sos proofs naturally yield to a computerized search via semidefinite programming. Nonnegative graph combinations admit a *Positivstellensatz*: any graph combination strictly positive on a graph profile $\mathcal{G}_{\mathcal{U}}$ is a sos [13, 14].

Hatami and Norine [10] show significant computational limitations on verifying inequalities between homomorphism densities. Firstly, they show that the problem of verifying the validity of an inequality between homomorphism densities is undecidable. This implies that there exist valid polynomial inequalities that cannot be certified even via rational sums of squares. We showed in [2] that natural combinatorial inequalities such as *Blakley-Roy inequalities*, $P_k \geq \text{edge}^k$, where P_k is a path of odd length k, cannot be certified by sos. We now show a much stronger obstruction to sums of squares.

In [3] we introduced a new notion of *sos-testable* graph combinations, which are more general than sums of squares and rational sums of squares. Roughly speaking, sos-testable graph combinations correspond to graph combinations whose nonnegativity can be recognized by sums of squares, although there is no explicit certificate of nonnegativity. More precise definition will be given below. We found large families of pure binomial graph density inequalities that are not sos-testable, and even their pure binomial approximations remain not sos-testable. These families include Blakley-Roy inequalities for odd paths.

We focus on *pure binomial inequalities*, i.e. inequalities of the form $G_1^{\alpha} \cdots G_k^{\alpha_k} \geq H_1^{\beta_1} \cdots H_m^{\beta_m}$. For a fixed graph collection $\mathcal{U}$, the exponent vectors of valid binomial inequalities form *a convex cone*. It is not not known whether deciding validity of a pure binomial inequality is undecidable.

Question 1. *Given two (not necessarily connected) graphs G_1 and G_2 is the question of whether $G_1 - G_2 \geq 0$ is a valid homomorphism density inequality decidable?*

In all of the examples we were able to do in [3] and [4] the cone of exponents of valid binomial inequalities is *rational polyhedral*, i.e. all binomial inequalities valid on $\mathcal{U}$ can be deduced from a finite collection of inequalities with integer exponents. The most general result we have is the following [4]:

Theorem 1. *Let $\mathcal{U}$ be a finite collection of connected, chordal, series-parallel graphs. Then exponents of binomial inequalities valid on the profile $\mathcal{G}_{\mathcal{U}}$ form a rational polyhedral cone.*

We ask whether this is true for an arbitrary finite collection of connected graphs:

Question 2. *Let $\mathcal{U}$ be a finite collection of connected graphs. Do exponents of binomial inequalities valid on the profile $\mathcal{G}_{\mathcal{U}}$ form a polyhedral cone. If yes, then is it necessarily a rational polyhedral cone?*

Sos profiles and sos-testable functions.
For a fixed positive integer d, define the *d-sos-profile*, denoted as $\mathcal{S}_d$, to be the set of all points on which all sos graph combinations $\sum[[a_j^2]]$, with all a_j having at most d edges in their constituent graphs, are nonnegative. Let the $(\mathcal{U}, d)$-sos profile $\mathcal{S}_{\mathcal{U},d}$ be the projection on $\mathcal{S}_d$ onto the graphs in $\mathcal{U}$. We proved in [3] that $\mathcal{S}_d$ is a basic, closed semialgebraic set, and all valid pure binomial inequalities on the sos-profile can be described explicitly as coming from 2×2 minors of a certain *moment matrix*. We showed that pure binomial inequalities that can be deduced in this way sometimes cannot even approximate valid binomial inequalities on the true profile $\mathcal{G}_{\mathcal{U}}$.

A graph combination a is *sos-testable* if it is nonnegative on $\mathcal{S}_d$ for some d. Sos-testable functions do not have to come with an explicit certificate of nonnegativity on an sos-profile. However, in principle, since $\mathcal{S}_d$ is a semialgebraic set, nonnegativity of a graph combination on $\mathcal{S}_d$ can be verified via real quantifier elimination. We show that if a graph combination a becomes sos-testable after multiplication by an sos-testable graph combination b, then a was already sos-testable. The class of sos-testable functions includes sums of squares and also rational sums of squares, but is quite likely significantly larger. It is not clear at this point whether even rational sos is a bigger class than just sos.

In [3] we exhibited concrete families of binomial graph density inequalities that are not sos-testable, even approximately. An example of such a binomial inequality are all Blakley-Roy inequalities for odd paths.

References

[1] G. Blekherman, P. A. Parrilo, and R. R. Thomas, *Semidefinite Optimization and Convex Algebraic Geometry* SIAM, (2012).

[2] G. Blekherman, A. Raymond, M. Singh, and R. R. Thomas. *Simple graph density inequalities with no sum of squares proofs* Combinatorica, (2020).

[3] G. Blekherman, A. Raymond, M. Singh, and R. R. Thomas. *Tropicalization of Graph Profiles* arXiv preprint arXiv:2004.05207, (2020).

[4] G. Blekherman, and A. Raymond, *A Path Forward: Tropicalization in Extremal Combinatorics* arXiv preprint arXiv:2108.06377, (2021).

[5] D. Colon, J. Fox, and B. Sudakov, *An approximate version of Sidorenko's conjecture* Geom. Funct. Anal. 20, no. 6, 1354–1366, (2010).

[6] D. Conlon, J. H. Kim, C. lee, and J. Lee, *Some advances on Sidorenko's conjecture* J. Lond. Math. Soc. (2) 98, no. 3, 593–608, (2018).

[7] P. Erdős, L. Lovász, and J. Spencer, *Strong independence of graphcopy functions* Graph theory and related topics (Proc. Conf., Univ. Waterloo, Waterloo, Ont., 1977), pp. 165–172, (1977).

[8] V. Falgas-Ravry and E. R. Vaughan, *Applications of the semi-definite method to the Turán density problem for 3-graphs* Combin. Probab. Comput. 22, no. 1, 21–54, (2013).

[9] H. Hatami, J. Hladký, D. Král', S. Norin, and A. Razborov, *On the number of pentagons in triangle-free graphs* J. Combin. Theory Ser. A 120, no. 3, 722–732, (2013).

[10] H. Hatami, S. Norin, *Undecidability of linear inequalities in graph homomorphism densities* J. Amer. Math. Soc. 24, no. 2, 547–565, (2011).
[11] J. H. Kim, C. Lee, and J. Lee, *Two approaches to Sidorenko's conjecture* Trans. Amer. Math. Soc.368, no. 7, 5057–5074, (2016).
[12] L. Lovász, *Large Networks and Graph Limits* American Mathematical Society Colloquium Publications, vol. 60, American Mathematical Society, Providence, RI, (2012).
[13] L. Lovász, B. Szegedy, *Random graphons and a weak Positivstellensatz for graphs* J. Graph Theory 70, no. 2, 214–225, (2012).
[14] T. Netzer, A. Thom, *Positivstellensätze for quantum multigraphs* J. Algebra 422, 504–519, (2015).
[15] V. Nikiforov, *The number of cliques in graphs of given order and size* Trans. Amer. Math. Soc. 363, no. 3, 1599–1618, (2011).
[16] A. A. Razborov, *Flag algebras* J. Symbolic Logic 72, no. 4, 1239–1282, (2007).
[17] A. A. Razborov, *On the minimal density of triangles in graphs* Combin. Probab. Comput. 17, no. 4, 603–618, (2008).
[18] A. A. Razborov, *On 3-hypergraphs with forbidden 4-vertex configurations* SIAM J. Discrete Math. 24, no. 3, 946–963, (2010).
[19] C. Reiher, *The clique density theorem* Ann. of Math. (2) 184, no. 3, 683–707, (2016).
[20] B. Szegedy, *An information theoretic approach to Sidorenko's conjecture* arXiv preprint arXiv:1406.6738, (2014).

Reporter: Ala Shayeghi

Participants

Prof. Dr. Guillaume Aubrun
Institut Camille Jordan
Université Claude Bernard Lyon 1
43 Boulevard du 11 novembre 1918
69622 Villeurbanne Cedex
FRANCE

Dr. Mario Berta
Imperial College London
Department of Computing
Huxley Building
180 Queen's Gate
London SW7 2AZ
UNITED KINGDOM

Prof. Dr. Greg Blekherman
School of Mathematics
Georgia Institute of Technology
686 Cherry Street
Atlanta GA 30332-0160
UNITED STATES

Prof. Dr. Nilanjana Datta
Department of Applied Mathematics &
Theoretical Physics
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 OWA
UNITED KINGDOM

Dr. Gemma De las Cuevas
Institut für Theoretische Physik
Universität Innsbruck
Technikerstr. 21a
6020 Innsbruck
AUSTRIA

Prof. Dr. Hamza Fawzi
Department of Applied Mathematics &
Theoretical Physics (DAMTP)
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WA
UNITED KINGDOM

Prof. Dr. Omar Fawzi
Mathématiques
École Normale Superieure de Lyon
46, Allée d'Italie
69364 Lyon Cedex 07
FRANCE

Dr. Sander Gribling
Institut de Recherche en Informatique
Fondamentale
Université de Paris
Bâtiment Sophie Germain
Case 7012
75205 Paris Cedex 13
FRANCE

Prof. Dr. Aram Harrow
Center for Theoretical Physics
Massachusetts Institute of
Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

Arne Heimendahl
Mathematisches Institut
Universität zu Köln
Weyertal 86 - 90
50931 Köln
GERMANY

Dr. Felix Huber
Institute of Theoretical Physics
Jagiellonian University
Lojasiewicza 6
30-348 Kraków
POLAND

Andreas Klingler
Institute for Theoretical Physics
University of Innsbruck
Technikerstr. 21A
6020 Innsbruck
AUSTRIA

Dr. Robert König
Zentrum für Mathematik
Technische Universität München
Boltzmannstraße 3
85748 Garching bei München
GERMANY

Prof. Dr. Cécilia A. Lancien
Institut de Mathématiques de Toulouse
Université Paul Sabatier
118, route de Narbonne
31062 Toulouse Cedex 9
FRANCE

Prof. Dr. Monique Laurent
Centrum Wiskunde & Informatica
(CWI)
Postbus 94079
1090 GB Amsterdam
NETHERLANDS

Prof. Dr. Debbie Leung
Dept. of Combinatorics & Optimization
University of Waterloo
Waterloo ON N2L 3G1
CANADA

Prof. Dr. Tim Netzer
Institut für Mathematik
Universität Innsbruck
Technikerstrasse 13
6020 Innsbruck
AUSTRIA

Harold Nieuwboer
Korteweg-de Vries Institute for
Mathematics and QuSoft
University of Amsterdam
Science Park 105
1098 XG Amsterdam
NETHERLANDS

Prof. Dr. Ryan O'Donnell
School of Computer Science
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3890
UNITED STATES

Prof. Dr. Pablo A. Parrilo
Department of Electrical Engineering
and Computer Science
Laboratory for Information and
Decision Systems
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

Prof. Dr. Vern I. Paulsen
Department of Pure Mathematics
University of Waterloo
200 University Avenue West
Waterloo ON N2L 3G1
CANADA

Prof. Dr. David Pérez-García
Facultad de Matematicas
Dpto. de Análisis Matemático y
Matemática Aplicada
Universidad Complutense de Madrid
Plaza de Ciencias 3
28040 Madrid
SPAIN

Dr. Stefano Pironio
Laboratoire d'Information Quantique
Université Libre de Bruxelles
CP 204
Avenue F.D. Roosevelt 50
1050 Bruxelles
BELGIUM

Anthony Polloreno
JILA
University of Colorado
Boulder CO 80302
UNITED STATES

Samuel Scalet
Department of Applied Mathematics & Theoretical Physics (DAMTP)
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WA
UNITED KINGDOM

Dr. Ala Shayeghi
Mathématiques
École Normale Superieure de Lyon
46, Allee d'Italie
69364 Lyon Cedex 07
FRANCE

William E. Slofstra
Department of Pure Mathematics
University of Waterloo
200 University Avenue West
Waterloo ON N2L 3G1
CANADA

Hoang Ta
Mathématiques
École Normale Superieure de Lyon
46, Allée d'Italie
69364 Lyon Cedex 07
FRANCE

Dr. Mirte van der Eyden
Institut für Mathematik
Universität Innsbruck
Technikerstr. 25
6020 Innsbruck
AUSTRIA

Prof. Dr. Thomas Vidick
Department of Computing and Mathematical Sciences
California Institute of Technology
Annenberg 207
1200 E. California Boulevard
Pasadena, CA 91125-5000
UNITED STATES

Prof. Dr. Michael Walter
Korteweg-de Vries Instituut for Mathematics
Universiteit van Amsterdam
Postbus 94079
1090 GB Amsterdam
NETHERLANDS

Prof. Dr. Andreas Winter
Universitat Autònoma de Barcelona
Departament de Física
Àrea de Física Teòrica
Edifici C
Campus de la UAB
08193 Bellaterra, Barcelona
SPAIN