LOCALLY RESTRICTED MEASUREMENTS ON A MULTIPARTITE QUANTUM SYSTEM: DATA HIDING IS GENERIC

GUILLAUME AUBRUN AND CÉCILIA LANCIEN

1. Introduction

How quantum measurements can help us make decisions? We consider a basic problem, the task of distinguishing two quantum states, where this question has a neat answer. Given a POVM (Positive Operator-Valued Measure) M on a Hilbert space $\mathcal{H}$, Matthews, Wehner and Winter [19] introduced its distinguishability norm $\|\cdot\|_{\mathrm{M}}$, which has the property that given a pair (ρ,σ) of quantum states on $\mathcal{H}$, $\|\rho-\sigma\|_{\mathrm{M}}$ is (up to a factor 1/2) the bias observed when the POVM M is used optimally to distinguish ρ from σ (the larger is the norm, the more efficient is the POVM). More generally, we can associate to a family of POVMs $\mathbf{M}$ the operational norm $\|\cdot\|_{\mathbf{M}} = \sup\{\|\cdot\|_{\mathrm{M}} \ : \ \mathrm{M}\in\mathbf{M}\}$ which corresponds to the bias achieved by the best POVM from the family.

In [1], the situation we more particularly look at is when the underlying global Hilbert space $\mathcal{H}$ is the tensor product of several local Hilbert spaces. Various classes of POVMs can then be defined on $\mathcal{H}$, corresponding to various levels of locality restrictions (see e.g. [19] or [15] for further information). For simplicity, let us focus on the case of a (finite-dimensional) bipartite system in which both parts play the same role and consider the Hilbert space $\mathcal{H} = \mathbf{C}^d \otimes \mathbf{C}^d$.

The most restricted class of POVMs on $\mathcal{H}$ is the one **LO** of local measurements, whose elements are tensor products of measurements on each of the sub-systems. This corresponds to the situation where parties are not allowed to communicate. As a relaxation of **LO**, one may consider the class **SEP** of separable measurements, whose elements are the measurements on $\mathcal{H}$ made of tensor operators. Important subclasses of **SEP** are the classes **LOCC** and $\mathbf{LOCC}^{\rightarrow}$ (Local Operations and Classical Communication) of measurements that can be implemented by a finite sequence of local operations on the sub-systems followed by classical communication between the parties (either two-way or one-way). Finally, as a further weakening of the locality constraints, one may look at the class **PPT** of positive under partial transpose measurements, whose elements are the measurements on $\mathcal{H}$ made of operators that remain positive when partially transposed on one sub-system.

It is clear from the definitions that we have the chain of inclusions

$$\mathbf{LO} \subset \mathbf{LOCC}^{\rightarrow} \subset \mathbf{LOCC} \subset \mathbf{SEP} \subset \mathbf{PPT} \subset \mathbf{ALL}$$

and consequently the chain of norm inequalities

$$\|\cdot\|_{\mathbf{LO}} \leqslant \|\cdot\|_{\mathbf{LOCC}^{\rightarrow}} \leqslant \|\cdot\|_{\mathbf{LOCC}} \leqslant \|\cdot\|_{\mathbf{SEP}} \leqslant \|\cdot\|_{\mathbf{PPT}} \leqslant \|\cdot\|_{\mathbf{ALL}}. \tag{1}$$

All the inequalities in (1) are known to be strict provided $d>2$ (the difference between $\|\cdot\|_{\mathbf{LOCC}^{\rightarrow}}$ and $\|\cdot\|_{\mathbf{LOCC}}$, as well as between $\|\cdot\|_{\mathbf{LOCC}}$ and $\|\cdot\|_{\mathbf{SEP}}$, having been established only very recently though, in [7]).

As for us, we are interested in the high-dimensional behaviour of these norms, and the general question we investigate is whether or not the various gaps in the hierarchy are bounded (independently of the dimension of the subsystems). It is already known that the gap between **PPT** and **ALL** is unbounded, an important example being provided by the symmetric state ς and the antisymmetric state α on $\mathbf{C}^d \otimes \mathbf{C}^d$ which satisfy (see e.g. [10])

$$\|\varsigma-\alpha\|_{\mathbf{ALL}} = 2 \quad \text{while} \quad \|\varsigma-\alpha\|_{\mathbf{PPT}} = \frac{4}{d+1}.$$

We show however (Theorem 2.1) that such feature is not generic. This is in contrast with the gap between **SEP** and **PPT** which we prove to be generically unbounded (Theorem 2.1). We also provide examples of unbounded gap between **LO** and $\mathbf{LOCC}^{\rightarrow}$ (Theorem 2.3) but we do not know if this situation is typical. Regarding the gaps between $\mathbf{LOCC}^{\rightarrow}$, **LOCC** and **SEP**, determining whether they are bounded remains an open problem.

Note also that for states of low rank, the gaps between these norms remain bounded. Indeed, it follows from the results of [15] that, for any Hermitian Δ of rank at most r on $\mathbf{C}^d \otimes \mathbf{C}^d$, we have $\|\Delta\|_{\mathrm{LO}} \geqslant \|\Delta\|_{\mathbf{ALL}}/18\sqrt{r}$. So we do not restrict our study to this kind of states, for which it would loose all relevance.

2. Discriminating power of the different classes of locally restricted measurements: Overview of our results

Our main result compares the efficiency of the classes $\mathbf{LOCC}^{\rightarrow}$, **LOCC**, **SEP**, **PPT** and **ALL** to perform a typical discrimination task. Here "typical" means the following: we consider the problem of distinguishing ρ from σ, where ρ and σ are random states, chosen independently at random with respect to the uniform measure (i.e. the Lebesgue measure induced by the Hilbert–Schmidt distance) on the set of all states. It turns out that the PPT constraint on the allowed measurements is not very restrictive, affecting typically the performance by only a constant factor, while the separability one implies a more substantial loss. This shows that generic bipartite states are data hiding: separable measurements (and even more so local measurements followed by classical communication) can poorly distinguish them (see [12] for another instance of this phenomenon).

Theorem 2.1. *There are universal constants $C, c > 0$ such that the following holds. Given a dimension d, let ρ and σ be independent random states, uniformly distributed on the set of states on $\mathbf{C}^d \otimes \mathbf{C}^d$. Then, with high probability,*

$$c \leqslant \|\rho - \sigma\|_{\mathbf{PPT}} \leqslant \|\rho - \sigma\|_{\mathbf{ALL}} \leqslant C,$$

$$\frac{c}{\sqrt{d}} \leqslant \|\rho - \sigma\|_{\mathbf{LOCC}^{\rightarrow}} \leqslant \|\rho - \sigma\|_{\mathbf{LOCC}} \leqslant \|\rho - \sigma\|_{\mathbf{SEP}} \leqslant \frac{C}{\sqrt{d}}.$$

Here, "with high probability" means that the probability that one of the conclusions fails is less than $\exp(-c_0 d)$ for some universal constant $c_0 > 0$.

An immediate consequence of these high probability estimates is that one can find in $\mathbf{C}^d \otimes \mathbf{C}^d$ exponentially many states which are pairwise data hiding.

Corollary 2.2. *There are universal constants $C, c > 0$ such that, if $\mathcal{A}$ denotes a set of $\exp(cd)$ independent random states uniformly distributed on the set of states on $\mathbf{C}^d \otimes \mathbf{C}^d$, with high probability any pair of distinct states $\rho, \sigma \in \mathcal{A}$ satisfies the conclusions of Theorem 2.1.*

We deduce Theorem 2.1 from estimates on the "size" of the unit balls for the norms dual to the distinguishability norms $\|\cdot\|_{\mathbf{M}}$, for $\mathbf{M} \in \{\mathbf{LOCC}^{\rightarrow}, \mathbf{LOCC}, \mathbf{SEP}, \mathbf{PPT}, \mathbf{ALL}\}$. More specifically, using techniques from asymptotic geometric functional analysis, we compute parameters known as the *mean width* and the *volume radius* of these convex bodies (a bit in the spirit of [4]). The use of concentration of measure (i.e. roughly speaking the fact that "reasonable" functions on a high-dimensional space have an exponentially small probability of deviating from their average) then allows to pass from these global estimates to estimates in a typical direction. A few tools from random matrix theory are eventually needed to get the precise results appearing in Theorem 2.1.

We also show that even the smallest amount of communication has a huge influence: we give examples of states which are perfectly distinguishable under local measurements and one-way classical communication but very poorly distinguishable under local measurements with no communication between the parties.

Theorem 2.3. *There is a universal constant $C > 0$ such that the following holds: for any dimension d, there exist states ρ and σ on $\mathbf{C}^d \otimes \mathbf{C}^d$ such that $\|\rho - \sigma\|_{\mathbf{LOCC}^{\rightarrow}} = 2$ while $\|\rho - \sigma\|_{\mathbf{LO}} \leqslant \frac{C}{\sqrt{d}}$.*

These states are constructed as follows: assuming without loss of generality that d is even, let E be a fixed $d/2$-dimensional subspace of $\mathbf{C}^d$, let $U_1, \ldots, U_d$ be random independent Haar-distributed unitaries on $\mathbf{C}^d$, and define the random states $\rho_i = U_i \frac{P_E}{d/2} U_i^\dagger$ and $\sigma_i = U_i \frac{P_{E^\perp}}{d/2} U_i^\dagger$, $1 \leqslant i \leqslant d$, on $\mathbf{C}^d$ (where P_E and $P_{E^\perp}$ denote the orthogonal projections onto E and $E^\perp$ respectively). Then, denoting by $\{|1\rangle, \ldots, |d\rangle\}$ an orthonormal basis of $\mathbf{C}^d$, define

$$\rho = \frac{1}{d} \sum_{i=1}^{d} |i\rangle\langle i| \otimes \rho_i \quad \text{and} \quad \sigma = \frac{1}{d} \sum_{i=1}^{d} |i\rangle\langle i| \otimes \sigma_i.$$

The pair (ρ, σ) fulfils the criteria of Theorem 2.3 with high probability.

Theorem 2.3 is built on the idea that, typically, a single POVM cannot succeed simultaneously in several "sufficiently different" discrimination tasks. It is made mathematically precise by a careful use of nets and Bernstein-type deviation inequalities in high dimension (a bit in the spirit of [3]).

3. Applications to data hiding

What Theorem 2.1 establishes is that generic bipartite states are data hiding for separable measurements but not for PPT measurements. The following can more specifically be stated: picking a subspace E at random from the set of $d^2/2$-dimensional subspaces of $\mathbf{C}^d \otimes \mathbf{C}^d$ (assuming without loss of generality that d is even), and then considering the states $\rho = \frac{P_E}{d^2/2}$ and $\sigma = \frac{P_{E^\perp}}{d^2/2}$, one gets examples of states which are perfectly distinguishable by some global

measurement and which are with high probability data hiding for separable measurements but not data hiding for PPT measurements. This somehow counterbalances the usually cited constructions of data hiding schemes using Werner states, which are data hiding in the exact same way for both separable and PPT measurements (see e.g. [9, 10, 11] and [19, 15]).

Also, we focused up to here on the bipartite case $\mathcal{H} = (\mathbf{C}^d)^{\otimes 2}$ for the sake of clarity. However, generalizations to the general k-partite case $\mathcal{H} = (\mathbf{C}^d)^{\otimes k}$ are quite straightforward, at least in the situation where the high-dimensional composite system of interest is made of a "small" number of "large" subsystems (i.e. k is fixed and d tends to infinity).

Let us denote by $\mathbf{PPT}_{d,k}$ and $\mathbf{SEP}_{d,k}$ the sets of respectively k-PPT and k-separable POVMs on $(\mathbf{C}^d)^{\otimes k}$. A multipartite analogue of Theorem 2.1 can then be derived, following the exact same lines of proof.

Theorem 3.1. *There exist constants $c_k, C_k > 0$ such that the following holds. Given a dimension d, let ρ and σ be independent random states, uniformly distributed on the set of states on $(\mathbf{C}^d)^{\otimes k}$. Then, with high probability,*

$$c_k \leqslant \|\rho - \sigma\|_{\mathbf{PPT}_{d,k}} \leqslant \|\rho - \sigma\|_{\mathbf{ALL}} \leqslant C_k,$$

$$\frac{c_k}{\sqrt{d^{k-1}}} \leqslant \|\rho - \sigma\|_{\mathbf{SEP}_{d,k}} \leqslant \frac{C_k}{\sqrt{d^{k-1}}}.$$

This means that, forgetting about the dependence on k and only focusing on the one on d, for "typical" states ρ, σ on $(\mathbf{C}^d)^{\otimes k}$, $\|\rho - \sigma\|_{\mathbf{PPT}_{d,k}}$ is of order 1, like $\|\rho - \sigma\|_{\mathbf{ALL}}$, while $\|\rho - \sigma\|_{\mathbf{SEP}_{d,k}}$ is of order $1/\sqrt{d^{k-1}}$.

In this multipartite setting, another quite natural question is the one of finding states that local observers can poorly distinguish if they remain alone but that they can distinguish substantially better though by gathering into any possible two groups. This type of problem was especially studied in [11]. Here is another result in that direction.

Define $\mathbf{bi-SEP}_{d,k}$ as the set of POVMs on $(\mathbf{C}^d)^{\otimes k}$ which are biseparable across any bipartition of $(\mathbf{C}^d)^{\otimes k}$. It may then be shown that for random states ρ, σ, independent and uniformly distributed on the set of states on $(\mathbf{C}^d)^{\otimes k}$, with high probability, $\|\rho - \sigma\|_{\mathbf{bi-SEP}_{d,k}} \simeq d^{-k/4}$ (whereas $\|\rho - \sigma\|_{\mathbf{SEP}_{d,k}} \simeq d^{-(k-1)/2}$ by Theorem 3.1). This means that on $(\mathbf{C}^d)^{\otimes k}$, with $k > 2$ fixed, restricting to POVMs which are biseparable across every bipartition is roughly the same as restricting to POVMs which are biseparable across one (balanced) bipartition, whereas imposing k-separability is a much tougher constraint that implies a dimensional loss in the distinguishing ability.

4. More general perspectives

We solved the issue of determining, for several classes of measurements $\mathbf{M}$, what is the typical value of the measured trace distance $\|\rho - \sigma\|_{\mathbf{M}}$ between two states ρ, σ. Several other "filtered through measurements" distances between ρ and σ can be defined in a completely analogous way, such as e.g. the measured fidelity distance $F_{\mathbf{M}}(\rho, \sigma)$ or the measured relative entropy distance $D_{\mathbf{M}}(\rho\|\sigma)$ (see e.g. [22]). These quantities are all closely related to one another by well-known inequalities. Our statements can thus be straightforwardly translated into statements on the typical value of $F_{\mathbf{M}}(\rho, \sigma)$ or $D_{\mathbf{M}}(\rho\|\sigma)$. Besides, such restricted distance measures have already found a tremendous amount of applications in quantum information theory (see e.g. [6] or [18] for two very recent ones, in two quite different topics). Understanding better what is their generic scaling (and ultimately the one of their regularised versions) is therefore of prime interest, amongst other, to assess how optimal are the bounds where they appear, what is the efficiency of the quantum information processing protocols where they are involved etc.

References

[1] **G. Aubrun, C. Lancien**, "Locally restricted measurements on a multipartite quantum system: data hiding is generic"; arXiv:1406.1959.

[2] **G.W. Anderson, A. Guionnet, O. Zeitouni**, *An Introduction to Random Matrices*, Cambridge Studies in Advanced Mathematics, Vol. 118, Cambridge University Press, Cambridge, 2010.

[3] **G. Aubrun, C. Lancien**, "Zonoids and sparsification of quantum measurements"; arXiv:1309.6003

[4] **G. Aubrun, S.J. Szarek**, "Tensor product of convex sets and the volume of separable states on N qudits", Phys. Rev. A. 73 (2006); arXiv:quant-ph/0503221.

[5] **R. Bhatia**, *Matrix analysis*, Graduate Texts in Mathematics, Vol. 169, Springer-Verlag, New-York, 1997.

[6] **S. Bäuml, M. Christandl, K. Horodecki, A. Winter**, "Limitations on quantum-key repeaters"; arXiv:1402.5927[quant-ph].

[7] **E. Chitambar, M-H. Hsieh**, "Asymptotic state discrimination and a strict hierarchy in distinguishability norms"; arXiv:1311.1536[quant-ph].

[8] **A. Defant, C. Michels**, "Norms of tensor product identities." Note di Matematica 25.1, 129–166 (2006).

[9] **D.P. DiVincenzo, D. Leung, B.M. Terhal**, "Hiding Bits in Bell States", Phys. Rev. Lett. 86(25), 5807–5810 (2001); arXiv:quant-ph/0011042.

[10] **D.P. DiVincenzo, D. Leung, B.M. Terhal**, "Quantum Data Hiding", IEEE Trans. Inf Theory 48(3), 580-599 (2002); arXiv:quant-ph/0103098.

[11] **T. Eggeling, R.F. Werner**, "Hiding classical data in multi-partite quantum states", Phys. Rev. Lett. 89.097905 (2002); arXiv:quant-ph/0203004.

[12] **P. Hayden, D. Leung, P. Shor, A. Winter**, " Randomizing quantum states: Constructions and applications", Commun. Math. Phys. 250(2), 371–391 (2004); arXiv:quant-ph/0307104.
[13] **C.W. Helstrom**, *Quantum detection and estimation theory*, Academic Press, New York, 1976.
[14] **A.S. Holevo**, "Statistical decision theory for quantum systems", J. Mult. Anal. 3, 337–394 (1973).
[15] **C. Lancien, A. Winter**, "Distinguishing multi-partite states by local measurements", Commun. Math. Phys. 323, 555–573 (2013); arXiv[quant-ph]:1206.2884.
[16] **M. Ledoux, M. Talagrand** *Probability in Banach Spaces: isoperimetry and processes*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 23, Springer-Verlag, Berlin Heidelberg, 1991.
[17] **P. Lévy**, *Problèmes concrets d'analyse fonctionnelle* (French), 2nd ed. Gauthier-Villars, Paris, 1951.
[18] **K. Li, G. Smith**, "Quantum de Finetti theorem measured with fully one-way LOCC norm"; arXiv:1408.6829[quant-ph].
[19] **W. Matthews, S. Wehner, A. Winter**, "Distinguishability of quantum states under restricted families of measurements with an application to data hiding", Comm. Math. Phys. 291(3) (2009); arXiv:0810.2327[quant-ph].
[20] **E. Meckes, M. Meckes**, "Spectral measures of powers of random matrices", Electron. Commun. Probab. 18.78, 1–13 (2013); arXiv:1210.2681[math.PR].
[21] **V.D. Milman, A. Pajor**, "Entropy and asymptotic geometry of non-symmetric convex bodies", Advances in Math. 152, 314–335 (2000).
[22] **M. Piani**, "Relative entropy of entanglement and restricted measurements", Phys. Rev. Lett. 103.160504 (2009); arXiv:0904.2705[quant-ph].
[23] **G. Pisier**, *The Volume of Convex Bodies and Banach Spaces Geometry*, Cambridge Tracts in Mathematics Volume 94, Cambridge University Press, Cambridge, 1989.
[24] **C.A. Rogers, G.C.Shephard**, "Convex bodies associated with a given convex body" *J. London Math. Soc.* 33, 270–281 (1958).
[25] **L. Santaló**, "An affine invariant for convex bodies of n-dimensional space" (Spanish), Portugaliae Math. 8, 155–161 (1949).
[26] **K. Życzkowski, H-J. Sommers**, "Induced measures in the space of mixed quantum states", J. Phys. A. 34, 7111–7124 (2001); arXiv:quant-ph/0012101.

Guillaume Aubrun, *Institut Camille Jordan, Université Claude Bernard Lyon 1, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne Cedex, France.*

E-mail: aubrun@math.univ-lyon1.fr

Cécilia Lancien, *Institut Camille Jordan, Université Claude Bernard Lyon 1, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne Cedex, France* and *Física Teòrica: Informació i Fenomens Quàntics, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain.*

E-mail: lancien@math.univ-lyon1.fr