Distinguishability norms on high-dimensional quantum systems

Approximating POVMs & Locally restricted POVMs on multipartite systems

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 project OSQPI.

Université Claude Bernard Lyon 1
UAB Universitat Autònoma de Barcelona

17th QIP, Barcelona, February 3-7 2014

1 Distinguishability norms and quantum state discrimination

System that can be in 2 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 outcomes of a POVM $\mathrm{M}=(M_i)_{i\in I}$ performed on it.

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) [14].

2 Distinguishability norms and convex geometry

Definition 2.1. *POVM $\mathrm{M}=(M_i)_{i\in I}$ on $\mathbf{C}^d$ (I discrete or not): $\forall\, i\in I,\ M_i\in\mathcal{H}_+(\mathbf{C}^d)$ and $\sum_{i\in I}M_i=\mathrm{Id}$.*

Associated distinguishability (semi-)norm: $\forall\,\Delta\in\mathcal{H}(\mathbf{C}^d),\ \|\Delta\|_{\mathrm{M}}:=\sum_{i\in I}|\,\mathrm{Tr}\,(\Delta M_i)|$.

Associated convex body K_{M}: dual of the unit ball for $\|\cdot\|_{\mathrm{M}}$ (i.e. unit ball for the norm dual to $\|\cdot\|_{\mathrm{M}}$).

Problem: What "kinds" of convex bodies are associated to POVMs?

Theorem 2.2. *Equivalence between*

K_{M} zonotope in $\mathcal{H}(\mathbf{C}^d)$ s.t. $\pm\mathrm{Id}\in K_{\mathrm{M}}$ and $K_{\mathrm{M}}\subset[-\mathrm{Id},\mathrm{Id}]$	*M discrete POVM on $\mathbf{C}^d$*
K_{M} zonoid in $\mathcal{H}(\mathbf{C}^d)$ s.t. $\pm\mathrm{Id}\in K_{\mathrm{M}}$ and $K_{\mathrm{M}}\subset[-\mathrm{Id},\mathrm{Id}]$	*M general POVM on $\mathbf{C}^d$*

Definition 2.3. *Zonotope: symmetric convex body which can be written as a finite Minkowski sum of segments.*
Zonoid: symmetric convex body which can be approximated in Hausdorff distance by zonotopes.

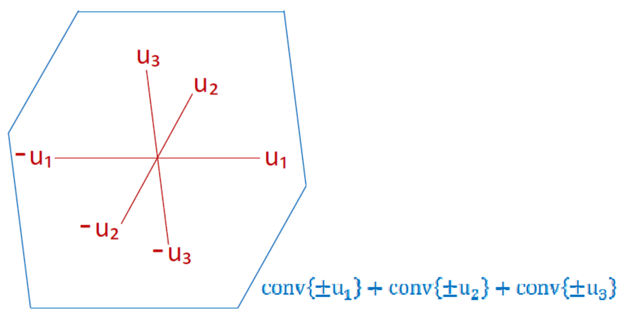

Figure 1: A zonotope in $\mathbf{R}^2$.

3 Approximating any POVM by a POVM with "few" outcomes

A new "dictionary" between quantum information and convex geometry

Zonotope in $\mathbf{R}^n$	K_{M} for a discrete POVM M on $\mathbf{C}^d$
Zonoid in $\mathbf{R}^n$	K_{M} for a general POVM M on $\mathbf{C}^d$
"Most symmetric" zonoid in $\mathbf{R}^n$ = Euclidean ball B_2^n	"Most symmetric" POVM on $\mathbf{C}^d$ = Uniform POVM U Dimension-independent equivalence between the distinguishability norm $\|\Delta\|_{\mathrm{U}}=d\int_{\|\psi\rangle\in S_2(\mathbf{C}^d)}\|\langle\psi\|\Delta\|\psi\rangle\|\mathrm{d}\psi$ and the Euclidean norm $\|\Delta\|_{2(1)}:=\sqrt{\mathrm{Tr}(\Delta^2)+(\mathrm{Tr}\,\Delta)^2}$ [13]: $\frac{1}{\sqrt{18}}\|\cdot\|_{2(1)}\leqslant\|\cdot\|_{\mathrm{U}}\leqslant\|\cdot\|_{2(1)}$.
Rudin (1967) [17]: Explicit construction of a zonotope Z in $\mathbf{R}^n$ which is the sum of $O(n^2)$ segments and s.t. $\frac{1}{C}Z\subset B_2^n\subset CZ.$	A 4-design POVM on $\mathbf{C}^d$ is already a "good" discretization of the uniform POVM, which has $\Omega(d^4)$ and $O(d^8)$ outcomes [1]. Explicit construction of an approximate 4-design POVM M on $\mathbf{C}^d$ s.t. $\frac{1}{C}\|\cdot\|_{\mathrm{U}}\leqslant\|\cdot\|_{\mathrm{M}}\leqslant C\|\cdot\|_{\mathrm{U}}$.
Figiel-Lindenstrauss-Milman (1977) [8]: A zonotope Z in $\mathbf{R}^n$ which is the sum of $O_\varepsilon(n)$ independent uniformly distributed random segments satisfies with high probability $(1-\varepsilon)Z\subset B_2^n\subset(1+\varepsilon)Z.$	**Theorem 3.1.** *A POVM M made of $O_\varepsilon(d^2)$ independent uniformly distributed rank-1 projectors (appropriately renormalized) satisfies with high probability* $(1-\varepsilon)\|\cdot\|_{\mathrm{U}}\leqslant\|\cdot\|_{\mathrm{M}}\leqslant(1+\varepsilon)\|\cdot\|_{\mathrm{U}}$. **Remark 3.2.** *Optimal dimensional order of magnitude: a POVM on $\mathbf{C}^d$ must have at least d^2 outcomes to be informationally complete.* **Main steps in the proof:** • Bernstein-type large deviation inequality for a sum of i.i.d centered ψ_1 r.v. (i.e. with sub-exponential tail) $\rightarrow$ Individual error term. • Net argument $\rightarrow$ Global error term.
Talagrand (1990) [18, 3]: Given any zonoid Y in $\mathbf{R}^n$, there exists a zonotope Z in $\mathbf{R}^n$ which is the sum of $O_\varepsilon(n\log n)$ segments and s.t. $Z\subset Y\subset(1+\varepsilon)Z.$	**Theorem 3.3.** *Given any POVM N on $\mathbf{C}^d$, there exists a sub-POVM M with $O_\varepsilon(d^2\log d)$ outcomes s.t.* $(1-\epsilon)\|\cdot\|_{\mathrm{N}}\leqslant\|\cdot\|_{\mathrm{M}}\leqslant\|\cdot\|_{\mathrm{N}}$.

Remark 3.4. ***The case of the local uniform POVM** $\mathrm{LU}=\mathrm{U}_1\otimes\cdots\otimes\mathrm{U}_k$ **on** $\mathbf{C}^{d_1}\otimes\cdots\otimes\mathbf{C}^{d_k}\equiv\mathbf{C}^d$**:***
Dimension-independent equivalence between $\|\cdot\|_{\mathrm{LU}}$ and a Euclidean norm (k-partite analog of $\|\cdot\|_{2(1)}$) [13].
$\rightarrow$ Existence of a separable rank-1 sub-POVM M with $O_\varepsilon(d^2)$ outcomes s.t. $(1-\varepsilon)\|\cdot\|_{\mathrm{LU}}\leqslant\|\cdot\|_{\mathrm{M}}\leqslant\|\cdot\|_{\mathrm{LU}}$.

Applications: "Good" distinguishing power of U and LU $\Rightarrow$ Bounds on the dimensionality reduction of quantum states [9], quasi-polynomial time algorithm to solve the WMP for separability [4] etc.
$\rightarrow$ Importance of being able to exhibit "implementable" POVMs already achieving near-to-optimal discrimination efficiency.

Open questions:
• Approximation of any POVM on $\mathbf{C}^d$ by a POVM, instead of a sub-POVM, with $\Theta(d^2)$, instead of $\Theta(d^2\log d)$, outcomes?
• Explicit construction of such POVM? (derandomization: expander codes, pseudorandom generators etc.)

4 "Typical" performance of PPT and separable measurements in distinguishing two bipartite states

Definition 4.1. *Let $\mathbf{M}$ be a set of POVMs on $\mathbf{C}^d$. The associated distinguishability (semi-)norm is*

$$\|\cdot\|_{\mathbf{M}}:=\sup_{\mathrm{M}\in\mathbf{M}}\|\cdot\|_{\mathrm{M}},$$

and the associated convex body is

$$K_{\mathbf{M}}=\mathrm{conv}\left(\bigcup_{\mathrm{M}\in\mathbf{M}}K_{\mathrm{M}}\right).$$

Mean-width of $K_{\mathbf{M}}$: $w(K_{\mathbf{M}}):=\int_{S_{HS}(\mathbf{C}^d)}\|\Delta\|_{\mathbf{M}}\mathrm{d}\sigma(\Delta)$.

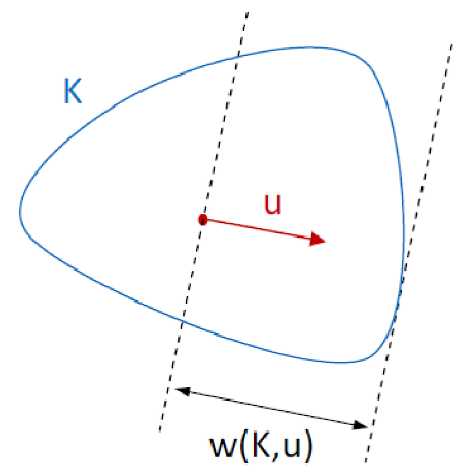

Figure 2: Mean-width of a convex body K in $\mathbf{R}^n$: $w(K)=\int_{u\in S_2^{n-1}}w(K,u)\mathrm{d}u$.

Problem: Seminal observation in quantum state discrimination [11, 12]: $\|\cdot\|_{\mathbf{ALL}}=\|\cdot\|_1$.
But on a multipartite system, there are locality constraints on the set $\mathbf{M}$ of POVMs that experimenters are able to implement: $\mathbf{LOCC}\subset\mathbf{SEP}\subset\mathbf{PPT}$.
$\rightarrow$ How do these restrictions affect their distinguishing power? $\|\cdot\|_{\mathbf{M}}\simeq\|\cdot\|_1$ or $\|\cdot\|_{\mathbf{M}}\ll\|\cdot\|_1$?

Motivation: Existence of data-hiding states on multipartite systems [6, 7] 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 $\mathbf{C}^d\otimes\mathbf{C}^d$, $\sigma=\frac{1}{d^2+d}(\mathrm{Id}+\mathrm{F})$ and $\alpha=\frac{1}{d^2-d}(\mathrm{Id}-\mathrm{F})$.
$\Delta=\sigma-\alpha$ is s.t. $\|\Delta\|_{\mathbf{LOCC}}\leqslant\|\Delta\|_{\mathbf{SEP}}=\|\Delta\|_{\mathbf{PPT}}=\frac{4}{d+1}\ll2=\|\Delta\|_1$.

Theorem 4.2. *There exist $c_0,c,C>0$ s.t. for ρ,σ random states on $\mathbf{C}^d\otimes\mathbf{C}^d$ (picked independently and uniformly), with probability greater than $1-e^{-c_0d^2}$,*

$$c\leqslant\|\rho-\sigma\|_{\mathbf{PPT}}\leqslant C\ \text{ and }\ \frac{c}{\sqrt{d}}\leqslant\|\rho-\sigma\|_{\mathbf{SEP}}\leqslant\frac{C}{\sqrt{d}}.$$

In comparison, $\|\rho-\sigma\|_{\mathbf{ALL}}=\|\rho-\sigma\|_1$ is typically of order 1. So the PPT constraint only affects observers' discriminating ability by a constant factor, whereas the separability one implies a dimensional loss.
$\rightarrow$ Data-hiding is "generic" [10].

Main steps in the proof:
• Estimate on the mean-width of the convex bodies associated to $\mathbf{PPT}$ and $\mathbf{SEP}$ on $\mathbf{C}^d\otimes\mathbf{C}^d$:
$K_{\mathbf{PPT}}=[-\mathrm{Id},\mathrm{Id}]\cap[-\mathrm{Id},\mathrm{Id}]^{\Gamma}$ and $K_{\mathbf{SEP}}=\{2\mathbf{R}^+\mathcal{S}-\mathrm{Id}\}\cap-\{2\mathbf{R}^+\mathcal{S}-\mathrm{Id}\}$, so by "volumic" arguments [16, 15, 2] $w(K_{\mathbf{PPT}})\simeq d$ and $w(K_{\mathbf{SEP}})\simeq\sqrt{d}$.
• ρ,σ independent uniformly distributed states on $\mathbf{C}^d\otimes\mathbf{C}^d$:
⋆ Estimate on the expected value $\mathbf{E}$ of $\|\rho-\sigma\|_{\mathbf{M}}$: by comparing random-matrix ensembles $\mathbf{E}\simeq\frac{w(K_{\mathbf{M}})}{d}$.
⋆ Estimate on the probability that $\|\rho-\sigma\|_{\mathbf{M}}$ deviates from $\mathbf{E}$: by concentration of measure for lipschitz functions on a sphere $\mathbf{P}\left(\left|\|\rho-\sigma\|_{\mathbf{M}}-\mathbf{E}\right|>t\right)\leqslant e^{-cd^2t^2}$.

Applications to quantum data-hiding: Let E be 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. $\|\rho-\sigma\|_{\mathbf{ALL}}=2$, and with high probability $\begin{cases}\|\rho-\sigma\|_{\mathbf{PPT}}\simeq1\\ \|\rho-\sigma\|_{\mathbf{SEP}}\simeq1/\sqrt{d}\end{cases}$.
$\rightarrow$ Examples of orthogonal states that are with high probability data-hiding for separable measurements but not data-hiding for PPT measurements (in contrast with Werner states which are equally separable and PPT data-hiding).

Open questions:
• Typical behaviour of $\|\cdot\|_{\mathbf{LOCC}}$? Of the same order as $\|\cdot\|_{\mathbf{SEP}}$ or much smaller? [5]
• **Generalization to the multipartite case** $(\mathbf{C}^d)^{\otimes k}$**:**
If k is fixed and $d\rightarrow+\infty$ ("small" number of "large" subsystems), then $\|\rho-\sigma\|_{\mathbf{PPT}}$ is of order 1, as $\|\rho-\sigma\|_{\mathbf{ALL}}$, whereas $\|\rho-\sigma\|_{\mathbf{SEP}}$ is of order $1/\sqrt{d^{k-1}}$ (same techniques as in the bipartite case).
But what about the opposite high-dimensional setting, i.e. $k\rightarrow+\infty$ and d fixed ("large" number of "small" subsystems)?

References

[1] **A. Ambainis, J. Emerson.**, "Quantum t-designs: t-wise independence in the quantum world".
[2] **G. Aubrun, S.J. Szarek**, "Tensor product of convex sets and the volume of separable states on N qudits".
[3] **J. Bourgain, J. Lindenstrauss, V. Milman**, "Approximation of zonoids by zonotopes".
[4] **F.G.S.L. Brandão, M. Christandl, J.T. Yard**, "Faithful Squashed Entanglement".
[5] **E. Chitambar, M-H. Hsieh**, "Asymptotic state discrimination and a strict hierarchy in distinguishability norms";
[6] **D.P. DiVincenzo, D. Leung, B.M. Terhal**, "Quantum Data Hiding".
[7] **T. Eggeling, R.F. Werner**, "Hiding classical data in multi-partite quantum states".
[8] **T. Figiel, J. Lindenstrauss, V.D. Milman**, "The dimension of almost spherical sections of convex bodies".
[9] **A.W. Harrow, A. Montanaro, A.J. Short**, "Limitations on quantum dimensionality reduction".
[10] **P. Hayden, D. Leung, P. Shor, A. Winter**, " Randomizing quantum states: Constructions and applications".
[11] **C.W. Helstrom**, *Quantum detection and estimation theory*.
[12] **A.S. Holevo**, "Statistical decision theory for quantum systems".
[13] **C. Lancien, A. Winter**, "Distinguishing multi-partite states by local measurements".
[14] **W. Matthews, S. Wehner, A. Winter**, "Distinguishability of quantum states under restricted families of measurements with an application to data hiding".
[15] **V.D. Milman, A. Pajor**, "Entropy and asymptotic geometry of non-symmetric convex bodies".
[16] **G. Pisier**, *The Volume of Convex Bodies and Banach Spaces Geometry*.
[17] **W. Rudin**, *Trigonometric series with gaps*.
[18] **M. Talagrand**, "Embedding subspaces of L_1 into ℓ_1^N".