Single trusted qubit is necessary and sufficient for quantum realisation of extremal no-signaling statistics

Ravishankar Ramanathan[1], **Michał Banacki[2,3]**, Ricard Ravell Rodríguez[2], Paweł Horodecki[2,4]

[1]Department of Computer Science, The University of Hong Kong; [2]International Centre for Theory of Quantum Technologies, University of Gdańsk; [3]Faculty of Mathematics, Physics and Informatics, University of Gdańsk; [4]Faculty of Applied Physics and Mathematics, National Quantum Information Centre, Gdańsk University of Technology

Abstract

We consider quantum statistics from the perspective of post-quantum no-signaling theories in which either none or only a certain number of quantum systems are trusted. These scenarios can be fully described by the so-called no-signaling boxes or no-signaling assemblages respectively. It has been shown so far that in the usual Bell non-locality scenario with a single measurement run, quantum correlations can never reproduce an extremal non-local point within the set of no-signaling boxes. We provide here a general no-go rule showing that the latter stays true even if arbitrary sequential measurements are allowed. On the other hand, we prove a positive result showing that already a single trusted qubit is enough for quantum theory to produce a self-testable extremal point within the corresponding set of no-signaling assemblages. This result provides a tool that opens up possibilities for security proofs of cryptographic protocols against general no-signaling adversaries in semi-device-independent scenarios.

No-go results for no-signaling boxes

Consider the polytope **NS** of all no-signaling boxes $P = \{p(\mathbf{a}|\mathbf{x})\}_{\mathbf{a},\mathbf{x}}$ describing Bell scenario related to the system of n separated parties A_i. Inside this set one can consider another polytope **Loc** of all local boxes (i.e. convex hull of all deterministic correlations) and the convex set **Q** of no-signaling boxes with *quantum realisation* given by

$$p(a_1,\ldots,a_n|x_1,\ldots,x_n) = \mathrm{Tr}\left(M^{(1)}_{a_1|x_1}\otimes\ldots\otimes M^{(n)}_{a_n|x_n}\rho_{A_1\ldots A_n}\right). \tag{1}$$

As it is well-known that **Loc** $\subsetneq$ **Q**, it is natural to ask whether it is possible to obtain a non-local extremal box in **NS** by appropriate choice of a quantum state and quantum measurements according to formula (1). It has been established [1] that this task is impossible (regardless of the number of parties, settings, and outcomes).

This question can be extended to the setting of sequential measurements (for the bipartite system) in which one can define the notion of general time-ordered no-signaling polytope **TONS** and its subsets **Qseq**, **TOLoc** consisting of correlations admitting respectively quantum and classical (local) realisation (see [2] for detailed definitions of considered convex sets).

No-go result in the sequential setting

Theorem 1. *[2] Let P be an extremal point of the time-ordered no-signaling polytope **TONS** (for the bipartite case) such that $P \notin$ **TOLoc**. Then $P \notin$ **Qseq**.*

This rules out the quantum realisation of extremal non-local statistics.

No-signaling assemblages

Consider a bipartite steering scenario in which two distant subsystems A (uncharacterised) and B (characterised) share a quantum state ρ_{AB}. According to measurements $M_{a|x}$ performed on A, the subsystem B is described by a *quantum assemblage* - a collection of subnormalised states

$$\sigma^{(B)}_{a|x} = \mathrm{Tr}_A\left(M_{a|x}\otimes\mathbb{1}\rho_{AB}\right). \tag{2}$$

One can can generalised this picture to the abstract notion of *no-signaling assemblage* $\Sigma^{(B)} = \left\{\sigma^{(B)}_{a|x}\right\}_{a,x}$ defined by the following no-signaling conditions $\forall_{a,x}\ \sigma^{(B)}_{a|x} \geq 0$, $\forall_{x,x'}\ \sum_a \sigma^{(B)}_{a|x} = \sigma^{(B)} = \sum_a \sigma^{(B)}_{a|x'}$ and $\mathrm{Tr}(\sigma^{(B)}) = 1$. However, it has been proven [3] that any bipartite no-signaling assemblage also admits *quantum realisation*, i.e. it can be expressed by formula (2). **Therefore, there is no post-quantum steering in the bipartite setting.**

The situation changes if we consider assemblages with three separated subsystems A, B, C in which a characterised quantum subsystem C shares with uncharacterised parties A, B a joint state described by some no-signaling (but possibly post-quantum) theory.

Tripartite no-signaling assemblage

Definition 2. [4] Tripartite *no-signaling assemblage* $\Sigma^{(C)} = \left\{\sigma^{(C)}_{ab|xy}\right\}_{a,b,x,y}$ is a collection of positive operators satisfying

$$\forall_{b,x,x',y}\ \sum_a \sigma^{(C)}_{ab|xy} = \sum_a \sigma^{(C)}_{ab|x'y}, \tag{3}$$

$$\forall_{a,x,y,y'}\ \sum_b \sigma^{(C)}_{ab|xy} = \sum_b \sigma^{(C)}_{ab|xy'}, \tag{4}$$

$$\forall_{x,y}\ \mathrm{Tr}\left(\sum_{a,b}\sigma^{(C)}_{ab|xy}\right) = 1. \tag{5}$$

Not all $\Sigma^{(C)}$ admit *quantum realisation* [4] given by

$$\sigma^{(C)}_{ab|xy} = \mathrm{Tr}_{AB}\left(M_{a|x}\otimes N_{b|y}\otimes\mathbb{1}\rho_{ABC}\right). \tag{6}$$

Therefore, quantum assemblages form a nontrivial convex subset inside the convex set of all no-signaling assemblages. The role of classical assemblages is played by the convex set of LHS (local hidden state) assemblages defined by formula $\sigma^{(C)}_{ab|xy} = \sum_i q_i p_i(a|x) p'_i(b|y)\sigma^{(C)}_i$ where $q_i \geq 0, \sum_i q_i = 1$ [5].

Inflexibility

Definition 3. [2] Consider a no-signaling assemblage $\Sigma^{(C)} = \{p_i|\psi_i\rangle\langle\psi_i|\}_i$ with all positions occupied by at most rank one operators. Any other assemblage $\tilde{\Sigma}^{(C)} = \{q_i|\psi_i\rangle\langle\psi_i|\}_i$ with the same states at the same positions and the additional property that $p_i = 0$ implies $q_i = 0$ is called *similar* to $\Sigma^{(C)}$.

Definition 4. [2] $\Sigma^{(C)}$ is *inflexible* if for any $\tilde{\Sigma}^{(C)}$ similar to $\Sigma^{(C)}$ we get $\Sigma^{(C)} = \tilde{\Sigma}^{(C)}$.

Note that in particular *inflexibility implies extremality* in the set of all no-signaling assemblages.

Realisation of extremal assemblages

In analogy to the fundamental question in non-locality, it is interesting to ask whether a quantum assemblage can realise an extremal non-classical point in the larger convex set of all no-signaling assemblages. **Remarkably this question admits an affirmative answer in the simplest nontrivial setting** (from now on we set $a, b, x, y \in \{0, 1\}$).

Quantum realisation of extremal assemblages

Proposition 5. *[2] For any pure genuine tripartite entangled state $|\psi_{ABC}\rangle \in \mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^d$ there exists a pair of PVMs $P_{a|x}$ with two outcomes on subsystem A (and respectively a pair of PVMs $Q_{b|y}$ with two outcomes on subsystem B) such that a no-signaling assemblage $\Sigma^{(C)}$ obtained by $\sigma^{(C)}_{ab|xy} = \mathrm{Tr}_{AB}\left(P_{a|x}\otimes Q_{b|y}\otimes\mathbb{1}|\psi_{ABC}\rangle\langle\psi_{ABC}|\right)$ is inflexible. In particular, $\Sigma^{(C)}$ is extremal, not LHS, and it is the only assemblage that maximally violates steering inequality $F_{\Sigma^{(C)}}$.*

$$F_{\Sigma^{(C)}}(\tilde{\Sigma}^{(C)}) = \sum_{a,b,x,y=0,1}\mathrm{Tr}(\rho_{ab|xy}\tilde{\sigma}^{(C)}_{ab|xy}) \qquad \rho_{ab|xy} = \begin{cases} 0 & \text{for } \sigma^{(C)}_{ab|xy} = 0, \\ \frac{\sigma^{(C)}_{ab|xy}}{\mathrm{Tr}(\sigma^{(C)}_{ab|xy})} & \text{for } \sigma^{(C)}_{ab|xy} \neq 0. \end{cases} \tag{7}$$

This proposition along with Jordan's lemma led to the following self-testing result.

Proposition 6. *[2] Consider any pure state $|\tilde{\psi}_{A'B'C}\rangle \in \mathbb{C}^{d_{A'}}\otimes\mathbb{C}^{d_{B'}}\otimes\mathbb{C}^{d_C}$ and assemblage $\tilde{\Sigma}^{(C)}$ with elements $\tilde{\sigma}^{(C)}_{ab|xy} = \mathrm{Tr}_{A'B'}\left(\tilde{P}_{a|x}\otimes\tilde{Q}_{b|y}\otimes\mathbb{1}|\tilde{\psi}_{A'B'C}\rangle\langle\tilde{\psi}_{A'B'C}|\right)$ where $\tilde{P}_{a|x}, \tilde{Q}_{b|y}$ define some PVMs. Then $F_{\Sigma^{(C)}}(\tilde{\Sigma}^{(C)})$ achieves a maximal value if and only if $V_{A'}\otimes V_{B'}\otimes\mathbb{1}|\tilde{\psi}_{A'B'C}\rangle = |\phi_{A''B''}\rangle|\psi_{ABC}\rangle$, and $(V_{A'}\otimes V_{B'}\otimes\mathbb{1})(\tilde{P}_{a|x}\otimes\tilde{Q}_{b|y}\otimes\mathbb{1})|\tilde{\psi}_{A'B'C}\rangle = |\phi_{A''B''}\rangle(P_{a|x}\otimes Q_{b|y}\otimes\mathbb{1})|\psi_{ABC}\rangle$ where $|\psi_{ABC}\rangle$, $P_{a|x}, Q_{b|y}$ and $F_{\Sigma^{(C)}}$ are like in Proposition 5, $V_{A'}, V_{B'}$ are some local isometries and $|\phi_{A''B''}\rangle$ is some irrelevant state shared by A and B.*

References

[1] R. Ramanathan, J. Tuziemski, M. Horodecki, P. Horodecki, Phys. Rev. Lett. **117**, 050401 (2016).

[2] R. Ramanathan, M. Banacki, R. R. Rodríguez, P. Horodecki, arXiv:2004.14782.

[3] L. P. Hughston, R. Jozsa, K. Wooters, Phys. Lett. A **183**,14 (1993).

[4] A. B. Sainz, N. Brunner, D. Cavalcanti, P. Skrzypczyk, T. Vértesi, Phys. Rev. Lett. **115**, 190403 (2015).

[5] A. B. Sainz, L. Aolita, M. Piani, M. J. Hoban, P. Skrzypczyk, New J. Phys. **20**, 083040 (2018).

Acknowledgements

M.B., R.R.R. and P.H. acknowledge support by the Foundation for Polish Science (IRAP project, ICTQT, contract no. 2018/MAB/5, co-financed by EU within Smart Growth Operational Programme). R.R. acknowledges support from the Start-up Fund 'Device-Independent Quantum Communication Networks' from The University of Hong Kong. This work was supported by the National Natural Science Foundation of China through grant 11675136, the Hong Kong Research Grant Council through grant 17300918, and the John Templeton Foundation through grants 60609, Quantum Causal Structures, and 61466, The Quantum Information Structure of Spacetime (qiss.fr). The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation.