Locally restricted POVMs on a multipartite quantum system

QIC, Vol. 15, No. 5-6, 512–540 (2014) - arXiv:1406.1959[quant-ph]

Guillaume Aubrun [a] , **Cécilia Lancien** [a,b]
a) Université Claude Bernard Lyon 1, b) Universitat Autònoma de Barcelona
This research was supported by the ANR projects OSQPI and StoQ.

18th QIP, Sydney, January 10-16 2015

1 Distinguishability norms and quantum state discrimination

System that can be in two quantum states, ρ or σ, with equal prior probabilities.
Task: Decide in which one it is most likely, based on the accessible experimental data, i.e. on the outcome of a POVM $\mathrm{M} = (M_i)_{i\in I}$ performed on it (only one sample available $\rightarrow$ single observation).
Optimal strategy: Whenever outcome i is obtained, guess ρ if $\mathrm{Tr}(\rho M_i) > \mathrm{Tr}(\sigma M_i)$, and σ otherwise.

Optimal probability of error: $P_e = \frac{1}{2}\left(1 - \sum_{i\in I}\left|\mathrm{Tr}\left(\left[\frac{1}{2}\rho - \frac{1}{2}\sigma\right] M_i\right)\right|\right) := \frac{1}{2}\left(1 - \left\|\frac{1}{2}\rho - \frac{1}{2}\sigma\right\|_{\mathrm{M}}\right)$.

$\rightarrow$ "Distinguishability norm" $\left\|\frac{1}{2}\rho - \frac{1}{2}\sigma\right\|_{\mathrm{M}}$ = Bias of the POVM M on the state pair (ρ, σ) [13].

2 Distinguishability norms and convex geometry

- POVM $\mathrm{M} = (M_i)_{i\in I}$ on $\mathbf{C}^d$: $\{M_i \,:\, i \in I\}$ positive operators on $\mathbf{C}^d$ s.t. $\sum_{i\in I} M_i = \mathrm{Id}$.
- Associated distinguishability (semi-)norm: for any Hermitian Δ on $\mathbf{C}^d$, $\|\Delta\|_{\mathrm{M}} := \sum_{i\in I}\left|\mathrm{Tr}\left(\Delta M_i\right)\right|$.
- Associated convex body K_{M}: dual of the unit ball for $\|\cdot\|_{\mathrm{M}}$ (i.e. unit ball for the norm dual to $\|\cdot\|_{\mathrm{M}}$).
- Width of K_{M} in a given direction:

$$w(K_{\mathrm{M}}, \Delta) := \sup_{X\in K_{\mathrm{M}}} \mathrm{Tr}(\Delta X) = \|\Delta\|_{\mathrm{M}},$$

for Δ having unit Hilbert-Schmidt norm.
- Mean-width of K_{M}:

$$w(K_{\mathrm{M}}) := \mathbf{E}\, w(K_{\mathrm{M}}, \Delta) = \mathbf{E}\,\|\Delta\|_{\mathrm{M}},$$

for Δ uniformly distributed on the Hilbert-Schmidt norm unit sphere.

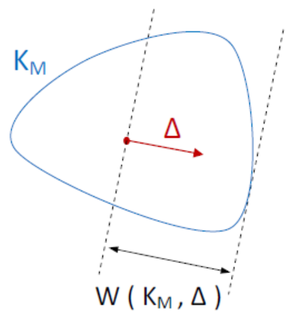

Figure 1: Width of K_{M} in the direction Δ

- For a whole set $\underline{\mathbf{M}}$ of POVMs on $\mathbf{C}^d$:
the associated distinguishability (semi-)norm is defined as $\|\cdot\|_{\underline{\mathbf{M}}} := \sup_{\mathrm{M}\in\underline{\mathbf{M}}} \|\cdot\|_{\mathrm{M}}$,
so that the associated convex body becomes $K_{\underline{\mathbf{M}}} = \mathrm{conv}\left(\bigcup_{\mathrm{M}\in\underline{\mathbf{M}}} K_{\mathrm{M}}\right)$.

3 Locally restricted measurements on a multipartite quantum system

Problem: Seminal observation in quantum state discrimination [10, 11]: $\|\cdot\|_{\underline{\mathbf{ALL}}} = \|\cdot\|_1$.
$\rightarrow$ For any two orthogonal quantum states, there exists a (global) POVM which perfectly discriminates them. But on a composite system, shared by several parties, there are locality constraints on the set $\underline{\mathbf{M}}$ of POVMs that experimenters are able to implement.

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

$\rightarrow$ How do these restrictions affect their distinguishing power? That is, do we have $\|\cdot\|_{\underline{\mathbf{M}}} \simeq \|\cdot\|_1$ or $\|\cdot\|_{\underline{\mathbf{M}}} \ll \|\cdot\|_1$ when the local dimensions grow?

Motivations:
- Existence of data-hiding states on multipartite systems [6, 8], i.e. states that would be well distinguished by a suitable global measurement but that are barely distinguishable by any local measurement.

Ex: Completely symmetric and antisymmetric states on $\mathbf{C}^d \otimes \mathbf{C}^d$, $\varsigma = \frac{1}{d^2+d}(\mathrm{Id} + \mathrm{F})$ and $\alpha = \frac{1}{d^2-d}(\mathrm{Id} - \mathrm{F})$.
$\Delta = \varsigma - \alpha$ is s.t. $\|\Delta\|_{\underline{\mathbf{LO}}} \leqslant \|\Delta\|_{\underline{\mathbf{LOCC}}} \leqslant \|\Delta\|_{\underline{\mathbf{SEP}}} = \|\Delta\|_{\underline{\mathbf{PPT}}} = \frac{4}{d+1} \ll 2 = \|\Delta\|_1$.
$\rightarrow$ Is this phenomenon generic or exceptional?
- Bounds valid for any Hermitian: very wide of the mark but known to be close from optimal [12].

Ex: On $\mathbf{C}^d \otimes \mathbf{C}^d$, $\frac{1}{\sqrt{18}d}\|\cdot\|_1 \leqslant \|\cdot\|_{\underline{\mathbf{LO}}} \leqslant \|\cdot\|_{\underline{\mathbf{LOCC}}} \leqslant \|\cdot\|_1$ and $\frac{1}{d}\|\cdot\|_1 \leqslant \|\cdot\|_{\underline{\mathbf{SEP}}} \leqslant \|\cdot\|_{\underline{\mathbf{PPT}}} \leqslant \|\cdot\|_1$.
$\rightarrow$ What about typical behaviours?

4 Unbounded gap between LO and one-way LOCC measurements

E a $d/2$-dimensional subspace of $\mathbf{C}^d$. $U_1, \ldots, U_d$ independent Haar-distributed unitaries on $\mathbf{C}^d$.
$\rightarrow$ 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 $\mathbf{C}^d$.
$\{|1\rangle, \ldots, |d\rangle\}$ an orthonormal basis of $\mathbf{C}^d$.
$\rightarrow$ Random states $\rho = \frac{1}{d}\sum_{i=1}^d |i\rangle\langle i| \otimes \rho_i$ and $\sigma = \frac{1}{d}\sum_{i=1}^d |i\rangle\langle i| \otimes \sigma_i$ on $\mathbf{C}^d \otimes \mathbf{C}^d$.

Theorem 4.1. *There exist universal constants $c_0, C > 0$ s.t. with probability greater than $1 - e^{-c_0 d}$,*

$$\|\rho - \sigma\|_{\underline{\mathbf{LOCC}}^{\rightarrow}} = 2 \;\; \textit{and} \;\; \|\rho - \sigma\|_{\underline{\mathbf{LO}}} \leqslant \frac{C}{\sqrt{d}}.$$

Examples of state pairs that local measurements can distinguish perfectly if one-way classical communication is allowed between the two parties, but very poorly if not.

Main steps in the proof:
- $\|\rho - \sigma\|_{\underline{\mathbf{LOCC}}^{\rightarrow}} = \frac{1}{d}\sum_{i=1}^d \|\rho_i - \sigma_i\|_1$, and for each $1 \leqslant i \leqslant d$, $\|\rho_i - \sigma_i\|_1 = 2$.
- $\|\rho - \sigma\|_{\underline{\mathbf{LO}}} = \frac{1}{d}\sup\left\{\sum_{i=1}^d \|\rho_i - \sigma_i\|_{\mathrm{M}} \;:\; \mathrm{M}\ \text{POVM on}\ \mathbf{C}^d\right\}$
  - ⋆ Existence of a net $\mathcal{R}$ of "reasonable" size in the set of POVMs on $\mathbf{C}^d$.
  - ⋆ For each $\mathrm{M} \in \mathcal{R}$ and each $1 \leqslant i \leqslant d$, $\mathbf{E}\|\rho_i - \sigma_i\|_{\mathrm{M}} \leqslant 2/\sqrt{d}$ [1].
  - ⋆ Berstein type bound on the large deviation probability from its average of a sum of independent ψ_1 random variables [3].

Applications to quantum data-locking: The states ρ and σ exhibit characteristic features of data-locking states [5, 7], i.e. states whose accessible mutual information (the maximum classical mutual information achievable by local measurements) drastically underestimates their quantum mutual information.

5 Typical performance of LOCC, SEP and PPT measurements in distinguishing two bipartite states

Theorem 5.1. *There exist universal constants $c_0, c, C > 0$ s.t. for ρ, σ random states on $\mathbf{C}^d \otimes \mathbf{C}^d$ (picked independently and uniformly), with probability greater than $1 - e^{-c_0 d^2}$,*

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

In comparison, $\|\rho - \sigma\|_{\underline{\mathbf{ALL}}} = \|\rho - \sigma\|_1$ is typically of order 1. So the PPT constraint only affects observers' discriminating ability by a constant factor, whereas the LOCC or SEP constraints imply a dimensional loss.
$\rightarrow$ Data-hiding is generic [9] (e.g. there exists a set of e^{cd} states on $\mathbf{C}^d \otimes \mathbf{C}^d$, for some universal constant $c > 0$, which are pairwise data-hiding).

Main steps in the proof:
- Estimate on the mean-width of the convex bodies associated to $\underline{\mathbf{PPT}}$, $\underline{\mathbf{SEP}}$ and $\underline{\mathbf{LOCC}}$ on $\mathbf{C}^d \otimes \mathbf{C}^d$:
$\begin{cases} K_{\underline{\mathbf{PPT}}} = [-\mathrm{Id}, \mathrm{Id}] \cap [-\mathrm{Id}, \mathrm{Id}]^\Gamma \\ K_{\underline{\mathbf{SEP}}} = \{2\mathbf{R}^+\mathcal{S} - \mathrm{Id}\} \cap -\{2\mathbf{R}^+\mathcal{S} - \mathrm{Id}\} \end{cases}$, therefore $\begin{cases} w(K_{\underline{\mathbf{PPT}}}) \simeq d \\ w(K_{\underline{\mathbf{SEP}}}) \simeq \sqrt{d} \end{cases}$, and the size of $K_{\underline{\mathbf{LOCC}}}$ is comparable to that of $K_{\underline{\mathbf{SEP}}}$ (geometric arguments [16, 14, 2]: volume of symmetrizations and intersections).
- ρ, σ independent uniformly distributed states on $\mathbf{C}^d \otimes \mathbf{C}^d$:
  - ⋆ Estimate on the expected value $\mathbf{E}$ of $\|\rho - \sigma\|_{\underline{\mathrm{M}}}$: by comparing averages over different ensembles of traceless random matrices, $\mathbf{E} \simeq w(K_{\underline{\mathrm{M}}})/d$.
  - ⋆ Estimate on the probability that $\|\rho - \sigma\|_{\underline{\mathrm{M}}}$ deviates from $\mathbf{E}$: by concentration of measure for lipschitz functions on a sphere $\mathbf{P}\left(\left|\|\rho - \sigma\|_{\underline{\mathrm{M}}} - \mathbf{E}\right| > t\right) \leqslant e^{-cd^2t^2}$.

Applications to quantum data-hiding: E a random $d^2/2$-dimensional subspace of $\mathbf{C}^d \otimes \mathbf{C}^d$.
$\rho = \frac{P_E}{d^2/2}$ and $\sigma = \frac{P_{E^\perp}}{d^2/2}$ are s.t. $\|\rho - \sigma\|_{\underline{\mathbf{ALL}}} = 2$, and with high probability $\begin{cases} \|\rho - \sigma\|_{\underline{\mathbf{PPT}}} \simeq 1 \\ \|\rho - \sigma\|_{\underline{\mathbf{SEP}}} \simeq 1/\sqrt{d} \end{cases}$.
$\rightarrow$ Examples of orthogonal states that are with high probability data-hiding for SEP POVMs but not data-hiding for PPT POVMs (in contrast with Werner states which are equally SEP and PPT data-hiding).

6 Summary, generalizations and open questions

Norm hierarchy	$\|\cdot\|_{\underline{\mathbf{LO}}} \leqslant$	$\|\cdot\|_{\underline{\mathbf{LOCC}}^{\rightarrow}} \leqslant$	$\|\cdot\|_{\underline{\mathbf{LOCC}}} \leqslant$	$\|\cdot\|_{\underline{\mathbf{SEP}}} \leqslant$	$\|\cdot\|_{\underline{\mathbf{PPT}}} \leqslant$	$\|\cdot\|_{\underline{\mathbf{ALL}}}$
Existing unbounded gap?	yes	yes	?	yes	yes	
Generic unbounded gap?	?	no	no	yes	no	

- **Generalizations to the multipartite case:**
On $(\mathbf{C}^d)^{\otimes k}$ with k fixed and $d \rightarrow +\infty$ (small number of large subsystems):
  - ⋆ $\|\rho - \sigma\|_{\underline{\mathbf{PPT}}}$ is of order 1, as $\|\rho - \sigma\|_{\underline{\mathbf{ALL}}}$, whereas $\|\rho - \sigma\|_{\underline{\mathbf{SEP}}}$ is of order $1/\sqrt{d^{k-1}}$.
  - ⋆ Imposing biseparability across every bipartition is roughly the same as imposing biseparability across one bipartition, while imposing full separability is a much tougher constraint.

$\rightarrow$ But what about the opposite high-dimensional setting, i.e. $k \rightarrow +\infty$ and d fixed (large number of small subsystems)?

- Generically, two-way over one-way classical communication does not present a marked improvement, but does one-way over no classical communication gives a clear advantage?
$\rightarrow$ Is the typical behaviour of $\|\cdot\|_{\underline{\mathbf{LO}}}$ of the same order as $\|\cdot\|_{\underline{\mathbf{LOCC}}^{\rightarrow}}$ or much smaller? [4]

- Typical behaviour of other "filtered through measurements" distances, such as measured relative entropy or measured fidelity [15] (and their regularised versions)?

References

[1] **G. Aubrun, C. Lancien**, "Zonoids and sparsification of quantum measurements".
[2] **G. Aubrun, S.J. Szarek**, "Tensor product of convex sets and the volume of separable states on N qudits".
[3] **D. Chafaï, O. Guédon, G. Lecué, A. Pajor**, *Interactions between compressed sensing, random matrices and high dimensional geometry*.
[4] **E. Chitambar, M-H. Hsieh**, "Asymptotic state discrimination and a strict hierarchy in distinguishability norms".
[5] **D.P. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, B.M. Terhal**, "Locking classical correlation in quantum states".
[6] **D.P. DiVincenzo, D. Leung, B.M. Terhal**, "Quantum Data Hiding".
[7] **F. Dupuis, J. Florjanczyk, P. Hayden, D. Leung**, "Locking classical information".
[8] **T. Eggeling, R.F. Werner**, "Hiding classical data in multi-partite quantum states".
[9] **P. Hayden, D. Leung, P. Shor, A. Winter**, " Randomizing quantum states: Constructions and applications".
[10] **C.W. Helstrom**, *Quantum detection and estimation theory*.
[11] **A.S. Holevo**, "Statistical decision theory for quantum systems".
[12] **C. Lancien, A. Winter**, "Distinguishing multi-partite states by local measurements".
[13] **W. Matthews, S. Wehner, A. Winter**, "Distinguishability of quantum states under restricted families of measurements with an application to data hiding".
[14] **V.D. Milman, A. Pajor**, "Entropy and asymptotic geometry of non-symmetric convex bodies".
[15] **M. Piani**, "Relative entropy of entanglement and restricted measurements".
[16] **G. Pisier**, *The Volume of Convex Bodies and Banach Spaces Geometry*.