Distinguishing multi-partite quantum states by local measurements

Final report of a research project achieved at the University of Bristol (United-Kingdom) from April 2nd to July 7th 2012 under the supervision of Prof Andreas Winter

Cécilia LANCIEN
Ecole Polytechnique Paris (France)

September 1st 2012

My Master degree research placement was carried out in the Mathematics Department of the University of Bristol (United-Kingdom) under the supervision of Andreas Winter, professor in the Quantum Computation and Information Group there at that time.

One could say that the starting point of the work achieved during that period was the paper by W. Matthews, A. Winter and S. Wehner [11]. In the latter, interesting results were stated regarding the distinguishability of quantum states under certain classes of measurements, in the special cases of single and bi partite quantum systems. No generalization to systems consisting of any number of parties had been found since then though, and looking closer at this open question was one of the main purposes of the project.
Our search turned out to end up quite fruitfully. The various results obtained indeed gave rise to the paper [33], submitted to Communications in Mathematical Physics, and published for now in extended abstract form in the Proceedings of the Asian Quantum Information Science Conference 2012 where they were exposed (August $23^{\text{rd}} - 26^{\text{th}}$ 2012, Suzhou, China). So of course, most of the new material presented in this report already appears in [33], even though sometimes from a slightly different approach. I would however describe the "spirit" of those two pieces of writing as being quite different. I tried here to come to a more self-contained account, including for instance in that end a more detailed description of the mathematical background our work relies on.

The remainder of this report is thus organized as follows.
Section 1 might be seen as a panorama (though definitely full of gaps) of the mathematical framework in which quantum physics and quantum information theories develop. In section 2, the general issue we have been concerned with, namely the one of distinguishing quantum states under some allowed measurements, is precisely stated. Section 3 is devoted to describing one specific type of measurement we got particularly interested in, mainly because of its nice symmetry properties. Surrounding results, not directly useful to our purpose but presumably of independent interest, are included there. To conclude this "preparatory" work, section 4 is aimed at explaining the sort of restrictions measurements on a multi-partite quantum system might be subject to, due basically to locality constraints. Then, in section 5, several quantitative results are proven regarding the capacity observers may have of discriminating between two multi-partite quantum states when they are only able to perform certain highly symmetric measurements on their own party. In section 6 eventually, not one but whole classes of locally restricted measurements are considered. To finish with, section 7 provides a summary of the various results obtained and a few open questions, among many non-cited others.
Appendices A, B and C present required mathematical tools from three distinct areas : the one of Hilbert spaces' geometry, the one of groups' linear representations, and the one of Von-Neumann algebras respectively. They contain more than the strictly necessary ideas, but nevertheless remain far from being exhaustive. As for appendix D, it is of completely different kind : an alternative way of proving one of our main results is given, and extended to some broader considerations.

Contents

1 Introduction : The postulates of quantum mechanics and its mathematical formalism

Quantum mechanics does not tell what laws a physical system must obey but only provides a conceptual framework for the development of such laws. It relies on a few basic postulates which connect the physical world to the mathematical formalism that enables its description. The reader is referred to [1] for a general and detailed reference on this topic, the account made here being clearly minimalist.

Postulate 1 : Associated to any isolated physical system is a Hilbert space $\mathcal{H}$ known as its *state space*. The system is then completely described by its *state*, or *density operator*, which is a positive (hence Hermitian) operator with trace one acting on $\mathcal{H}$.
A state ρ is said to be *pure* if there exists $|\psi\rangle \in \mathcal{H}$ such that $\rho = |\psi\rangle\langle\psi|$. It is otherwise referred to as being *mixed*.
If a system is known to be in state ρ_i with probability p_i for $i \in I$, then it may be described by the density operator $\rho = \sum_{i\in I} p_i\rho_i$ which is called a *mixture* of the density operators ρ_i.

Postulate 2 : The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have K sub-systems, numbered 1 through K, with sub-system i in state ρ_i for all $1 \leq i \leq K$, then the joint state of the total system is $\rho_1 \otimes \cdots \otimes \rho_n$.

Postulate 3 : The evolution of a closed quantum system (i.e. a system that is not interacting in any way with other systems) is described by a *unitary transformation* : if the system is in state ρ at time t and in state ρ' at time t', then there exists a unitary operator U acting on the system's state space (that depends only on t and t', not on ρ and ρ') such that $\rho' = U\rho U^\dagger$.

Postulate 4 : A quantum measurement performed on a physical system is described by a set $\{M_i, i \in I\}$ of *Positive Operator-Valued Measure (POVM) elements*, which are positive operators acting on the system's state space satisfying the *completeness equation* $\sum_{i\in I} M_i = \mathbb{1}$ (where $\mathbb{1}$ is the identity operator).
The index $i \in I$ refers to the measurement outcomes that may occur in the experiment. If the state of the system immediately before the measurement is ρ, then, for all $i \in I$, the probability that result i occurs is given by $\mathbb{P}_\rho(i) = \mathrm{Tr}(M_i\rho)$ (so that the completeness equation simply expresses the fact that probabilities sum to one). The fact that each state ρ generates a probability distribution $\mathbb{P}_\rho$ on the outputs $i \in I$ of a given measurement $\{M_i, i \in I\}$ is known as the *Born rule for measurements*.
We can actually be more precise : M_i being positive, $\sqrt{M_i}$ is well defined (*cf* Appendix A.1), and the state of the system just after the measurement that yielded outcome i is $\dfrac{\sqrt{M_i}\rho\sqrt{M_i}^\dagger}{\mathrm{Tr}(M_i\rho)}$.

It may be pointed out that the free evolution $\rho \mapsto U\rho U^\dagger$ and the measurement $\rho \mapsto \dfrac{\sqrt{M}\rho\sqrt{M}^\dagger}{\mathrm{Tr}(M\rho)}$ are two particular examples of *quantum operations*, i.e. operations that transform a quantum state into another. The most general way of describing such transformations is by a *Completely Positive and Trace Preserving (CPTP)* map.

- $\Lambda : \mathcal{M}_m(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C})$ is *Completely Positive (CP)* if :

$$\forall\ p \in \mathbb{N},\ \forall\ \rho \in \mathcal{M}_{m\times p}(\mathbb{C}),\ \rho \geq \mathbb{0}_{m\times p} \Rightarrow (\Lambda \otimes \mathbb{1}_p)(\rho) \geq \mathbb{0}_{n\times p}$$

  $\mathbb{C}^m$ here describes the state space of the input principal system and $\mathbb{C}^n$ the state space of the output principal system, whereas $\mathbb{C}^p$ should be thought of as the state space of any environment the system of interest might be coupled with. Thus, positivity of operators on the space of the global composite system is preserved when applying Λ to the part that acts on the principal system's space and leaving the part that acts on the environment's space invariant.

- $\Lambda : \mathcal{M}_m(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C})$ is *Trace Preserving (TP)* if :

$$\forall\ \rho \in \mathcal{M}_m(\mathbb{C}),\ \rho \geq \mathbb{0}_m \Rightarrow \mathrm{Tr}\Lambda(\rho) = \mathrm{Tr}\rho$$

Λ being a CPTP map is actually equivalent to the existence of so-called *Kraus operators* $(V_i)_{i\in I}$ that satisfy the completeness relation $\sum_{i\in I} V_i V_i^\dagger = \mathbb{1}$ and that are such that Λ can be written in the operator-sum representaion as $\Lambda(\rho) = \sum_{i\in I} V_i \rho V_i^\dagger$.

2 The general problem of distinguishing two quantum states under restricted families of measurements

2.1 Error probability and bias of a single POVM on a state pair

We consider the situation where a system (with associated Hilbert space $\mathcal{H}$ of finite dimension N) can be either in state ρ or in state σ, with equal prior probabilities $\frac{1}{2}$. We would like to guess with the smallest probability of error in which of those two states it is by only performing one given POVM $(M_i)_{i\in I}$ on it. We therefore base our decision on the so-called *maximum likelihood rule*. That is : knowing that $\mathrm{Tr}(M_i\rho) > \mathrm{Tr}(M_i\sigma)$ for $i \in \widetilde{I}$ and $\mathrm{Tr}(M_i\rho) < \mathrm{Tr}(M_i\sigma)$ for $i \in I \setminus \widetilde{I}$, we decide on ρ if outcome $i \in \widetilde{I}$ is observed and on σ otherwise. The probability of error is thus, denoting by s the random variable "effective state of the system" and by d the random variable "state of the system we decide to be more likely after carrying out the measurement" :

$$\begin{aligned} P_E =& \mathbb{P}(s=\sigma, d=\rho) + \mathbb{P}(s=\rho, d=\sigma) \\ =& \mathbb{P}(s=\sigma)\mathbb{P}(d=\rho|s=\sigma) + \mathbb{P}(s=\rho)\mathbb{P}(d=\sigma|s=\rho) \\ =& \frac{1}{2}\sum_{i\in\widetilde{I}} \mathrm{Tr}(M_i\sigma) + \frac{1}{2}\sum_{i\in I\setminus\widetilde{I}} \mathrm{Tr}(M_i\rho) \end{aligned}$$

Defining M as $M := \sum_{i\in\widetilde{I}} M_i$ (and hence $\mathbb{1}_{\mathcal{H}} - M$ as $\mathbb{1}_{\mathcal{H}} - M := \sum_{i\in I\setminus\widetilde{I}} M_i$ since $\sum_{i\in I} M_i = \mathbb{1}_{\mathcal{H}}$) the probability of error takes value : $P_E = \frac{1}{2}\mathrm{Tr}(M\sigma) + \frac{1}{2}\mathrm{Tr}((\mathbb{1}_{\mathcal{H}} - M)\rho) = \frac{1}{2} - \frac{1}{2}\mathrm{Tr}(M(\rho-\sigma))$, where we just used that $\mathrm{Tr}\rho = 1$ in the last step.

Denoting by $\{|i\rangle, i \in I\}$ an orthonormal basis of $\mathbb{C}^{|I|}$, we define the CPTP map (from the set of Hermitian matrices on $\mathcal{H}$ to the set of Hermitian matrices on $\mathbb{C}^{|I|}$) associated with $(M_i)_{i\in I}$ by :

$$\mathcal{M} : \Delta \mapsto \sum_{i\in I} \mathrm{Tr}(M_i\Delta)|i\rangle\langle i|$$

We thus have, for $\Delta := \rho - \sigma$:
$\|\mathcal{M}(\Delta)\|_1 = \sum_{i\in I} |\mathrm{Tr}(M_i\Delta)| = \sum_{i\in\widetilde{I}} \mathrm{Tr}(M_i\Delta) - \sum_{i\in I\setminus\widetilde{I}} \mathrm{Tr}(M_i\Delta) = \mathrm{Tr}(M\Delta) - \mathrm{Tr}((\mathbb{1}_{\mathcal{H}} - M)\Delta) = 2\mathrm{Tr}(M\Delta)$
We only used here first that, by assumption, $\mathrm{Tr}(M_i\Delta) > 0$ for $i \in \widetilde{I}$ and $\mathrm{Tr}(M_i\Delta) < 0$ for $i \in I \setminus \widetilde{I}$, and then that $\mathrm{Tr}\Delta = 0$.

So in the end, the probability of error when trying to discriminate state ρ from state σ by performing the POVM $(M_i)_{i\in I}$ may be written as :

$$P_E = \frac{1}{2} - \frac{1}{2}\left\|\mathcal{M}\left(\frac{1}{2}\rho - \frac{1}{2}\sigma\right)\right\|_1$$

The quantity $\left\|\mathcal{M}\left(\frac{1}{2}\rho - \frac{1}{2}\sigma\right)\right\|_1$ is therefore called the *bias* of the POVM $(M_i)_{i\in I}$ on the state pair (ρ, σ).

Remark 2.1 *We can easily generalize the discrimination task described above to states ρ and σ with non necessarily equal prior probabilities, q and $1-q$ respectively. Indeed, the only change in that case is that we are now dealing with the general Hermitian matrix $q\rho-(1-q)\sigma$ instead of the traceless one $\frac{1}{2}\rho-\frac{1}{2}\sigma$. So for instance, the probability of error is then equal to :*

$$P_E = \frac{1}{2} - \frac{1}{2}\big\|\mathcal{M}(q\rho-(1-q)\sigma)\big\|_1$$

This result is actually nothing more than the generalization of a classical statistics' result in hypothesis testing (see for instance [2] for a general reference). There, the optimal discrimination between two hypotheses modelled as probability distributions $\{P(i), i\in I\}$ and $\{Q(i), i\in I\}$, with prior probabilities q and $1-q$ respectively, is in fact given by the maximum likelihood rule, so that the minimum probability of error takes value : $P_E = \frac{1}{2} - \frac{1}{2}\big\|qP-(1-q)Q\big\|_1$, where $\|f\|_1 := \sum_{i\in I}|f(i)|$.

2.2 Maximum bias achievable by a set of POVMs : distinguishability norms

We are now interested in looking at the maximum bias achievable on a state pair (ρ,σ) (which corresponds to the minimum probability of error when trying to discriminate between states ρ and σ) when we are allowed POVMs in a given set $\mathbf{M}$. We will denote it by :

$$\left\|\frac{1}{2}\rho-\frac{1}{2}\sigma\right\|_{\mathbf{M}} := \max_{(M_i)_{i\in I}\in\mathbf{M}}\left\|\mathcal{M}\left(\frac{1}{2}\rho-\frac{1}{2}\sigma\right)\right\|_1$$

Remark 2.2 *The notation $\|\cdot\|_{\mathbf{M}}$ seems to presume that the quantity we defined above is a norm. It is actually, whatever the set of POVMs $\mathbf{M}$, a semi-norm : it is non-negative, homogeneous and obeys the triangle inequality. It may however vanish on a non-zero matrix $\Delta\neq\mathbb{0}_{\mathcal{H}}$ in the general case. This is excluded when the set of POVMs $\mathbf{M}$ is informationally complete, i.e. when for any matrix $\Delta\neq\mathbb{0}_{\mathcal{H}}$ there exists a POVM $(M_i)_{i\in I}\in\mathbf{M}$ and an index $i_0\in I$ such that $Tr(M_{i_0}\Delta)\neq 0$. This is equivalent to demanding that the operators M_i, $i\in I$, $(M_i)_{i\in I}\in\mathbf{M}$, span the whole space $\mathcal{F}(\mathcal{H})\equiv\mathcal{M}_N(\mathbb{C})$ of linear operators on $\mathcal{H}$: Span$(\{M_i, i\in I, (M_i)_{i\in I}\in\mathbf{M}\}) = \mathcal{M}_N(\mathbb{C})$ (so that any density operator ρ on $\mathcal{H}$ can be reconstructed from its outcome statistics $\{Tr(M_i\rho), i\in I, (M_i)_{i\in I}\in\mathbf{M}\}$ when measures from the set $\mathbf{M}$ are carried on, which justifies the designation informationally complete). This especially implies that the total number of (distinct) POVM elements in $\mathbf{M}$ is greater than $N^2 = dim\ \mathcal{M}_N(\mathbb{C})$. All the sets $\mathbf{M}$ of POVMs we will later be lead to consider will have such property, and the norm $\|\cdot\|_{\mathbf{M}}$ will be called the distinguishability norm associated with $\mathbf{M}$.*

Something else that is worth pointing at is that we can actually, without any loss of generality, restrict ourselves to considering 2-outcome POVMs $(M, \mathbb{1}_{\mathcal{H}}-M)$. Indeed, we have just seen that, on a given state pair (ρ,σ), the POVM $(M_i)_{i\in I}$ will achieve the same bias as the POVM $\left(\sum_{i\in\widetilde{I}}M_i, \mathbb{1}_{\mathcal{H}}-\sum_{i\in\widetilde{I}}M_i\right)$ where $\widetilde{I} = \{i\in I,\ \mathrm{Tr}(M_i\rho) > \mathrm{Tr}(M_i\sigma)\}$.
In other words, for any set $\mathbf{M}$ of POVMs, there exists a set $\widetilde{\mathbf{M}}$ of 2-outcome POVMs such that $\|\cdot\|_{\mathbf{M}} = \|\cdot\|_{\widetilde{\mathbf{M}}}$, which may be defined as $\widetilde{\mathbf{M}} := \left\{\big(M, \mathbb{1}_{\mathcal{H}}-M\big),\ \exists(M_i)_{i\in I}\in\mathbf{M}, \exists\widetilde{I}\subset I : M = \sum_{i\in\widetilde{I}}M_i\right\}$.

Yet, for any 2-outcome POVM $(M, \mathbb{1}_{\mathcal{H}}-M)$ with associated CPTP map $\mathcal{M}$, and any traceless matrix Δ, we have : $\|\mathcal{M}(\Delta)\|_1 = |\mathrm{Tr}(M\Delta)| + |\mathrm{Tr}((\mathbb{1}_{\mathcal{H}}-M)\Delta)| = 2|\mathrm{Tr}(M\Delta)| = |\mathrm{Tr}((2M-\mathbb{1}_{\mathcal{H}})\Delta)|$, where we just used twice that $\mathrm{Tr}\Delta = 0$.
So for any set of 2-outcome POVMs $\widetilde{\mathbf{M}}$:

$$\|\rho-\sigma\|_{\widetilde{\mathbf{M}}} = \max_{\left(\frac{\mathbb{1}_{\mathcal{H}}+A}{2}, \frac{\mathbb{1}_{\mathcal{H}}-A}{2}\right)\in\widetilde{\mathbf{M}}} \big|\mathrm{Tr}(A(\rho-\sigma))\big|$$

The advantage of such rewritting of the problem is that the condition for $(M, \mathbb{1}_{\mathcal{H}} - M)$ to be a 2-outcome POVM, that is $\mathbb{0}_{\mathcal{H}} \leq M \leq \mathbb{1}_{\mathcal{H}}$, can be expressed in a more symmetric way in terms of $A_M := 2M - \mathbb{1}_{\mathcal{H}}$ as $-\mathbb{1}_{\mathcal{H}} \leq A_M \leq \mathbb{1}_{\mathcal{H}}$ i.e. simply $\|A_M\|_\infty \leq 1$.
Hence, it immediately follows by duality (*cf* appendix A.1) that when all the 2-outcome POVMs are allowed :

$$\|\rho - \sigma\|_{\mathbf{ALL}} = \max_{\|A\|_\infty \leq 1} \left|\mathrm{Tr}(A(\rho - \sigma))\right| = \|\rho - \sigma\|_1$$

Remark 2.3 *Once again, this can be generalized to states ρ and σ with any respective prior probabilities q and $1-q$. Let indeed $(M, \mathbb{1}_{\mathcal{H}} - M)$ be a 2-outcome POVM. We then have for any (non necessarily traceless) Hermitian matrix Δ :*

$$\|\Delta\|_M = \max_{A \in [\mathbb{1}_{\mathcal{H}} - 2M; 2M - \mathbb{1}_{\mathcal{H}}]} \left|Tr(A\Delta)\right|$$

The difference with the particular case of a traceless Δ is that the maximum $\max_{A \in [\mathbb{1}_{\mathcal{H}} - 2M; 2M - \mathbb{1}_{\mathcal{H}}]} \left|Tr(A\Delta)\right|$ is in general not attained for $A \in \{\mathbb{1}_{\mathcal{H}} - 2M, 2M - \mathbb{1}_{\mathcal{H}}\}$ an extremal point of the operator interval $[\mathbb{1}_{\mathcal{H}} - 2M; 2M - \mathbb{1}_{\mathcal{H}}]$.
Thus, for all set of 2-outcome POVMs $\widetilde{\mathbf{M}}$ and all Hermitian matrix Δ :

$$\|\Delta\|_{\widetilde{\mathbf{M}}} = \max_{(M, \mathbb{1}_{\mathcal{H}} - M) \in \widetilde{\mathbf{M}}} \left(\max_{A \in [\mathbb{1}_{\mathcal{H}} - 2M; 2M - \mathbb{1}_{\mathcal{H}}]} \left|Tr(A\Delta)\right| \right)$$

So the result $\|\Delta\|_{\mathbf{ALL}} = \|\Delta\|_1$ remains valid for any Hermitian matrix Δ, especially one of the form $2(q\rho - (1-q)\sigma)$. This is one of the seminal observations by Holevo [3] and Helstrom [4] in the field of quantum state discrimination.

Now, the general problem we are dealing with is to compare, for various informationally complete sets of POVMs $\mathbf{M} \subset \mathbf{ALL}$, the bias achievable in discriminating two states when only measurements in $\mathbf{M}$ are allowed to the one achievable when all measurements are allowed. As just stated, this is equivalent to comparing the distinguishability norm $\|\cdot\|_{\mathbf{M}}$ associated with $\mathbf{M}$ to the 1-norm $\|\cdot\|_1$, especially when applied to traceless matrices.
More precisely, defining $\lambda(\mathbf{M})$ and $\mu(\mathbf{M})$ as $\lambda(\mathbf{M}) := \inf_{\|\Delta\|_1 = 1} \|\Delta\|_{\mathbf{M}}$ and $\mu(\mathbf{M}) := \sup_{\|\Delta\|_1 = 1} \|\Delta\|_{\mathbf{M}}$, and in the same way $\lambda_0(\mathbf{M})$ and $\mu_0(\mathbf{M})$ as $\lambda_0(\mathbf{M}) := \inf_{\substack{\|\Delta\|_1 = 1 \\ \mathrm{Tr}\Delta = 0}} \|\Delta\|_{\mathbf{M}}$ and $\mu_0(\mathbf{M}) := \sup_{\substack{\|\Delta\|_1 = 1 \\ \mathrm{Tr}\Delta = 0}} \|\Delta\|_{\mathbf{M}}$, we will be interested in finding bounds on $\lambda(\mathbf{M}) \leq \lambda_0(\mathbf{M})$ and $\mu_0(\mathbf{M}) \leq \mu(\mathbf{M})$.

One first statement we can make about those constants of domination λ and μ (as well as λ_0 and μ_0) is the following : if $\mathbf{M}$ and $\mathbf{M}'$ are two sets of informationally complete POVMs such that $\mathbf{M} \subset \mathbf{M}'$, then, by definition, $\|\cdot\|_{\mathbf{M}} \leq \|\cdot\|_{\mathbf{M}'}$, so $\lambda(\mathbf{M}) \leq \lambda(\mathbf{M}')$ and $\mu(\mathbf{M}) \leq \mu(\mathbf{M}')$.

What is more, if $(\mathbf{M}_j)_{j \in J}$ is a sequence of informationally complete sets of POVMs and $(p_j)_{j \in J}$ is a sequence of positive coefficients that sum to 1, then the convex combination $\mathbf{M}' := \sum_{j \in J} p_j \mathbf{M}_j$ is an informationally complete set of POVMs that is such that $\|\cdot\|_{\mathbf{M}'} = \sum_{j \in J} p_j \|\cdot\|_{\mathbf{M}_j}$. Subsequently, $\lambda(\mathbf{M}') \geq \sum_{j \in J} p_j \lambda(\mathbf{M}_j)$ and $\mu(\mathbf{M}') \leq \sum_{j \in J} p_j \mu(\mathbf{M}_j)$. And this property actually remains true for J being any set equiped with a probability measure $\{dp(j)\}_{j \in J}$ and $\{\mathbf{M}(j)\}_{j \in J}$ being a distribution of informationally complete sets of POVMs on J (by just replacing the discrete sum on J by a continuous integration on J).

Now, we also have that for all informationally complete set of POVMs $\mathbf{M}$ and all unitary matrix on $\mathcal{H}$ $U \in \mathcal{U}(N)$, $U\mathbf{M}U^{-1}$ is an informationally complete set of POVMs which is such that $\|\cdot\|_{U\mathbf{M}U^{-1}} = \|\cdot\|_{\mathbf{M}}$ (by invariance of the trace under conjugation). So $\lambda(U\mathbf{M}U^{-1}) = \lambda(\mathbf{M})$ and $\mu(U\mathbf{M}U^{-1}) = \mu(\mathbf{M})$.

Puting those two previous results together, we get that for any informationally complete set of POVMs $\mathbf{M}$ and any probability measure $dp(U)$ on the unitary group $\mathcal{U}(N)$:

$$\lambda\left(\int_{\mathcal{U}(N)} U\mathbf{M}U^{-1}dp(U)\right) \geq \lambda(\mathbf{M}) \text{ and } \mu\left(\int_{\mathcal{U}(N)} U\mathbf{M}U^{-1}dp(U)\right) \leq \mu(\mathbf{M})$$

This implies that, amongst all sets of POVMs made of one single informationally complete POVM, the one for which λ is the largest as well as μ is the smallest is the one consisting of the uniform POVM. That is why we shall later be especially interested in it.

Remark 2.4 *: All those basic observations on how distinguishability norms relate to the* 1*-norm were already stated in [11], which the reader is referred to for further information, and especially the interpretation of distinguishability norms as norms associated with certain convex bodies (cf also appendix A.2).*

However, let us point out from now that, although the 1-norm seems at first sight to be the most meaningful reference norm in this context, it will actually appear that the 2-norm is perhaps' a more relevant figure of merit for understanding state discrimination with a fixed set of measurements. Indeed, we will show that, when dealing with (actually non necessarily traceless) operators on a multi-partite system, the distinguishability norm associated with local measurements that are "sufficiently symmetric" (in a sense to be defined later) is essentially equivalent to a multi-partite generalization of the 2-norm : when comparing the two, the constants of domination depend only on the number of parties and not on their dimension.

3 t-design POVMs

In this section, we define and discuss some properties of an outstanding category of highly symmetric POVMs (which the uniform POVM is the most particular example of), that is the one of the so-called *t-design POVMs.*

3.1 Spherical t-designs

3.1.1 Definition and main properties

Let $\mathcal{H} \equiv \mathbb{C}^N$ be a finite N-dimensional Hilbert space.

We denote by $d\psi$ the uniform probability measure on the unit vectors of $\mathcal{H}$, i.e. the (existing and unique) unitary invariant measure over $\mathcal{H}$'s unit sphere normalized by $\int_{\langle\psi|\psi\rangle=1} d\psi = 1$.

We then have : $\int_{\langle\psi|\psi\rangle=1} |\psi\rangle\langle\psi| d\psi = \frac{\mathbb{1}_{\mathcal{H}}}{N}$.

And more generally, for all $t \in \mathbb{N}^*$, $\int_{\langle\psi|\psi\rangle=1} \left(|\psi\rangle\langle\psi|\right)^{\otimes t} d\psi$ is the normalized orthogonal projector on the completely symmetric subspace of $\mathcal{H}^{\otimes t}$ (*cf* appendix B.3) :

$$\int_{\langle\psi|\psi\rangle=1} \left(|\psi\rangle\langle\psi|\right)^{\otimes t} d\psi = \frac{\Pi^{\perp}_{\mathcal{S}(\mathcal{H},t)}}{\binom{N+t-1}{t}} = \frac{1}{N \times \cdots \times (N+t-1)} \sum_{\sigma\in\mathfrak{S}_t} U_\sigma \tag{1}$$

Definition 3.1 *Let $\{p_k, 1 \leq k \leq m\}$ be a probability distribution and $\{|\phi_k\rangle, 1 \leq k \leq m\}$ be a set of unit vectors in $\mathcal{H}$. Let also $t \in \mathbb{N}^*$. $\{(p_k, |\phi_k\rangle), 1 \leq k \leq m\}$ is a spherical t-design if :*

$$\sum_{k=1}^{m} p_k \left(|\phi_k\rangle\langle\phi_k|\right)^{\otimes t} = \int_{\langle\psi|\psi\rangle=1} \left(|\psi\rangle\langle\psi|\right)^{\otimes t} d\psi$$

If $p_k = \frac{1}{m}$ for all $1 \leq k \leq m$, $\{(p_k, |\phi_k\rangle), 1 \leq k \leq m\}$ is said to be a proper spherical t-design. It may otherwise be referred to as a weighted spherical t-design.

From this definition, it is immediate to see that if $\{(p_k, |\phi_k\rangle), 1 \leq k \leq m\}$ is a spherical t-design, then necessarily $m \geq \binom{N+t-1}{t}$. Indeed, each of the $\left(|\phi_k\rangle\langle\phi_k|\right)^{\otimes t}$ is a rank-1 projector on $\mathcal{H}^{\otimes t}$, whereas $\Pi^{\perp}_{\mathcal{S}(\mathcal{H},t)}$ is a rank-$\binom{N+t-1}{t}$ projector on $\mathcal{H}^{\otimes t}$ (*cf* appendix B.3).
However, this bound is far from optimal, and we actually have the following : if $\{(p_k, |\phi_k\rangle), 1 \leq k \leq m\}$ is a spherical t-design, then necessarily $m \geq \binom{N+\lceil t/2 \rceil - 1}{\lceil t/2 \rceil}\binom{N+\lfloor t/2 \rfloor - 1}{\lfloor t/2 \rfloor}$. A spherical t-design that achieves this bound (which by the way has to be proper) is called *minimal* or *tight*.

Proposition 3.2 *$\{(p_k, |\phi_k\rangle), 1 \leq k \leq m\}$ is a spherical t-design if and only if for all polynomial $P(X_1, \ldots, X_N, Y_1, \ldots, Y_N)$ homogeneous of degree t in the X_q and in the Y_q, $1 \leq q \leq N$:*

$$\sum_{k=1}^{m} p_k P(\phi_k) = \int_{\langle\psi|\psi\rangle=1} P(\psi) d\psi$$

where $P(\phi) := P(\alpha_1, \ldots, \alpha_N, \alpha_1^*, \ldots, \alpha_N^*)$ for $\phi = \sum_{q=1}^{N} \alpha_q |q\rangle$ (with $\{|q\rangle, 1 \leq q \leq N\}$ an orthonormal basis of $\mathcal{H}$).

Proof : Let us write definition 3.1 in an orthonormal basis $\{|q\rangle, 1 \leq q \leq N\}$ of $\mathcal{H}$.
$\{(p_k, |\phi_k\rangle), 1 \leq k \leq m\}$ is a spherical t-design if and only if :

$$\sum_{k=1}^{m} p_k \left(\sum_{q,q'=1}^{N} \langle q|\phi_k\rangle\langle q'|\phi_k\rangle^* |q\rangle\langle q'| \right)^{\otimes t} = \int_{\langle\psi|\psi\rangle=1} \left(\sum_{q,q'=1}^{N} \langle q|\psi\rangle\langle q'|\psi\rangle^* |q\rangle\langle q'| \right)^{\otimes t} d\psi$$

Now, using the fact that $\left\{ \bigotimes_{n=1}^{t} |q_n\rangle\langle q'_n|, 1 \leq q_1, q'_1 \ldots q_t, q'_t \leq N \right\}$ is a basis of the vector space of linear operators on $\mathcal{H}^{\otimes t}$, this is equivalent to the equality of each of the coefficients :

$$\forall\ 1 \leq q_1, q'_1 \ldots q_t, q'_t \leq N,\ \sum_{k=1}^{m} p_k \prod_{n=1}^{t} \langle q_n|\phi_k\rangle\langle q'_n|\phi_k\rangle^* = \int_{\langle\psi|\psi\rangle=1} \prod_{n=1}^{t} \langle q_n|\psi\rangle\langle q'_n|\psi\rangle^* d\psi$$

And this is exactly the result of proposition 3.2 for all homogeneous degree t monomials, which concludes the proof.

In other words, a spherical t-design is a set of weighted unitary vectors that is such that the average value over it of any degree t polynomial is the same as its average value over all uniformly weighted unitary vectors.

Proposition 3.3 *$\{(p_k, |\phi_k\rangle), 1 \leq k \leq m\}$ is a spherical t-design if and only if :*

$$\sum_{k,j=1}^{m} p_k p_j |\langle\phi_k|\phi_j\rangle|^{2t} = \frac{1}{\binom{N+t-1}{t}}$$

Proof : Let us define the matrix M on $\mathcal{H}^{\otimes t}$ as : $M := \sum_{k=1}^{m} p_k \left(|\phi_k\rangle\langle\phi_k|\right)^{\otimes t} - \frac{1}{\binom{N+t-1}{t}} \Pi^{\perp}_{\mathcal{S}(\mathcal{H},t)}$.

Then, by definition 3.1 :

$$\{(p_k,|\phi_k\rangle), 1\leq k\leq m\}\ t\text{-design} \Leftrightarrow M=\mathbb{0}_{\mathcal{H}^{\otimes t}}$$
$$\Leftrightarrow \mathrm{Tr}_{\mathcal{H}^{\otimes t}}(M^\dagger M)=0$$
$$\Leftrightarrow \sum_{k,j=1}^{m} p_k p_j |\langle\phi_k|\phi_j\rangle|^{2t} - \frac{1}{\binom{N+t-1}{t}} = 0$$

$$\text{Indeed}: \begin{cases} \mathrm{Tr}\Big[\big(|\phi_k\rangle\langle\phi_k|^{\otimes t}\big)^\dagger |\phi_j\rangle\langle\phi_j|^{\otimes t}\Big] = \mathrm{Tr}\Big[\langle\phi_k|\phi_j\rangle^t |\phi_k\rangle\langle\phi_j|^{\otimes t}\Big] = |\langle\phi_k|\phi_j\rangle|^{2t} \\ \mathrm{Tr}\Big[\big(|\phi_k\rangle\langle\phi_k|^{\otimes t}\big)^\dagger \Pi^\perp_{\mathcal{S}(\mathcal{H},t)}\Big] = \mathrm{Tr}\Big[\big(\Pi^\perp_{\mathcal{S}(\mathcal{H},t)}\big)^\dagger |\phi_k\rangle\langle\phi_k|^{\otimes t}\Big] \\ \mathrm{Tr}\Big[\big(\Pi^\perp_{\mathcal{S}(\mathcal{H},t)}\big)^\dagger \Pi^\perp_{\mathcal{S}(\mathcal{H},t)}\Big] = \mathrm{Tr}\Big[\Pi^\perp_{\mathcal{S}(\mathcal{H},t)}\Big] = \binom{N+t-1}{t} \end{cases}.$$

Remark 3.4 *It may be pointed out that the inequality* $\sum_{k,j=1}^{m} p_k p_j |\langle\phi_k|\phi_j\rangle|^{2t} \geq \frac{1}{\binom{N+t-1}{t}}$ *stands for any set* $\{(p_k,|\phi_k\rangle), 1\leq k\leq m\}$ *(due to the trivial* $Tr_{\mathcal{H}^{\otimes t}}(M^\dagger M)\geq 0$ *for any matrix* M *on* $\mathcal{H}^{\otimes t}$*). A spherical* t*-design is hence a weighted set* $\{(p_k,|\phi_k\rangle), 1\leq k\leq m\}$ *that minimizes its so-called* t^{th} *order potential* $V_t := \sum_{k,j=1}^{m} p_k p_j |\langle\phi_k|\phi_j\rangle|^{2t}$*. Such characterization of spherical* t*-designs has a practical interest since it allows to look for them numerically by parametrizing a weighted set and minimizing its* t^{th} *order potential.*
An example of such operational procedure is provided by the following :
We would like to construct a spherical t*-design from* m *orthonormal bases* $\mathcal{B}_k := \{|\psi_k^j\rangle, 1\leq j\leq N\}$, $1\leq k\leq m$, *of* $\mathcal{H}$*. Each unit vector* $|\psi_k^j\rangle$, $1\leq k\leq m$, $1\leq j\leq N$, *is hence given weight* $p_k^j\geq 0$, *with the normalization constraint* $\sum_{\substack{1\leq k\leq m\\ 1\leq j\leq N}} p_k^j = 1$*. Then, defining the* $\lambda_{k,k'}^{j,j'}$, $1\leq k,k'\leq m$, $1\leq j,j'\leq N$, *as* $\lambda_{k,k'}^{j,j'} := |\langle\psi_k^j|\psi_{k'}^{j'}\rangle|\geq 0$*, those must satisfy the normalization constraint* $\sum_{1\leq j'\leq N} \lambda_{k,k'}^{j,j'} = 1$ *for all* $1\leq k,k'\leq m$ *and* $1\leq j\leq N$*. So we eventually have to minimize the quantity* $\sum_{\substack{1\leq k,k'\leq m\\ 1\leq j,j'\leq N}} p_k^j p_{k'}^{j'} \big(\lambda_{k,k'}^{j,j'}\big)^t$ *under the* $1+m^2+N$ *constraints mentioned above.*

Proposition 3.5 $\{(p_k,|\phi_k\rangle), 1\leq k\leq m\}$ *is a spherical* t*-design if and only if for all polynomial* Q *of degree at most* t *:*

$$\sum_{k,j=1}^{m} p_k p_j Q\left(|\langle\phi_k|\phi_j\rangle|^2\right) = \int_{\langle\psi|\psi\rangle=\langle\varphi|\varphi\rangle=1} Q\left(|\langle\psi|\varphi\rangle|^2\right) d\psi d\varphi$$

Proof : The result of proposition 3.5 is actually nothing more than the one of proposition 3.3 :

$$\{(p_k,|\phi_k\rangle)\}_{1\leq k\leq m}\ t\text{-design} \Leftrightarrow \forall\ s\leq t,\ \{(p_k,|\phi_k\rangle)\}_{1\leq k\leq m}\ s\text{-design}$$
$$\Leftrightarrow \forall\ s\leq t,\ \sum_{k,j=1}^{m} p_k p_j |\langle\phi_k|\phi_j\rangle|^{2s} = \frac{1}{\binom{N+s-1}{s}} = \int_{\langle\psi|\psi\rangle=\langle\varphi|\varphi\rangle=1} |\langle\psi|\varphi\rangle|^{2s} d\psi d\varphi$$
$$\Leftrightarrow \forall\ Q=\sum_{n=0}^{t}\alpha_n X^n,\ \sum_{k,j=1}^{m} p_k p_j Q\left(|\langle\phi_k|\phi_j\rangle|^2\right) = \int_{\langle\psi|\psi\rangle=\langle\varphi|\varphi\rangle=1} Q\left(|\langle\psi|\varphi\rangle|^2\right) d\psi d\varphi$$

where the last equivalence is simply by linearity.

For a more complete account on spherical t-designs the reader is referred to [12] (where a more geometric approach is also provided), [13] (where the link with *frames* and *spherical codes* is made) or [14].

3.1.2 Explicit constructions of spherical proper designs

• Spherical proper 1-designs

Let $\{|q\rangle, 1 \leq q \leq N\}$ be an orthonormal basis of $\mathcal{H}$. $\left\{\left(\frac{1}{N}, |q\rangle\right), 1 \leq q \leq N\right\}$ is then obviously a minimal spherical proper 1-design on $\mathcal{H}$.
Thus, there exist minimal spherical proper 1-designs on $\mathcal{H}$ whatever its dimension N.

• Spherical proper 2-designs

∗ Spherical proper 2-designs from complete sets of MUB

Definition 3.6 *Let $\mathcal{B}$ and $\mathcal{B}'$ be two orthonormal bases of $\mathcal{H}$. They are said to be Mutually Unbiased Bases (MUB) of $\mathcal{H}$ if :* $\forall\ (|b\rangle, |b'\rangle) \in \mathcal{B} \times \mathcal{B}',\ |\langle b|b'\rangle| = \frac{1}{\sqrt{N}}$

In view of physical applications, the main interest of having available two MUB $\mathcal{B}$ and $\mathcal{B}'$ is the following : If a quantum system is prepared in a state $|b\rangle\langle b|$ with $|b\rangle \in \mathcal{B}$, then no information can be retrieved when the POVM $(|b'\rangle\langle b'|)_{|b'\rangle \in \mathcal{B}'}$ is performed on it (all the outcomes of the measurement occur with same probability $\frac{1}{N}$).

Theorem 3.7 *Let $\mathcal{B}_k := \left\{|\phi_k^j\rangle, 1 \leq j \leq N\right\}$, $1 \leq k \leq N+1$, be $N+1$ pairwise MUB of $\mathcal{H}$, which means that $|\langle\phi_k^j|\phi_{k'}^{j'}\rangle| = \begin{cases} \delta_{j,j'} & \text{if } k = k' \\ \frac{1}{\sqrt{N}} & \text{if } k \neq k' \end{cases}$. Then, $\left\{\left(\frac{1}{N(N+1)}, |\phi_k^j\rangle\right), 1 \leq k \leq N+1, 1 \leq j \leq N\right\}$ is a spherical proper 2-design on $\mathcal{H}$.*

Proof :

$$\begin{aligned}
\sum_{\substack{1\leq k,k'\leq N+1 \\ 1\leq j,j'\leq N}} \frac{1}{N^2(N+1)^2}\left|\langle\phi_k^j|\phi_{k'}^{j'}\rangle\right|^4 &= \frac{1}{N(N+1)} \sum_{\substack{1\leq k\leq N+1 \\ 1\leq j\leq N}} \left|\langle\phi_k^j|\phi_1^1\rangle\right|^4 \\
&= \frac{1}{N(N+1)}\left(1 + N^2 \times \frac{1}{N^2}\right) \\
&= \frac{2}{N(N+1)} \\
&= \frac{1}{\binom{N+1}{2}}
\end{aligned}$$

And by proposition 3.3, this actually proves that $\left\{\left(\frac{1}{N(N+1)}, |\phi_k^j\rangle\right), 1 \leq k \leq N+1, 1 \leq j \leq N\right\}$ is a spherical 2-design.

The remaining question is now the one of the existence of such sets of $N+1$ pairwise MUB of $\mathcal{H}$ (those are called *complete* or *maximal* since there actually exist at most $N+1$ pairwise MUB of $\mathcal{H}$). The following theorem provides a partial answer.

Theorem 3.8 *If $N = p^d$ with p a prime number and $d \in \mathbb{N}^*$, then there exists a complete set of MUB of $\mathcal{H}$.*

Proof : Let us first consider the case when $N = p$ with p prime. In what follows, all sums on the indices are to be understood mod p.
We denote by $\{|q\rangle, 0 \leq q \leq p-1\}$ an orthonormal basis of $\mathcal{H}$ and we define the operators X and Z acting on $\mathcal{H}$ by : $X|q\rangle = |q+1\rangle$ and $Z|q\rangle = \omega|q\rangle$, where $\omega := e^{2i\pi/p}$.
Hence, $\forall\ 0 \leq k \leq p-1,\ XZ^k|q\rangle = \omega^{kq}|q+1\rangle$. So for all $0 \leq k \leq p-1$, the eigenvectors of XZ^k are $\left\{|\phi_k^j\rangle := \frac{1}{\sqrt{p}}\sum_{l=0}^{p-1}\omega^{-jl-ks_l}|l\rangle, 0 \leq j \leq p-1\right\}$, where $s_l := \sum_{m=l}^{p-1} m$ (with associated eigenvalues $\{\omega^j, 0 \leq j \leq p-1\}$). Yet for all $0 \leq k, k' \leq p-1$ and all $0 \leq j \leq p-1$, $XZ^{k'}|\phi_k^j\rangle = \omega^{j+k-k'}|\phi_k^{j+k-k'}\rangle$, which means that the eigenvectors of XZ^k are cyclically shifted under the action of $XZ^{k'}$.
This implies that the set of orthonormal bases of $\mathcal{H}$ consisting respectively of the eigenvectors of Z and of the eigenvectors of the XZ^k, $0 \leq k \leq p-1$, form a set of $p+1$ pairwise MUB of $\mathcal{H}$.

In the general case when $N = p^d$ with p prime and $d \in \mathbb{N}^*$, we have $\mathcal{H} \equiv (\mathbb{C}^p)^{\otimes d}$. We can thus use the previous result to show that the set of orthonormal bases of $\mathcal{H}$ consisting respectively of the eigenvectors of $Z^{\otimes d}$ and of the eigenvectors of the $\bigotimes_{i=1}^{d} XZ^{k_i}$, $0 \leq k_i \leq p-1$, $1 \leq i \leq d$, form a set of $p^m + 1$ pairwise MUB of $\mathcal{H}$

Such construction of spherical proper 2-designs from complete sets of MUB is described and discussed in greater depth in [16].

∗Minimal spherical proper 2-designs from SIC-POVMs

Definition 3.9

- *A POVM is informationally complete (IC) if it has enough measurement outcomes to uniquely determine any quantum state. Now, a density operator ρ on $\mathcal{H}$ has N^2-1 independent entries (due to the trace constraint $Tr_{\mathcal{H}}\rho = 1$), and a POVM $(M_i)_{i\in I}$ on $\mathcal{H}$ has $|I|-1$ independent elements (due to the completeness constraint $\sum_{i\in I} M_i = \mathbb{1}_{\mathcal{H}}$). So an IC POVM on $\mathcal{H}$ must have at least N^2 elements. In such case, it is said to be minimal.*

- *A POVM $(M_i)_{i\in I}$ is symmetric (S) if its elements have pairwise identical Hilbert-Schmidt inner product, i.e. $\forall\ i \neq j, i' \neq j' \in I,\ Tr(M_i M_j) = Tr(M_{i'} M_{j'})$.*

- *A SIC POVM is a minimal symmetric informationally complete POVM. A SIC POVM on $\mathcal{H}$ is thus given by N^2 subnormalized rank 1 projectors on $\mathcal{H}$ $\left(P_k := \frac{1}{N}|\phi_k\rangle\langle\phi_k|\right)_{1\leq k\leq N^2}$ such that $\forall\ 1 \leq j \neq k \leq N^2,\ Tr(P_j P_k) = \frac{1}{N^2(N+1)}$. This is equivalent to demanding that the unit vectors $|\phi_k\rangle$, $1 \leq k \leq N^2$, satisfy $\forall\ 1 \leq j \neq k \leq N^2,\ \left|\langle\phi_j|\phi_k\rangle\right|^2 = \frac{1}{N+1}$, or to put it differently that $\left\{Span\big(|\phi_k\rangle\big), 1 \leq k \leq N^2\right\}$ be a maximal set of equiangular lines in $\mathcal{H}$.*

Theorem 3.10 *If $\left(\frac{1}{N}|\phi_k\rangle\langle\phi_k|\right)_{1\leq k\leq N^2}$ is a SIC POVM on $\mathcal{H}$, then $\left\{\left(\frac{1}{N^2}, |\phi_k\rangle\right), 1 \leq k \leq N^2\right\}$ is a minimal spherical proper 2-design on $\mathcal{H}$.*

Proof :

$$\begin{aligned}\sum_{1\leq j,k\leq N^2}\frac{1}{N^4}\left|\langle\phi_j|\phi_k\rangle\right|^4 =& \frac{1}{N^4}\left(\sum_{1\leq j\leq N^2}\left|\langle\phi_j|\phi_j\rangle\right|^4+\sum_{1\leq j\neq k\leq N^2}\left|\langle\phi_j|\phi_k\rangle\right|^4\right)\\ =&\frac{1}{N^4}\left(N^2\times 1+N^2(N^2-1)\times\frac{1}{(N+1)^2}\right)\\ =&\frac{2}{N(N+1)}\\ =&\frac{1}{\binom{N+1}{2}}\end{aligned}$$

And by proposition 3.3, this actually proves that $\left\{\left(\frac{1}{N^2},|\phi_k\rangle\right),1\leq k\leq N^2\right\}$ is a spherical 2-design.

Remark 3.11 *In fact, it also stands that, conversely, if* $\left\{\left(\frac{1}{N^2},|\phi_k\rangle\right),1\leq k\leq N^2\right\}$ *is a spherical proper* 2*-design on* $\mathcal{H}$*, then* $\left(\frac{1}{N}|\phi_k\rangle\langle\phi_k|\right)_{1\leq k\leq N^2}$ *is a SIC POVM on* $\mathcal{H}$*.*
Indeed, defining the $\lambda_{j,k}$*,* $1\leq j\neq k\leq N^2$*, as* $\lambda_{j,k}:=\left|\langle\phi_j|\phi_k\rangle\right|^2$*, we have by proposition 3.3 (using the fact that* $\left\{\left(\frac{1}{N^2},|\phi_k\rangle\right),1\leq k\leq N^2\right\}$ *is a spherical proper both* 1*- and* 2*-design on* $\mathcal{H}$*) :*

$$\begin{cases}\sum_{j,k}\lambda_{j,k}=\frac{N^4}{\binom{N}{1}}-N^2=N^2(N-1)\\ \sum_{j,k}\left(\lambda_{j,k}\right)^2=\frac{N^4}{\binom{N+1}{2}}-N^2=\frac{N^2(N-1)}{N+1}\end{cases}$$

Yet, the plane $\sum_{j,k}\lambda_{j,k}=N^2(N-1)$ *and the sphere* $\sum_{j,k}\left(\lambda_{j,k}\right)^2=\frac{N^2(N-1)}{N+1}$ *in* $\mathbb{R}^{N^2(N^2-1)}$ *have one single point of intersection which is there point of tangency* $\left(\frac{1}{N+1},\ldots,\frac{1}{N+1}\right)$*.*
We thus have : $\forall\ 1\leq j\neq k\leq N^2,\ \left|\langle\phi_j|\phi_k\rangle\right|^2=\frac{1}{N+1}$*, which exactly means that* $\left(\frac{1}{N}|\phi_k\rangle\langle\phi_k|\right)_{1\leq k\leq N^2}$ *is a SIC POVM on* $\mathcal{H}$

Once again, the remaining question is the one of the existence of such SIC POVMs on $\mathcal{H}$.
One known construction is the one of the so-called *group covariant* SIC POVMs, i.e. those for which the unit vectors $\left(|\phi_k\rangle\right)_{1\leq k\leq N^2}$ are generated by one single unit vector $|\phi_1\rangle$ (called the *fiducial vector*) under the action of a subgroup of the unitary group $\mathcal{U}(N)$.
For instance, denoting by $\{|q\rangle,0\leq q\leq N-1\}$ an orthonormal basis of $\mathcal{H}$, and defining as previously the operators X and Z on $\mathcal{H}$ by $X|q\rangle=|q+1\rangle$ (mod N) and $Z|q\rangle=e^{2i\pi/N}|q\rangle$, a fiducial vector $|\psi\rangle$ associated with the action on $\mathcal{H}$ of the Heisenberg-Weyl group (i.e. the group generated by X and Z) must satisfy : $\forall\ 0\leq k,k'\leq N-1,\ (k,k')\neq(0,0),\ \left|\langle\psi|X^kZ^{k'}|\psi\rangle\right|^2=\frac{1}{N+1}$. If such $|\psi\rangle$ exists, the associated group covariant SIC POVM is then $\left(\frac{1}{N}X^kZ^{k'}|\psi\rangle\right)_{0\leq k,k'\leq N-1}$.
Such fiducial vectors are known to exist for $N\leq 16$ and $N\in\{19,24,28,35,48\}$, and are conjectured to exist for all N. Much more on this matter, and on the link between SIC-POVMs and minimal spherical proper 2-designs, may be found in [15].

3.2 t-design POVMs

For a given $t \in \mathbb{N}^*$, let $\{(p_k, |\phi_k\rangle), 1 \leq k \leq m\}$ be a spherical t-design. It is then automatically a spherical s-design for all $s \leq t$. So in particular, $\sum_{k=1}^{m} p_k |\phi_k\rangle\langle\phi_k| = \frac{1}{N}\mathbb{1}_{\mathcal{H}}$.
Thus, $D_{(\mathcal{H},t)} := (M_k)_{1\leq k\leq m}$, with $M_k := N p_k |\phi_k\rangle\langle\phi_k|$ for all $1 \leq k \leq m$, is a POVM, which we will call a t-design POVM (see [11] and [17] for more details on those POVMs with high symmetry properties).

Denoting by $\{|k\rangle, 1 \leq k \leq m\}$ an orthonormal basis of $\mathbb{C}^m$, the associated CPTP map from the set of Hermitian matrices on $\mathcal{H}$ to the set of Hermitian matrices on $\mathbb{C}^m$ is given by :

$$\mathcal{D}_{(\mathcal{H},t)} : \Delta \mapsto \sum_{k=1}^{m} \mathrm{Tr}(M_k \Delta)|k\rangle\langle k| = N \sum_{k=1}^{m} p_k \mathrm{Tr}\big(|\phi_k\rangle\langle\phi_k|\Delta\big)|k\rangle\langle k|$$

So, for all Hermitian matrix Δ on $\mathcal{H}$, denoting by S_Δ the random variable that takes value $\mathrm{Tr}\big(|\phi_k\rangle\langle\phi_k|\Delta\big)$ with probability p_k for all $1 \leq k \leq m$, we have :

$$\|\Delta\|_{D_{(\mathcal{H},t)}} = \|\mathcal{D}_{(\mathcal{H},t)}(\Delta)\|_1 = N \sum_{k=1}^{m} p_k \big|\mathrm{Tr}\big(|\phi_k\rangle\langle\phi_k|\Delta\big)\big| = N\mathbb{E}\big(|S_\Delta|\big) \tag{2}$$

Regarding such t-design POVM $D_{(\mathcal{H},t)}$, another important result we will need later on is the following one. For all Hermitian matrix Δ on $\mathcal{H}$ with associated random variable S_Δ :

$$\mathbb{E}\big((S_\Delta)^t\big) = \sum_{k=1}^{m} p_k \Big(\mathrm{Tr}_{\mathcal{H}}\big(|\phi_k\rangle\langle\phi_k|\Delta\big)\Big)^t = \sum_{k=1}^{m} p_k \mathrm{Tr}_{\mathcal{H}^{\otimes t}}\big(|\phi_k\rangle\langle\phi_k|^{\otimes t}\Delta^{\otimes t}\big) = \mathrm{Tr}_{\mathcal{H}^{\otimes t}}\left(\left(\sum_{k=1}^{m} p_k |\phi_k\rangle\langle\phi_k|^{\otimes t}\right)\Delta^{\otimes t}\right)$$

Then, using the fact that $D_{(\mathcal{H},t)}$ is a t-design POVM and recalling equation 1, we get :

$$\mathbb{E}\big((S_\Delta)^t\big) = \mathrm{Tr}_{\mathcal{H}^{\otimes t}}\left(\left(\frac{1}{N \times \cdots \times (N+t-1)} \sum_{\sigma \in \mathfrak{S}_t} U_\sigma\right)\big(\Delta^{\otimes t}\big)\right) \tag{3}$$

It might be worth noting at that point that $\{(d\psi, |\psi\rangle), \langle\psi|\psi\rangle = 1\}$ is a spherical ∞-design. So the uniform POVM on $\mathcal{H}$, $U_{\mathcal{H}} := (N|\psi\rangle\langle\psi|d\psi)_{\langle\psi|\psi\rangle=1}$ is an ∞-design POVM.
For all Hermitian matrix Δ on $\mathcal{H}$, denoting, just as previously, by S_Δ the random variable that takes value $\mathrm{Tr}(|\phi\rangle\langle\phi|\Delta)$ with probability $d\psi$, we have :

$$\|\Delta\|_{U_{\mathcal{H}}} = N \int_{\langle\psi|\psi\rangle=1} \big|\mathrm{Tr}(|\phi\rangle\langle\phi|\Delta)\big| d\psi = N\mathbb{E}\big(|S_\Delta|\big)$$

And for all $t \in \mathbb{N}^*$:

$$\begin{aligned}\mathbb{E}\big((S_\Delta)^t\big) &= \int_{\langle\psi|\psi\rangle=1} \big(\mathrm{Tr}_{\mathcal{H}}\big(|\psi\rangle\langle\psi|\Delta\big)\big)^t d\psi = \int_{\langle\psi|\psi\rangle=1} \mathrm{Tr}_{\mathcal{H}^{\otimes t}}\big(|\psi\rangle\langle\psi|^{\otimes t}\Delta^{\otimes t}\big) d\psi \\ &= \mathrm{Tr}_{\mathcal{H}^{\otimes t}}\left(\left(\int_{\langle\psi|\psi\rangle=1} |\psi\rangle\langle\psi|^{\otimes t} d\psi\right)\big(\Delta^{\otimes t}\big)\right) = \mathrm{Tr}_{\mathcal{H}^{\otimes t}}\left(\left(\frac{1}{N \times \cdots \times (N+t-1)} \sum_{\sigma \in \mathfrak{S}_t} U_\sigma\right)\big(\Delta^{\otimes t}\big)\right)\end{aligned}$$

4 Locally restricted measurements on a multi-partite quantum system

Let $\mathcal{H}_1, \ldots, \mathcal{H}_K$ be K finite dimensional Hilbert spaces (with $N_i := \dim H_i$ for all $1 \leq i \leq K$) and $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_K$ be their tensor product Hilbert space (of dimension $N := N_1 \times \cdots \times N_K$).

4.1 Different classes of locally restricted POVMs

Several classes of POVMs can be defined on the K-partite Hilbert space $\mathcal{H}$ due to various levels of locality restrictions.

The most restricted class of POVMs on $\mathcal{H}$ is the one of *local measurements* whose elements are tensor products of measurements on each of the sub-systems :

$$\mathbf{LO} := \left\{ \left(\bigotimes_{i=1}^{K} M_{j_i}^{(i)} \right)_{j_1 \in J_1, \ldots, j_K \in J_K} , \ \left(M_{j_i}^{(i)} \right)_{j_i \in J_i} \text{ POVM on } \mathcal{H}_i, \ 1 \leq i \leq K \right\}$$

More generally, **LOCC** is the class of measurements that can be implemented by a finite sequence of local operations on the sub-systems followed by classical communication between the parties.

We can then consider the class of *separable measurements* whose elements are the measurements on $\mathcal{H}$ that can be factorized as a tensor product of operators acting only on one sub-system :

$$\mathbf{SEP} := \left\{ \left(\bigotimes_{i=1}^{K} M_{j}^{(i)} \right)_{j \in J} \text{ POVM on } \mathcal{H} \right\}$$

Finally, there is the class of the *positive under partial transpose measurements* whose elements are the measurements on $\mathcal{H}$ that remain positive when partially transposed on any combination of the sub-systems :

$$\mathbf{PPT} := \left\{ (M_j)_{j \in J} \text{ POVM on } \mathcal{H}, \ \forall \ j \in J, \ \forall \ I \subset \{1, \ldots, K\}, \ M_j^{\Gamma_I} \geq \mathbb{0}_{\mathcal{H}} \right\}$$

where, for all $I \subset \{1, \ldots, K\}$ the partial transposition on $\mathcal{H}_I := \bigotimes_{i \in I} \mathcal{H}_i$ is defined by its action on factorized operators on $\mathcal{H}$: $(M_1 \otimes \cdots \otimes M_K)^{\Gamma_I} := \left(\bigotimes_{i \in I} M_i^T \right) \otimes \left(\bigotimes_{i \notin I} M_i \right)$, M_i^T denoting the usual transpose of M_i.
Let us point out that, even though the expression of a matrix's transpose depends on the chosen basis, its eigenvalues on the contrary are intrinsic. So the PPT notion is indeed well defined.

Remark 4.1 *It is clear from the definitions that we have the chain of inclusions :*

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

The most widely used inclusions in many questions related to operations on multi-partite quantum systems are certainly $\mathbf{LOCC} \subset \mathbf{SEP}$ *and* $\mathbf{LOCC} \subset \mathbf{PPT}$*. Indeed, however natural it might seem in this context, the class of* **LOCC** *operations is mathematically hard to characterize, contrary to the ones of* **SEP** *operations and even more so of* **PPT** *operations.*
Nevertheless, all those inclusions are well-known to be strict, at least in non trivial dimensions (the most intriguing being perhaps' $\mathbf{LOCC} \subsetneq \mathbf{SEP}$*, as proven in [20]).*
See also [18] for a very complete review on the subject.

4.2 An example of highly symmetric local POVMs : tensor products of t-design POVMs

One example of local POVMs on $\mathcal{H}$ we shall be concerned with are those that are tensor products of t-design POVMs on the $\mathcal{H}_i$, $1 \leq i \leq K$.

Let us be more definite. For all $1 \leq i \leq K$, let $\{(p_k^{(i)}, |\phi_k^{(i)}\rangle), 1 \leq k \leq m_i\}$ be a spherical t-design on $\mathcal{H}_i$, and $D_{(\mathcal{H}_i,t)} := \left(M_k^{(i)} := N_i p_k^{(i)} |\phi_k^{(i)}\rangle\langle\phi_k^{(i)}| \right)_{1 \leq k \leq m_i}$ be the associated t-design POVM.

We then consider the following local POVM on $\mathcal{H}$: $D_{(\mathcal{H},t)} := \bigotimes_{i=1}^{K} D_{(\mathcal{H}_i,t)} = \left(\bigotimes_{i=1}^{K} M_{k_i}^{(i)}\right)_{\substack{1\leq k_i\leq m_i \\ 1\leq i\leq K}}$.

For all Hermitian matrix Δ on $\mathcal{H}$, denoting, just as we did it before, by S_Δ the random variable taking value $\mathrm{Tr}_{\mathcal{H}}\left(\left(\bigotimes_{i=1}^{K}|\phi_{k_i}^{(i)}\rangle\langle\phi_{k_i}^{(i)}|\right)\Delta\right)$ with probability $\prod_{i=1}^{K} p_{k_i}^{(i)}$ for all $1\leq k_1\leq m_1,\ldots,1\leq k_K\leq m_K$, we have, by a straightforward generalization of equation 2 to the multi-partite case :

$$\|\Delta\|_{D_{(\mathcal{H},t)}} = \left(\prod_{i=1}^{K} N_i\right) \sum_{\substack{1\leq k_i\leq m_i \\ 1\leq i\leq K}} \left(\prod_{i=1}^{K} p_{k_i}^{(i)}\right) \left|\mathrm{Tr}_{\mathcal{H}}\left(\left(\bigotimes_{i=1}^{K}|\phi_{k_i}^{(i)}\rangle\langle\phi_{k_i}^{(i)}|\right)\Delta\right)\right| = N\mathbb{E}\big(|S_\Delta|\big)$$

And in the same way, generalizing equation 3 :

$$\begin{aligned}
\mathbb{E}\big(\left(S_\Delta\right)^t\big) =& \sum_{\substack{1\leq k_i\leq m_i \\ 1\leq i\leq K}} \left(\prod_{i=1}^{K} p_{k_i}^{(i)}\right) \mathrm{Tr}_{\mathcal{H}^{\otimes t}}\left(\left(\bigotimes_{i=1}^{K}|\phi_{k_i}^{(i)}\rangle\langle\phi_{k_i}^{(i)}|\right)^{\otimes t}\Delta^{\otimes t}\right) \\
=& \mathrm{Tr}_{\mathcal{H}^{\otimes t}}\left(\left(\bigotimes_{i=1}^{K}\left(\sum_{k_i=1}^{m_i} p_{k_i}^{(i)}|\phi_{k_i}^{(i)}\rangle\langle\phi_{k_i}^{(i)}|^{\otimes t}\right)\right)\left(\Delta^{\otimes t}\right)\right) \\
=& \mathrm{Tr}_{\mathcal{H}^{\otimes t}}\left(\left(\bigotimes_{i=1}^{K}\frac{1}{N_i\times\cdots\times(N_i+t-1)}\sum_{\sigma_i\in\mathfrak{S}_t} U_{\sigma_i}\right)\left(\Delta^{\otimes t}\right)\right) \qquad (4)
\end{aligned}$$

A special case is of course as previously mentioned the tensor product of the uniform POVMs on the $\mathcal{H}_i$, $1\leq i\leq K$: $U_{\mathcal{H}} := \bigotimes_{i=1}^{K} U_{\mathcal{H}_i}$ where, for all $1\leq i\leq K$, $U_{\mathcal{H}_i} := (N_i|\psi_i\rangle\langle\psi_i|d\psi_i)_{\langle\psi_i|\psi_i\rangle=1}$ (with $d\psi_i$ the uniform distribution on the unit vectors of $\mathcal{H}_i$, normalized by $\int_{\langle\psi_i|\psi_i\rangle=1} d\psi_i = 1$).

5 Bounds on the distinguishability norm associated with one single highly symmetric local measurement on a multi-partite quantum system

5.1 "Multi-partite modified 2-norm" : definition and preliminary results

Let as before $\mathcal{H}_i\equiv\mathbb{C}^{N_i}$, $1\leq i\leq K$, be K finite dimensional Hilbert spaces, and $\mathcal{H}=\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_K\equiv\mathbb{C}^N$, $N=N_1\times..\times N_K$, be their tensor product Hilbert space.

Definition 5.1 *For any Hermitian matrix Δ on $\mathcal{H}$, we define its "K-partite modified 2-norm" as :*

$$\|\Delta\|_{2(K)} := \sqrt{\sum_{I\subset\{1,\ldots,K\}} Tr_{\mathcal{H}\setminus\mathcal{H}_I}\left(Tr_{\mathcal{H}_I}\Delta\right)^2}$$

with the shorthand $\mathcal{H}_I := \mathcal{H}_{i_1}\otimes\cdots\otimes\mathcal{H}_{i_p}$ for $I=\{i_1,\ldots,i_p\}$.

Note that for $K=1$, the sum above only contains two terms, and the "1-partite modified 2-norm" $\|\Delta\|_{2(1)}=\sqrt{(\mathrm{Tr}\Delta)^2+\mathrm{Tr}(\Delta^2)}$ reduces to the usual 2-norm $\|\Delta\|_2=\sqrt{\mathrm{Tr}(\Delta^2)}$ on traceless Hermitian matrices Δ.

Theorem 5.2 *For all Hermitian matrix Δ on $\mathcal{H}$:*

$$Tr_{\mathcal{H}^{\otimes 2}}\left(\left(\bigotimes_{i=1}^{K}\sum_{\sigma_i\in\mathfrak{S}_2}U_{\sigma_i}\right)(\Delta^{\otimes 2})\right)=\|\Delta\|_{2(K)}^2 \tag{5}$$

Proof : To prove theorem 5.2, let us first deal with the following auxiliary problem.
Let $H=A\otimes B$ be a finite dimensional 2-partite Hilbert space. For all Hermitian matrix P on H and all unit vectors $|a\rangle,|a'\rangle\in A$ and $|b\rangle,|b'\rangle\in B$ we denote by $P_{a,b}^{a',b'}$ the matrix element $\langle b|\otimes\langle a|P|a'\rangle\otimes|b'\rangle$.
Let $\sigma=(\sigma_A,\sigma_B)\in\mathfrak{S}_2^2$ be a pair of permutations. For all Hermitian matrix Δ on H, we have, with $|a_1\rangle$, $|a_2\rangle$ and $|b_1\rangle$, $|b_2\rangle$ respectively running through an orthonormal basis of A and B :

$$\mathrm{Tr}_{H^{\otimes 2}}\big((U_{\sigma_A}\otimes U_{\sigma_B})(\Delta^{\otimes 2})\big)=\sum_{a_1,b_1,a_2,b_2}\Delta_{a_1,b_1}^{a_{\sigma_A(1)},b_{\sigma_B(1)}}\Delta_{a_2,b_2}^{a_{\sigma_A(2)},b_{\sigma_B(2)}}$$

We now consider the particular case $\sigma_A=id$ and $\sigma_B=(12)$, in which we have :

$$\mathrm{Tr}_{H^{\otimes 2}}\big((U_{\sigma_A}\otimes U_{\sigma_B})(\Delta^{\otimes 2})\big)=\sum_{a_1,b_1,a_2,b_2}\Delta_{a_1b_1}^{a_1b_2}\Delta_{a_2b_2}^{a_2b_1}=\sum_{b_1,b_2}\big[\mathrm{Tr}_A\Delta\big]_{b_1}^{b_2}\big[\mathrm{Tr}_A\Delta\big]_{b_2}^{b_1}=\mathrm{Tr}_B\left(\big[\mathrm{Tr}_A\Delta\big]^2\right)$$

Now, let us return to our initial problem.
For all $\sigma\in\mathfrak{S}_2^K$, we may write $\mathcal{H}=\mathcal{A}(\sigma)\otimes\mathcal{B}(\sigma)$, where $\mathcal{A}(\sigma):=\mathcal{H}_{i_1}\otimes\cdots\otimes\mathcal{H}_{i_a}$ with $\sigma_{i_1},\ldots,\sigma_{i_a}=id$ and $\mathcal{B}(\sigma):=\mathcal{H}_{i_{a+1}}\otimes\cdots\otimes\mathcal{H}_{i_K}$ with $\sigma_{i_{a+1}},\ldots,\sigma_{i_K}=(12)$. And hence :

$$\begin{aligned}\mathrm{Tr}_{\mathcal{H}^{\otimes 2}}\left(\left(\bigotimes_{i=1}^{K}\sum_{\sigma_i\in\mathfrak{S}_2}U_{\sigma_i}\right)(\Delta^{\otimes 2})\right)&=\sum_{\sigma\in\mathfrak{S}_2^K}\mathrm{Tr}_{\mathcal{H}^{\otimes 2}}\left(\left(\bigotimes_{i=1}^{K}U_{\sigma_i}\right)(\Delta^{\otimes 2})\right)\\&=\sum_{\sigma\in\mathfrak{S}_2^K}\mathrm{Tr}_{\mathcal{H}\setminus\mathcal{A}(\sigma)}\left(\mathrm{Tr}_{\mathcal{A}(\sigma)}\Delta\right)^2\\&=\sum_{I\subset\{1,\ldots,K\}}\mathrm{Tr}_{\mathcal{H}\setminus\mathcal{H}_I}\left(\mathrm{Tr}_{\mathcal{H}_I}\Delta\right)^2\end{aligned}$$

which, recalling the definition of $\|\cdot\|_{2(K)}$, is exactly the advertized result.

Theorem 5.3 *For all Hermitian matrix Δ on $\mathcal{H}$:*

$$Tr_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K}\sum_{\sigma_i\in\mathfrak{S}_4}U_{\sigma_i}\right)(\Delta^{\otimes 4})\right)\leq 18^K\|\Delta\|_{2(K)}^4 \tag{6}$$

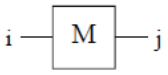
Proof : The proof of theorem 5.3 requires several intermediate results.

Since we cannot proceed by inspection of the 24^K K-tuples of $\mathfrak{S}_4^K$ as we could do it with the 2^K K-tuples of $\mathfrak{S}_2^K$, our first task will be to find a way of restricting our attention to only a few elements of $\mathfrak{S}_4$ without any loss of generality. In that end, our strategy can be described as follows.

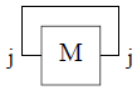
Consider a Hilbert space $\mathcal{H}$ and Hermitian matrices M_1,M_2,M_3,M_4 on $\mathcal{H}$.
For a given $\sigma\in\mathfrak{S}_4$ and the corresponding unitary matrix U_σ on $\mathcal{H}^{\otimes 4}$, we may write :
$\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\big(U_\sigma(M_1\otimes M_2\otimes M_3\otimes M_4)\big)=\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}(XY^\dagger)$ with X and Y two matrices on $\mathcal{H}^{\otimes 4}$ such that there exist $\sigma',\sigma''\in\mathfrak{S}_4$ such that $\begin{cases}\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}(XX^\dagger)=\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\big(U_{\sigma'}(M_1\otimes M_2\otimes M_2\otimes M_1)\big)\\ \mathrm{Tr}_{\mathcal{H}^{\otimes 4}}(YY^\dagger)=\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\big(U_{\sigma''}(M_4\otimes M_3\otimes M_3\otimes M_4)\big)\end{cases}$.

In order to easily visualize into which pair $(\sigma',\sigma'')\in\mathfrak{S}_4\times\mathfrak{S}_4$ each $\sigma\in\mathfrak{S}_4$ splits, we can make use of Penrose's ingenious tensor diagrams, which we briefly explain here (see [10]) :

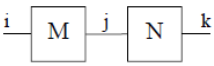
For any Hermitian matrix M on $\mathcal{H}$ and unit vectors $|i\rangle, |j\rangle \in \mathcal{H}$ we represent the matrix element $\langle i|M|j\rangle$ by the following diagram with terminals :



Then, summing matrix elements for a unit vector running through an orthonormal basis of $\mathcal{H}$ is represented by joining the corresponding terminals.
So for instance, $\mathrm{Tr}_{\mathcal{H}}(M) = \sum_j \langle j|M|j\rangle$ is represented by :



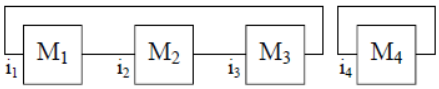
And in the same way, $\langle i|MN|k\rangle = \sum_j \langle i|M|j\rangle\langle j|N|k\rangle$ is represented by :



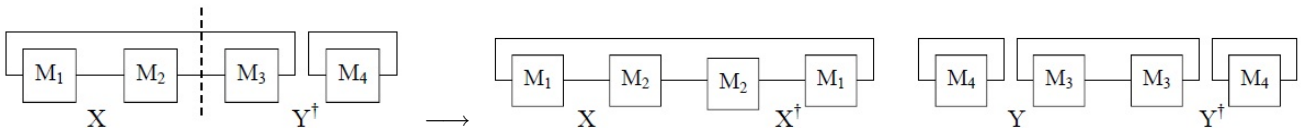
Yet, for Hermitian matrices M_1, M_2, M_3, M_4 on $\mathcal{H}$ and $\sigma \in \mathfrak{S}_4$, we have :

$$\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\big(U_\sigma(M_1 \otimes M_2 \otimes M_3 \otimes M_4)\big) = \sum_{i_1,i_2,i_3,i_4\rangle} \langle i_|M_1|i_{\sigma(1)}\rangle\langle i_2|M_2|i_{\sigma(2)}\rangle\langle i_3|M_3|i_{\sigma(3)}\rangle\langle i_4|M_4|i_{\sigma(4)}\rangle$$

So for instance, $\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\big(U_{(123)}(M_1 \otimes M_2 \otimes M_3 \otimes M_4)\big)$ is represented by :



And in this case, the splitting procedure described above can be schematically represented by :



which means that $\sigma = (123)$ splits into $\sigma' = (1234)$ and $\sigma'' = (23)$

Then, using the Cauchy-Schwarz inequality, we get :

$$\begin{aligned}\big|\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\big(U_\sigma(M_1 \otimes M_2 \otimes M_3 \otimes M_4)\big)\big| &= \big|\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}(XY^\dagger)\big| \\ &\leq \sqrt{\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}(XX^\dagger)\ \mathrm{Tr}_{\mathcal{H}^{\otimes 4}}(YY^\dagger)} \\ &= \sqrt{\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\big(U_{\sigma'}(M_1 \otimes M_2 \otimes M_2 \otimes M_1)\big)\ \mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\big(U_{\sigma''}(M_4 \otimes M_3 \otimes M_3 \otimes M_4)\big)}\end{aligned}$$

What we have gained by doing so is that σ' and σ'' cannot be any permutation : they necessarily belong to the subset $\mathfrak{S} := \{id, (14), (23), (1234), (1432), (12)(34), (14)(23)\}$ of $\mathfrak{S}_4$ containing the permutations that are equal to their opposite under the exchange $1 \leftrightarrow 4$ and $2 \leftrightarrow 3$ (i.e. under the conjugation by $(14)(23)$).

We now have to see more precisely in which pair $(\sigma', \sigma'') \in \mathfrak{S} \times \mathfrak{S}$ each of the elements $\sigma \in \mathfrak{S}_4$ breaks down. First of all, it is clear that the seven elements of $\mathfrak{S}$ split into twice themselves. Similarly, if

Conjugacy class	σ	σ'	σ''
(1^4)	id	id	id
$(2^1,1^2)$	(12)	(12)(34)	id
	(13)	(14)	(23)
	(14)	(14)	(14)
	(23)	(23)	(23)
	(24)	(23)	(14)
	(34)	id	(12)(34)
(2^2)	(12)(34)	(12)(34)	(12)(34)
	(13)(24)	(14)(23)	(14)(23)
	(14)(23)	(14)(23)	(14)(23)
$(3^1,1^1)$	(123)	(1234)	(23)
	(132)	(1432)	(23)
	(124)	(1234)	(14)
	(142)	(1432)	(14)
	(134)	(14)	(1234)
	(143)	(14)	(1432)
	(234)	(23)	(1234)
	(243)	(23)	(1432)
(4^1)	(1234)	(1234)	(1234)
	(1243)	(1234)	(1432)
	(1324)	(14)(23)	(14)(23)
	(1342)	(1432)	(1234)
	(1432)	(1432)	(1432)
	(1423)	(14)(23)	(14)(23)

Figure 1: Table of the splitting map Split : $\mathfrak{S}_4 \longrightarrow \mathfrak{S} \times \mathfrak{S}$, Split$(\sigma) = (\sigma', \sigma'')$, grouped according to conjugacy classes of σ.

σ splits into (σ', σ''), then its conjugate $(14)(23)\sigma(14)(23)$ splits into (σ'', σ'). We are thus left with actually looking at 9 permutations, one of which being invariant under the conjugation by (14)(23) and the 8 others providing the result for their 8 respective conjugates by switching σ' and σ''. The resulting splitting map Split : $\sigma \in \mathfrak{S}_4 \mapsto (\sigma', \sigma'') \in \mathfrak{S} \times \mathfrak{S}$ for each $\sigma \in \mathfrak{S}_4$ can then easily be constructed and looked up in the table of Figure 1.

Turning back to the problem we are dealing with, we would thus have for all $\sigma \in \mathfrak{S}_4^K$, applying the splitting map to each σ_i, $1 \leq i \leq K$:

$$\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K} U_{\sigma_i}\right)(\Delta^{\otimes 4})\right) \leq \sqrt{\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K} U_{\sigma_i'}\right)(\Delta^{\otimes 4})\right)}\sqrt{\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K} U_{\sigma_i''}\right)(\Delta^{\otimes 4})\right)} \qquad (7)$$

So what we have for the moment is that, in order to bound the trace $\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K} U_{\sigma_i}\right)(\Delta^{\otimes 4})\right)$ for any $\sigma \in \mathfrak{S}_4^K$, it would be sufficient to bound it for $\sigma \in \mathfrak{S}^K$.

With this aim in view, let us deal with the following auxiliary problem.

Let $H = A \otimes \cdots \otimes G$ be a finite dimensional 7-partite Hilbert space. For all Hermitian matrix P on H and all unit vectors $|a\rangle, |a'\rangle \in A, \ldots, |g\rangle, |g'\rangle \in G$ we denote by $P_{a,\ldots,g}^{a',\ldots,g'}$ the matrix element $\langle g| \otimes \cdots \otimes \langle a|P|a'\rangle \otimes \cdots \otimes |g'\rangle$.

Let $\sigma = (\sigma_A, .., \sigma_G) \in \mathfrak{S}_4^7$ be a 7-tuple of permutations.
For all hermitian matrix Δ on H, we have, with the $|a_q\rangle, \ldots, |g_q\rangle$, $1 \leq q \leq 4$, respectively running

through an orthonormal basis of $A, \dots, G$:

$$\mathrm{Tr}_{H^{\otimes 4}}\big((U_{\sigma_A} \otimes \cdots \otimes U_{\sigma_G})(\Delta^{\otimes 4})\big) = \sum_{\substack{a_1,\dots,g_1\\ a_2,\dots,g_2\\ a_3,\dots,g_3\\ a_4,\dots,g_4}} \prod_{q=1}^{4} \Delta_{a_q,\dots,g_q}^{a_{\sigma_A(q)},\dots,g_{\sigma_G(q)}}$$

We now consider the particular case $\sigma_A = id$, $\sigma_B = (14)$, $\sigma_C = (23)$, $\sigma_D = (1234)$, $\sigma_E = (1432)$, $\sigma_F = (12)(34)$ and $\sigma_G = (14)(23)$, in which we have :

$$\begin{aligned}
&\mathrm{Tr}_{H^{\otimes 4}}\big((U_{\sigma_A} \otimes \cdots \otimes U_{\sigma_G})(\Delta^{\otimes 4})\big)\\
&= \sum_{\substack{a_1,\dots,g_1\\ a_2,\dots,g_2\\ a_3,\dots,g_3\\ a_4,\dots,g_4}} \Delta_{a_1b_4c_1d_2e_4f_2g_4}^{a_1b_4c_1d_2e_4f_2g_4} \Delta_{a_2b_2c_3d_3e_1f_1g_3}^{a_2b_2c_3d_3e_1f_1g_3} \Delta_{a_3b_3c_2d_4e_2f_4g_2}^{a_3b_3c_2d_4e_2f_4g_2} \Delta_{a_4b_1c_4d_1e_3f_3g_1}^{a_4b_1c_4d_1e_3f_3g_1}\\
&= \sum_{\substack{b_1,d_1,\dots,g_1\\ c_2,\dots,g_2\\ c_3,\dots,g_3\\ b_4,d_4,\dots,g_4}} \Big[\big(\mathrm{Tr}_{A\otimes C}\Delta\big)^{\Gamma_E}\Big]_{b_1d_1e_4f_1g_1}^{b_4d_2e_1f_2g_4} \Big[\big(\mathrm{Tr}_{A\otimes B}\Delta\big)^{\Gamma_E}\Big]_{c_2d_2e_1f_2g_2}^{c_3d_3e_2f_1g_3} \Big[\big(\mathrm{Tr}_{A\otimes B}\Delta\big)^{\Gamma_E}\Big]_{c_3d_3e_2f_3g_3}^{c_2d_4e_3f_4g_2} \Big[\big(\mathrm{Tr}_{A\otimes C}\Delta\big)^{\Gamma_E}\Big]_{b_4d_4e_3f_4g_4}^{b_1d_1e_4f_3g_1}
\end{aligned}$$

where Γ_E denotes the partial transposition on E.

Let us introduce the so-called *maximally entangled matrix* on $F \otimes F$: $M_{F\otimes F} := \sum_{f,\widetilde{f}} |f\rangle \otimes |f\rangle\langle\widetilde{f}| \otimes \langle\widetilde{f}|$.

Now, letting $J := C \otimes D \otimes E \otimes G$, $P := \big(\mathrm{Tr}_{A\otimes B}\Delta\big)^{\Gamma_E}$ and $R := (P \otimes \mathbb{1}_F)(\mathbb{1}_J \otimes M_{F\otimes F})(P \otimes \mathbb{1}_F)$, we have that for all $j, j', f, f', \widetilde{f}, \widetilde{f}'$:

$$R_{j,f,\widetilde{f}}^{j',f',\widetilde{f}'} = \sum_{\substack{j'',j'''\\ f'',f'''\\ \widetilde{f}'',\widetilde{f}'''}} \Big(P_{j,f}^{j'',f''}\delta_{\widetilde{f}''=\widetilde{f}}\Big)\Big(\delta_{j'''=j''}\delta_{\widetilde{f}''=f'',\widetilde{f}'''=f'''}\Big)\Big(P_{j''',f'''}^{j',f'}\delta_{\widetilde{f}'''=\widetilde{f}'}\Big) = \sum_{j''} P_{j,f}^{j'',\widetilde{f}} P_{j'',\widetilde{f}'}^{j',f'}$$

Likewise, letting $K := B \otimes D \otimes E \otimes G$, $Q := \big(\mathrm{Tr}_{A\otimes C}\Delta\big)^{\Gamma_E}$ and $S := (Q \otimes \mathbb{1}_F)(\mathbb{1}_K \otimes M_{F\otimes F})(Q \otimes \mathbb{1}_F)$, we have that for all $k, k', f, f', \widetilde{f}, \widetilde{f}'$: $S_{k,f',\widetilde{f}'}^{k',f,\widetilde{f}} = \sum_{k''} Q_{k,f'}^{k'',\widetilde{f}'} Q_{k'',\widetilde{f}}^{k',f}$.

We now just have to make the following identifications :

$$\begin{cases}
j := (c_2, d_2, e_1, g_2), \quad j' := (c_2, d_4, e_3, g_2), \quad j'' := (c_3, d_3, e_2, g_3)\\
k := (b_4, d_4, e_3, g_4), \quad k' := (b_4, d_2, e_1, g_4), \quad k'' := (b_1, d_1, e_4, g_1)\\
f := f_2, \quad f' := f_4, \quad \widetilde{f} := f_1, \quad \widetilde{f}' := f_3
\end{cases}$$

And to notice that we can actually sum on j'' and k'' independently.

We thus get :

$$\begin{aligned}\mathrm{Tr}_{H^{\otimes 4}}\big((U_{\sigma_A}\otimes\cdots\otimes U_{\sigma_G})(\Delta^{\otimes 4})\big) =& \sum_{\substack{e_1,f_1\\ c_2,d_2,f_2,g_2\\ e_3,f_3\\ b_4,d_4,f_4,g_4}} R^{c_2,d_4,e_3,g_2,f_4,f_3}_{c_2,d_2,e_1,g_2,f_2,f_1} S^{b_4,d_2,e_1,g_4,f_2,f_1}_{b_4,d_4,e_3,g_4,f_4,f_3}\\ =&\sum_{\substack{e_1,f_1\\ d_2,f_2\\ e_3,f_3\\ d_4,f_4}} \big(\mathrm{Tr}_{C\otimes G}R\big)^{d_4,e_3,f_4,f_3}_{d_2,e_1,f_2,f_1}\big(\mathrm{Tr}_{B\otimes G}S\big)^{d_2,e_1,f_2,f_1}_{d_4,e_3,f_4,f_3}\\ =&\mathrm{Tr}_{D\otimes E\otimes F\otimes F}\big[\big(\mathrm{Tr}_{C\otimes G}R\big)\big(\mathrm{Tr}_{B\otimes G}S\big)\big]\end{aligned}$$

Yet, defining $\widetilde{P}$ and $\widetilde{Q}$ as $\widetilde{P} := \big(P\otimes \mathbb{1}_F\big)\left(\mathbb{1}_J\otimes\sum_f |f\rangle\otimes|f\rangle\right)$ and $\widetilde{Q} := \big(Q\otimes \mathbb{1}_F\big)\left(\mathbb{1}_J\otimes\sum_f |f\rangle\otimes|f\rangle\right)$, we see that $R=\widetilde{P}\widetilde{P}^\dagger$ and $S=\widetilde{Q}\widetilde{Q}^\dagger$. Hence R and S are positive matrices, and so are $\mathrm{Tr}_{C\otimes G}R$ and $\mathrm{Tr}_{B\otimes G}S$. Thus, using the fact that, for positive matrices V and W, $\mathrm{Tr}(VW)\leq(\mathrm{Tr}V)(\mathrm{Tr}W)$, we get :

$$\mathrm{Tr}_{D\otimes E\otimes F\otimes F}\Big(\big(\mathrm{Tr}_{C\otimes G}R\big)\big(\mathrm{Tr}_{B\otimes G}S\big)\Big)\leq\Big(\mathrm{Tr}_{(H\backslash A\otimes B)\otimes F}R\Big)\Big(\mathrm{Tr}_{(H\backslash A\otimes C)\otimes F}S\Big)$$

Now : $\mathrm{Tr}_{(H\backslash A\otimes B)\otimes F}R=\mathrm{Tr}_{H\backslash A\otimes B}\big(P^2\left(\mathbb{1}_J\otimes\mathrm{Tr}_F M_{F\otimes F}\right)\big)=\mathrm{Tr}_{H\backslash A\otimes B}\big(P^2\left(\mathbb{1}_J\otimes\mathbb{1}_F\right)\big)=\mathrm{Tr}_{H\backslash A\otimes B}P^2$
With the similar result for S and Q : $\mathrm{Tr}_{(H\backslash A\otimes C)\otimes F}S=\mathrm{Tr}_{H\backslash A\otimes C}Q^2$

And finally : $\mathrm{Tr}_{H\backslash A\otimes B}P^2=\mathrm{Tr}_{H\backslash A\otimes B}\Big(\big(\mathrm{Tr}_{A\otimes B}\Delta\big)^{\Gamma_E}\Big)^2=\mathrm{Tr}_{H\backslash A\otimes B}\big(Tr_{A\otimes B}\Delta\big)^2$
With the similar result for Q : $\mathrm{Tr}_{H\backslash A\otimes C}Q^2=\mathrm{Tr}_{H\backslash A\otimes C}\big(\mathrm{Tr}_{A\otimes C}\Delta\big)^2$

So in the end, what we eventually get is :

$$\mathrm{Tr}_{H^{\otimes 4}}\big((U_{\sigma_A}\otimes\cdots\otimes U_{\sigma_G})(\Delta^{\otimes 4})\big)\leq\Big[\mathrm{Tr}_{H\backslash A\otimes B}\big(Tr_{A\otimes B}\Delta\big)^2\Big]\Big[\mathrm{Tr}_{H\backslash A\otimes C}\big(Tr_{A\otimes C}\Delta\big)^2\Big]\tag{8}$$

Bearing this useful result in mind, we can now return to our initial problem.

For all $\pi\in\mathfrak{S}^K$, we can define the following factors of the global Hilbert space $\mathcal{H}$:

- $\mathcal{A}(\pi):=\mathcal{H}_{i_1}\otimes\cdots\otimes\mathcal{H}_{i_a}$ with $\pi_{i_1},\ldots,\pi_{i_a}=id$
- $\mathcal{B}(\pi):=\mathcal{H}_{i_{a+1}}\otimes\cdots\otimes\mathcal{H}_{i_b}$ with $\pi_{i_{a+1}},\ldots,\pi_{i_b}=(14)$
- $\mathcal{C}(\pi):=\mathcal{H}_{i_{b+1}}\otimes\cdots\otimes\mathcal{H}_{i_c}$ with $\pi_{i_{b+1}},\ldots,\pi_{i_c}=(23)$
- $\mathcal{D}(\pi):=\mathcal{H}_{i_{c+1}}\otimes\cdots\otimes\mathcal{H}_{i_d}$ with $\pi_{i_{c+1}},\ldots,\pi_{i_d}=(1234)$
- $\mathcal{E}(\pi):=:\mathcal{H}_{i_{d+1}}\otimes\cdots\otimes\mathcal{H}_{i_e}$ with $\pi_{i_{d+1}},\ldots,\pi_{i_e}=(1432)$
- $\mathcal{F}(\pi):=\mathcal{H}_{i_{e+1}}\otimes\cdots\otimes\mathcal{H}_{i_f}$ with $\pi_{i_{e+1}},\ldots,\pi_{i_f}=(12)(34)$
- $\mathcal{G}(\pi):=\mathcal{H}_{i_{f+1}}\otimes\cdots\otimes\mathcal{H}_{i_K}$ with $\pi_{i_{f+1}},\ldots,\pi_{i_K}=(14)$

$\mathcal{H}$ can then be written as : $\mathcal{H}=\mathcal{A}(\pi)\otimes\mathcal{B}(\pi)\otimes\mathcal{C}(\pi)\otimes\mathcal{D}(\pi)\otimes\mathcal{E}(\pi)\otimes\mathcal{F}(\pi)\otimes\mathcal{G}(\pi)$.

Hence, using consecutively the two intermediate equations 7 and 8, and twice the arithmetic-geometric mean inequality, we have :

$$
\begin{aligned}
&\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K}\sum_{\sigma_i\in\mathfrak{S}_4}U_{\sigma_i}\right)\left(\Delta^{\otimes 4}\right)\right)\\
&=\sum_{\sigma\in\mathfrak{S}_4^K}\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K}U_{\sigma_i}\right)\left(\Delta^{\otimes 4}\right)\right)\\
&\leq\sum_{\sigma\in\mathfrak{S}_4^K}\sqrt{\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K}U_{\sigma'_i}\right)\left(\Delta^{\otimes 4}\right)\right)}\sqrt{\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K}U_{\sigma''_i}\right)\left(\Delta^{\otimes 4}\right)\right)}\\
&\leq\sum_{\sigma\in\mathfrak{S}_4^K}\sqrt{\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{B}(\sigma')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{B}(\sigma')}\Delta\right)^2\right]\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{C}(\sigma')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{C}(\sigma')}\Delta\right)^2\right]}\\
&\qquad\times\sqrt{\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{B}(\sigma'')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{B}(\sigma'')}\Delta\right)^2\right]\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{C}(\sigma'')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{C}(\sigma'')}\Delta\right)^2\right]}\\
&\leq\sum_{\sigma\in\mathfrak{S}_4^K}\frac{1}{2}\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{B}(\sigma')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{B}(\sigma')}\Delta\right)^2\right]\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{C}(\sigma')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{C}(\sigma')}\Delta\right)^2\right]\\
&\qquad+\frac{1}{2}\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{B}(\sigma'')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{B}(\sigma'')}\Delta\right)^2\right]\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{C}(\sigma'')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{C}(\sigma'')}\Delta\right)^2\right]\\
&=\sum_{\sigma\in\mathfrak{S}_4^K}\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{B}(\sigma')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{B}(\sigma')}\Delta\right)^2\right]\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{C}(\sigma')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{C}(\sigma')}\Delta\right)^2\right]\\
&\leq\sum_{\sigma\in\mathfrak{S}_4^K}\frac{1}{2}\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{B}(\sigma')}\left(Tr_{\mathcal{A}\otimes\mathcal{B}(\sigma')}\Delta\right)^2\right]^2+\frac{1}{2}\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{C}(\sigma')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{C}(\sigma')}\Delta\right)^2\right]^2\\
&=\sum_{\sigma\in\mathfrak{S}_4^K}\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}\otimes\mathcal{B}(\sigma')}\left(\mathrm{Tr}_{\mathcal{A}\otimes\mathcal{B}(\sigma')}\Delta\right)^2\right]^2
\end{aligned}
$$

where we made use in the last lines of the symmetry of the roles played by σ' and σ'' on the one hand, $\mathcal{B}(\sigma')$ and $\mathcal{C}(\sigma')$ on the other, when σ spans $\mathfrak{S}_4^K$.

The only thing that ultimately remains to notice is that, amongst the 24 permutations π of $\mathfrak{S}_4$, 2 of them are such that $\pi'=id$ (namely id and (34)) and 4 of them are such that $\pi'=(14)$ (namely (14), (13), (134) and (143)). Hence, for all $1\leq m\leq K$, there are $6^m\times 18^{K-m}$ K-tuples of permutations whose first m elements π are such that π' is either id or (14), and whose following $K-m$ elements π are such that π' is neither id nor (14). So for one given subset $\{i_1,\ldots,i_m\}\subset\{1,\ldots,K\}$, there are $6^m\times 18^{K-m}$ K-tuples of permutations σ that are such that $\mathcal{A}\otimes\mathcal{B}(\sigma')=H_{i_1}\otimes\cdots\otimes H_{i_m}$.

Therefore, we finally obtain :

$$
\begin{aligned}
\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K}\sum_{\sigma_i\in\mathfrak{S}_4}U_{\sigma_i}\right)\left(\Delta^{\otimes 4}\right)\right)&\leq 18^K\sum_{I\subset\{1,..,K\}}\left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{H}_I}\left(\mathrm{Tr}_{\mathcal{H}_I}\Delta\right)^2\right]^2\\
&\leq 18^K\left[\sum_{I\subset\{1,..,K\}}\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{H}_I}\left(\mathrm{Tr}_{\mathcal{H}_I}\Delta\right)^2\right]^2
\end{aligned}
$$

which, recalling the definition of $\|\cdot\|_{2(K)}$, is exactly the advertized result.

5.2 Bounds on the distinguishability norm associated with tensor products of t-design POVMs

In what follows, we consider $D_{(\mathcal{H},t)}$ a tensor product of t-design POVMs on the $\mathcal{H}_i$, $1 \leq i \leq K$, as defined in section 4.2. For all Hermitian matrix Δ on $\mathcal{H}$, we will also denote, exactly as in the latter, by S_Δ the random variable such that $\|\Delta\|_{D_{(\mathcal{H},t)}} = N\mathbb{E}\big(|S_\Delta|\big)$.

5.2.1 Upper bound on $\|\cdot\|_{D_{(\mathcal{H},t)}}$ when $t \geq 2$

For any random variable S, we have by Jensen's inequality : $\mathbb{E}(|S|) \leq \sqrt{\mathbb{E}(S^2)}$.
Applied to S_Δ, it implies the following upper bound on $\|\Delta\|_{D_{(\mathcal{H},t)}}$:

$$\|\Delta\|_{D_{(\mathcal{H},t)}} \leq N\sqrt{\mathbb{E}\big((S_\Delta)^2\big)} \tag{9}$$

Yet if $t \geq 2$, we have using equation 4 :

$$\mathbb{E}\big((S_\Delta)^2\big) = \mathrm{Tr}_{\mathcal{H}^{\otimes 2}}\left(\left(\bigotimes_{i=1}^{K} \frac{1}{N_i(N_i+1)} \sum_{\sigma_i \in \mathfrak{S}_2} U_{\sigma_i}\right)\left(\Delta^{\otimes 2}\right)\right)$$

So plugging that into equation 9 we get that if $t \geq 2$:

$$\|\Delta\|_{D_{(\mathcal{H},t)}} \leq \left[\prod_{i=1}^{K} \frac{N_i}{N_i+1} \mathrm{Tr}_{\mathcal{H}^{\otimes 2}}\left(\left(\bigotimes_{i=1}^{K} \sum_{\sigma_i \in \mathfrak{S}_2} U_{\sigma_i}\right)\left(\Delta^{\otimes 2}\right)\right)\right]^{1/2}$$

And using theorem 5.2, we eventually get the following upper bound on $\|\Delta\|_{D_{(\mathcal{H},t)}}$ when $t \geq 2$:

$$\|\Delta\|_{D_{(\mathcal{H},t)}} \leq \|\Delta\|_{2(K)} \tag{10}$$

5.2.2 Lower bound on $\|\cdot\|_{D_{(\mathcal{H},t)}}$ when $t \geq 4$

For any random variable S, we have by Hölder's inequality : $\mathbb{E}(S^2) = \mathbb{E}(|S|^{2/3}|S|^{4/3}) \leq \mathbb{E}(|S|)^{2/3}\mathbb{E}(S^4)^{1/3}$
i.e. $\mathbb{E}(|S|) \geq \sqrt{\dfrac{\mathbb{E}(S^2)^3}{\mathbb{E}(S^4)}}$.
Applied to S_Δ, it implies the following lower bound on $\|\Delta\|_{D_{(\mathcal{H},t)}}$:

$$\|\Delta\|_{D_{(\mathcal{H},t)}} \geq N\sqrt{\frac{\mathbb{E}\big((S_\Delta)^2\big)^3}{\mathbb{E}\big((S_\Delta)^4\big)}} \tag{11}$$

Yet if $t \geq 4$, we have using equation 4 :

$$\begin{aligned}
\mathbb{E}\big((S_\Delta)^2\big) =& \mathrm{Tr}_{\mathcal{H}^{\otimes 2}}\left(\left(\bigotimes_{i=1}^{K} \frac{1}{N_i(N_i+1)} \sum_{\sigma_i \in \mathfrak{S}_2} U_{\sigma_i}\right)\left(\Delta^{\otimes 2}\right)\right) \\
\mathbb{E}\big((S_\Delta)^4\big) =& \mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^{K} \frac{1}{N_i(N_i+1)(N_i+2)(N_i+3)} \sum_{\sigma_i \in \mathfrak{S}_4} U_{\sigma_i}\right)\left(\Delta^{\otimes 4}\right)\right)
\end{aligned}$$

So plugging that into equation 11 we get that if $t \geq 4$:

$$\|\Delta\|_{D_{(\mathcal{H},t)}} \geq \left[\prod_{i=1}^{K} \frac{(N_i+2)(N_i+3)}{(N_i+1)^2} \frac{\left[\mathrm{Tr}_{\mathcal{H}^{\otimes 2}} \left(\left(\bigotimes_{i=1}^{K} \sum_{\sigma_i \in \mathfrak{S}_2} U_{\sigma_i} \right) (\Delta^{\otimes 2}) \right) \right]^3}{\mathrm{Tr}_{\mathcal{H}^{\otimes 4}} \left(\left(\bigotimes_{i=1}^{K} \sum_{\sigma_i \in \mathfrak{S}_4} U_{\sigma_i} \right) (\Delta^{\otimes 4}) \right)} \right]^{1/2}$$

And using theorems 5.2 and 5.3, we eventually get the following lower bound on $\|\Delta\|_{D_{(\mathcal{H},t)}}$ for $t \geq 4$:

$$\|\Delta\|_{D_{(\mathcal{H},t)}} \geq \frac{1}{18^{K/2}} \|\Delta\|_{2(K)} \tag{12}$$

5.2.3 Equivalence between $\|\cdot\|_{D_{(\mathcal{H},t)}}$ and $\|\cdot\|_{2(K)}$ when $t \geq 4$

Combining equations 10 and 12, we get the following estimate on $\|\Delta\|_{D_{(\mathcal{H},t)}}$ when $t \geq 4$:

$$\frac{1}{18^{K/2}} \|\Delta\|_{2(K)} \leq \|\Delta\|_{D_{(\mathcal{H},t)}} \leq \|\Delta\|_{2(K)} \tag{13}$$

This solves an open problem from [11], showing that for any number K of parties, the distinguishability norm associated with a tensor product of K local t-design POVMs is essentially equivalent to a certain K-partite relative of the 2-norm when $t \geq 4$. Indeed, the norm equivalence is in terms of constants of domination which depend only on the number of local parties, and not on the local dimensions.

5.3 Lower bound on $\lambda(U_{\mathcal{H}})$

As already mentioned, the results obtained for POVMs on $\mathcal{H}$ that are tensor products of t-design POVMs on the $\mathcal{H}_i$, $1 \leq i \leq K$, especially apply to the case of $U_{\mathcal{H}}$ the tensor product of the uniform POVMs (i.e. ∞-design POVMs) on the $\mathcal{H}_i$, $1 \leq i \leq K$.
From equation 13, this means that for all Hermitian matrix Δ on $\mathcal{H}$:

$$\frac{1}{18^{K/2}} \|\Delta\|_{2(K)} \leq \|\Delta\|_{U_{\mathcal{H}}} \leq \|\Delta\|_{2(K)}$$

This particularly implies that for all Hermitian matrix Δ on $\mathcal{H}$:

$$\|\Delta\|_{U_{\mathcal{H}}} \geq \frac{1}{18^{K/2}} \|\Delta\|_{2(K)} \geq \frac{1}{18^{K/2}} \|\Delta\|_2 \geq \frac{1}{18^{K/2}\sqrt{N}} \|\Delta\|_1$$

where we just used the immediate $\|\Delta\|_2 \leq \|\Delta\|_{2(K)}$ followed by the Cauchy-Schwarz inequality for the Hilbert-Schmidt inner product (*cf* appendix A.1) $\|\Delta\|_1 = \mathrm{Tr}|\Delta| \leq \sqrt{\mathrm{Tr}(\mathbb{1}_{\mathcal{H}}^2)\mathrm{Tr}(\Delta^2)} = \sqrt{N}\|\Delta\|_2$.

As a consequence : $\lambda_0(U_{\mathcal{H}}) \geq \lambda(U_{\mathcal{H}}) \geq \frac{1}{18^{K/2}\sqrt{N}}$

5.4 Upper bound on $\lambda_0(U_{\mathcal{H}})$

Our aim is now to show that the lower bound previously found for the constant of domination $\lambda_0(U_{\mathcal{H}})$ is actually close to optimal. For that, it would be sufficient to exhibit a traceless Hermitian matrix $\Delta \neq \mathbb{0}_{\mathcal{H}}$ on $\mathcal{H}$ such that $\|\Delta\|_{U_{\mathcal{H}}} \leq \frac{1}{\alpha^{K/2}\sqrt{N}} \|\Delta\|_1$ with $\alpha > 1$. This would indeed imply that $\lambda_0(U_{\mathcal{H}}) \leq \frac{1}{\alpha^{K/2}\sqrt{N}}$ with $\alpha > 1$, and subsequently that the distinguishing power of $U_{\mathcal{H}}$ "truly" decreases as $\frac{1}{C^{K/2}\sqrt{N}}$ with $C > 1$ when the dimension N of the global system $\mathcal{H}$ and the number K of sub-systems increase (independently).

In that end, we will make use of the following general result.

Theorem 5.4 *Let $\mathcal{H}(n)$ be a finite n-dimensional Hilbert space ($n \geq 2$) equipped with an orthonormal basis $\{|k\rangle, 1 \leq k \leq n\}$. We denote by $U_{\mathcal{H}(n)}$ the uniform POVM on $\mathcal{H}(n)$.*

For all $a \leq \lfloor n/2 \rfloor$, the Hermitian matrix $\Delta(a) := \frac{1}{2a}\left(\sum_{k=1}^{a} |k\rangle\langle k| - \sum_{k=a+1}^{2a} |k\rangle\langle k|\right)$ on $\mathcal{H}(n)$ satisfies : $Tr(\Delta(a)) = 0$, $\|\Delta(a)\|_1 = 1$ and $\|\Delta(a)\|_{U_{\mathcal{H}(n)}} = \frac{(2a)!}{(2^a a!)^2}$.

So in particular : $Tr(\Delta(\lfloor n/2 \rfloor)) = 0$, $\|\Delta(\lfloor n/2 \rfloor)\|_1 = 1$ and $\|\Delta(\lfloor n/2 \rfloor)\|_{U_{\mathcal{H}(n)}} \underset{n\to\infty}{\sim} \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}}$.

Proof : Each unit vector $|\psi\rangle \in \mathcal{H}(n)$ may be written as $|\psi\rangle = \sum_{k=1}^{n}(\psi_k + i\psi'_k)|k\rangle$ with $\psi_k, \psi'_k \in \mathbb{R}$ for all $1 \leq k \leq n$ and $\sum_{k=1}^{n}(\psi_k)^2 + (\psi'_k)^2 = 1$. So for all $a \leq \lfloor n/2 \rfloor$:

$$\begin{aligned}
\|\Delta(a)\|_{U_{\mathcal{H}(n)}} &= n\int_{\langle\psi|\psi\rangle=1} \big|\mathrm{Tr}\big(|\psi\rangle\langle\psi|\Delta(a)\big)\big| d\psi \\
&= n\int_{\langle\psi|\psi\rangle=1} \frac{1}{2a}\left|\sum_{k=1}^{a}\big[(\psi_k)^2 + (\psi'_k)^2\big] - \sum_{k=a+1}^{2a}\big[(\psi_k)^2 + (\psi'_k)^2\big]\right| d\psi \\
&= \frac{n}{2a}\mathbb{E}_{\substack{\psi_k,\psi'_k\sim\mathcal{N}(0,1/2n)\\ 1\leq k\leq n}}\left(\left|\sum_{k=1}^{a}\big[(\psi_k)^2 + (\psi'_k)^2\big] - \sum_{k=a+1}^{2a}\big[(\psi_k)^2 + (\psi'_k)^2\big]\right|\right) \\
&= \frac{1}{4a}\mathbb{E}_{\substack{\widetilde{\psi}_k,\widetilde{\psi}'_k\sim\mathcal{N}(0,1)\\ 1\leq k\leq n}}\left(\left|\sum_{k=1}^{a}\big[(\widetilde{\psi}_k)^2 + (\widetilde{\psi}'_k)^2\big] - \sum_{k=a+1}^{2a}\big[(\widetilde{\psi}_k)^2 + (\widetilde{\psi}'_k)^2\big]\right|\right) \\
&= \frac{1}{4a}\mathbb{E}_{X,Y\sim\chi^2(2a)}\big(|X-Y|\big)
\end{aligned}$$

where $\mathcal{N}(\mu, \sigma^2)$ denotes the Gaussian distribution of mean μ and variance σ^2, and $\chi^2(k)$ denotes the chi-squared distribution with k degrees of freedom, and where all the identically distributed random variables are independent.

Now, the probability density function of $\chi^2(k)$ is : $f_k(t) = \mathbb{1}_{\{t>0\}}\frac{1}{2\Gamma(k/2)}\left(\frac{t}{2}\right)^{k/2-1} e^{-t/2}$.

So : $f_{2a}(t) = \mathbb{1}_{\{t>0\}}\frac{1}{2(a-1)!}\left(\frac{t}{2}\right)^{a-1} e^{-t/2}$, and hence :

$$\begin{aligned}
\|\Delta(a)\|_{U_{\mathcal{H}(n)}} &= \frac{1}{16a\big[(a-1)!\big]^2}\int_0^\infty\int_0^\infty |x-y|\left(\frac{x}{2}\right)^{a-1}\left(\frac{y}{2}\right)^{a-1} e^{-(x+y)/2}dxdy \\
&= \frac{1}{2^{2a}a\big[(a-1)!\big]^2}\int_0^\infty\int_{-u}^{u} |v|\left(u^2-v^2\right)^{a-1} e^{-u}dvdu \\
&= \frac{1}{\big[2^a a!\big]^2}\int_0^\infty u^{2a}e^{-u}du \\
&= \frac{(2a)!}{\big[2^a a!\big]^2}
\end{aligned}$$

where we made the change of variables $u = \frac{x+y}{2}$, $v = \frac{x-y}{2}$ between the first and the second line.

In particular : $\|\Delta(\lfloor n/2 \rfloor)\|_{U_{\mathcal{H}(n)}} = \frac{(2\lfloor n/2 \rfloor)!}{\big[2^{\lfloor n/2 \rfloor}(\lfloor n/2 \rfloor)!\big]^2} \underset{n\to\infty}{\sim} \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}}$ (by Stirling's formula, or even more simply by using known results on Wallis' integrals).

Since $\frac{2}{\pi} < 1$, this implies that : $\exists\ \dfrac{2}{\pi} < \delta < 1,\ \exists\ \widetilde{n} \geq 2 :\ \forall\ n \geq \widetilde{n},\ \|\Delta(\lfloor n/2 \rfloor)\|_{U_{\mathcal{H}(n)}} \leq \sqrt{\delta}\dfrac{1}{\sqrt{n}}$.

Yet, the sequence $\left(W(n) := \dfrac{(2\lfloor n/2 \rfloor)!}{\left[2^{\lfloor n/2 \rfloor}(\lfloor n/2 \rfloor)!\right]^2} \right)_{n \geq 2}$, is such that : $W(n) = \dfrac{n+2}{n+1} W(n+2)$.

Hence, if $W(n+2) \leq \sqrt{\delta}\dfrac{1}{\sqrt{n+2}}$, then $W(n) \leq \sqrt{\delta}\dfrac{1}{\sqrt{n}}\dfrac{\sqrt{n+2}\sqrt{n}}{n+1} \leq \sqrt{\delta}\dfrac{1}{\sqrt{n}}$.

So by induction, we actually have : $\forall\ n \geq 2,\ \|\Delta(\lfloor n/2 \rfloor)\|_{U_{\mathcal{H}(n)}} \leq \sqrt{\delta}\dfrac{1}{\sqrt{n}}$.

We may now turn back to our initial issue.

For all $1 \leq i \leq K$, we denote by $\{|k_i\rangle, 1 \leq k_i \leq N_i\}$ an orthonormal basis of $\mathcal{H}_i$, and by $U_{\mathcal{H}_i}$ the uniform POVM on $\mathcal{H}_i$.

We then define the Hermitian matrix Δ_i on $\mathcal{H}_i$ as : $\Delta_i := \dfrac{1}{2\lfloor N_i/2 \rfloor}\left(\sum_{k_i=1}^{\lfloor N_i/2 \rfloor} |k_i\rangle\langle k_i| - \sum_{k_i=\lfloor N_i/2 \rfloor+1}^{2\lfloor N_i/2 \rfloor} |k_i\rangle\langle k_i| \right)$.

By theorem 5.4, it is such that : $\mathrm{Tr}_{\mathcal{H}_i}(\Delta_i) = 0$, $\|\Delta_i\|_1 = 1$ and $\|\Delta_i\|_{U_{\mathcal{H}_i}} \leq \sqrt{\delta}\dfrac{1}{\sqrt{N_i}}$.

We now consider the Hermitian matrix $\Delta := \bigotimes_{i=1}^{K} \Delta_i$ on $\mathcal{H}$, which is such that :

$\mathrm{Tr}_{\mathcal{H}}(\Delta) = \prod_{i=1}^{K} \mathrm{Tr}_{\mathcal{H}_i}(\Delta_i) = 0$, $\|\Delta\|_1 = \prod_{i=1}^{K} \|\Delta_i\|_1 = 1$ and $\|\Delta\|_{U_{\mathcal{H}}} = \prod_{i=1}^{K} \|\Delta_i\|_{U_{\mathcal{H}_i}} \leq \prod_{i=1}^{K} \sqrt{\delta}\dfrac{1}{\sqrt{N_i}} = \dfrac{1}{(1/\delta)^{K/2}\sqrt{N}}$
(exploiting the tensor product of both state and measurement).
Thus : $\lambda(U_{\mathcal{H}}) \leq \lambda_0(U_{\mathcal{H}}) \leq \dfrac{1}{(1/\delta)^{K/2}\sqrt{N}}$ with $\dfrac{1}{\delta} > 1$.

Remark 5.5 *Theorem 5.4 may also be of use to see that the lower bound in equation 12 really is "good" too, i.e. that its dependence on K is "real" : the constant relating $\|\cdot\|_{D_{(\mathcal{H},t)}}$, $t \geq 4$, to $\|\cdot\|_{2(K)}$ indeed has to decrease as a power of K. For this it is enough to analyse a specific tensor product of K local 4-design POVMs, and we choose $U_{\mathcal{H}} := U_{\mathcal{H}_1} \otimes \cdots \otimes U_{\mathcal{H}_K}$, the tensor product of the K uniform POVMs on sub-systems $\mathcal{H}_i$, $1 \leq i \leq K$. This is an interesting measurement since each of the $U_{\mathcal{H}_i}$ is an ∞-design POVM on $\mathcal{H}_i$, so in particular a 4-design POVM, and the complete symmetry is exploited in theorem 5.4 to make calculations feasible.*
Whereas equation 12 gives us $\dfrac{1}{18^{K/2}}\|\Delta\|_2 \leq \dfrac{1}{18^{K/2}}\|\Delta\|_{2(K)} \leq \|\Delta\|_{U_{\mathcal{H}}}$, the following also holds :
There exists a Hermitian matrix $\Delta \neq \mathbb{0}_{\mathcal{H}}$ on $\mathcal{H}$ such that $\|\Delta\|_{U_{\mathcal{H}}} = \dfrac{1}{2^{K/2}}\|\Delta\|_{2(K)} = \dfrac{1}{2^{K/2}}\|\Delta\|_2$.
In fact, define this time for all $1 \leq i \leq K$ the Hermitian Δ_i on $\mathcal{H}_i$ as $\Delta_i := \dfrac{1}{2}|\phi_i\rangle\langle\phi_i| - \dfrac{1}{2}|\varphi_i\rangle\langle\varphi_i|$, where $|\phi_i\rangle$ and $|\varphi_i\rangle$ are two orthogonal unit vectors of $\mathcal{H}_i$. Clearly $\|\Delta_i\|_{2(1)} = \|\Delta_i\|_2 = \dfrac{1}{\sqrt{2}}$, while theorem 5.4 applied to $a = 1$ yields $\|\Delta_i\|_{U_{\mathcal{H}_i}} = \dfrac{2!}{(2!)^2} = \dfrac{1}{2}$.
Now, define the Hermitian Δ on $\mathcal{H}$ as $\Delta := \bigotimes_{i=1}^{K} \Delta_i$. It is such that $\|\Delta\|_{2(K)} = \|\Delta\|_2 = \dfrac{1}{2^{K/2}}$ and $\|\Delta\|_{U_{\mathcal{H}}} = \dfrac{1}{2^K}$. So we actually have $\|\Delta\|_{U_{\mathcal{H}}} = \dfrac{1}{2^{K/2}}\|\Delta\|_{2(K)} = \dfrac{1}{2^{K/2}}\|\Delta\|_2$, and we are done.

5.5 Lower bound on $\mu_0(U_{\mathcal{H}})$

To begin with, let us point out a few very general facts.
For any POVM M on $\mathcal{H}$, $\mu(M) = 1$. Indeed, denoting by $\mathcal{M}$ its associated CPTP map, we have : $\Delta \geq \mathbb{0}_{\mathcal{H}} \ \Rightarrow\ \|\Delta\|_M = \|\mathcal{M}(\Delta)\|_1 = \|\Delta\|_1$.

Nevertheless, we might have $\mu_0(M) < 1$ since the inequality $\|\mathcal{M}(\Delta)\|_1 \leq \|\Delta\|_1$ is typically strict for a traceless matrix Δ (that has both positive and negative eigenvalues).
What is more, by the triangle inequality, $\mu_0(M)$ is attained on an extremal point of the convex set of traceless and trace norm 1 Hermitian matrices on $\mathcal{H}$, which means on a matrix Δ of the form $\Delta = \frac{1}{2}|\phi\rangle\langle\phi| - \frac{1}{2}|\varphi\rangle\langle\varphi|$ where $|\phi\rangle$ and $|\varphi\rangle$ are orthogonal unit vectors of $\mathcal{H}$.

Regarding the particular case of $U_{\mathcal{H}}$, the tensor product of the uniform POVMs on the $\mathcal{H}_i$, $1 \leq i \leq K$, we have the following result :

Theorem 5.6 $\mu_0(U_{\mathcal{H}}) \geq \dfrac{1}{2}$

Proof : Let $\widetilde{U}_{\mathcal{H}}$ be the uniform POVM on $\mathcal{H}$. As just stated, $\mu_0(\widetilde{U}_{\mathcal{H}})$ is attained on a matrix of the form $\Delta = \frac{1}{2}|\phi\rangle\langle\phi| - \frac{1}{2}|\varphi\rangle\langle\varphi|$ with $|\phi\rangle$ and $|\varphi\rangle$ orthogonal unit vectors of $\mathcal{H}$. Yet, by theorem 5.4 applied to $n = N$ and $a = 1$, we have that all the matrices Δ of this form actually yield the same $\|\Delta\|_{\widetilde{U}_{\mathcal{H}}}$, namely $\frac{2!}{(2!)^2} = \frac{1}{2}$.
Now, $\widetilde{U}_{\mathcal{H}}$ being "more symmetric" than $U_{\mathcal{H}}$, we have : $\mu_0(U_{\mathcal{H}}) \geq \mu_0(\widetilde{U}_{\mathcal{H}})$, and we are done.

6 Bounds on the distinguishability norm associated with sets of locally restricted measurements on a multi-partite quantum system

Let as before $\mathcal{H}_i \equiv \mathbb{C}^{N_i}$, $1 \leq i \leq K$, be K finite dimensional Hilbert spaces, and $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_K \equiv \mathbb{C}^N$, $N = N_1 \times \cdots \times N_K$, be their tensor product Hilbert space.
We shall now move on to investigating the properties of the measurement norms associated with not one but a whole class of locally restricted measurements on $\mathcal{H}$.

6.1 Lower bound on λ(SEP)

In the bi-partite case $K = 2$ very precise results exist regarding the characterization of the set of bi-separable positive operators on $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Those are sumed up, for instance, in [18].
An especially interesting one is the following (see [19] for comments and detailed proof) : A positive Hermitian $M \in \mathcal{M}_{N_1 \times N_2}(\mathbb{C})$ is separable (i.e. can be written as a tensor product of two positive Hermitians $M_1 \in \mathcal{M}_{N_1}(\mathbb{C})$ and $M_2 \in \mathcal{M}_{N_2}(\mathbb{C})$) if and only if for all $p \in \mathbb{N}$ and all positive map $\Lambda_1 \in \mathcal{L}(\mathcal{M}_{N_1}(\mathbb{C}), \mathcal{M}_p(\mathbb{C}))$ the Hermitian $(\Lambda_1 \otimes \mathrm{Id}_2)(M) \in \mathcal{M}_{p \times N_2}(\mathbb{C})$ is positive.

Remark 6.1 *Let us note that the transposition on the first subsystem $T_1 \in \mathcal{L}(\mathcal{M}_{N_1}(\mathbb{C}), \mathcal{M}_{N_1}(\mathbb{C}))$ is just one example of positive map in the special case $p = N_1$. So the positivity under partial transposition criterion "$M \geq \mathbb{O}_{N_1 \times N_2} \Rightarrow (T_1 \otimes Id_2)(M) \geq \mathbb{O}_{N_1 \times N_2}$" is nothing more than one necessary condition for separability amongst other. It is however known to be one of the "strongest", being also sufficient for $\mathcal{H} \equiv \mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathcal{H} \equiv \mathbb{C}^3 \otimes \mathbb{C}^2$ (again see [18] and [19] for a more advanced discussion).*

Theorem 6.2 below is actually very profound : it states, which is *a priori* not intuitive, that on a bi-partite Hilbert space, the unit ball for the Hilbert-Schmidt norm centred on the identity operator contains only separable operators.

Theorem 6.2 *Let δ be an Hermitian matrix on $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$.*
If $\|\delta\|_2 \leq 1$, then $\mathbb{1}_{\mathcal{H}} + \delta$ and $\mathbb{1}_{\mathcal{H}} - \delta$ are both separable Hermitian matrices on $\mathcal{H}$.

Proof : To begin with, let us point out that if $\|\delta\|_2 \leq 1$ then automatically $\|\delta\|_\infty \leq \|\delta\|_2 \leq 1$, so we already actually have that $\mathbb{1}_{N_1 \times N_2} + \delta$ and $\mathbb{1}_{N_1 \times N_2} - \delta$ are both positive.
The remainder of the demonstration relies heavily on the above mentioned characterization of bi-separable positive operators *via* positive maps. We only outline here its main ideas, referring the

reader to [21] for more details and accuracy.
One first basic observation we can make is that by linearity we can focus w.l.o.g. on positive maps $\Lambda_1 \in \mathcal{L}(\mathcal{M}_{N_1}(\mathbb{C}), \mathcal{M}_p(\mathbb{C}))$ that are s.t. $\Lambda_1(\mathbb{1}_{N_1}) = \mathbb{1}_p$.
Yet, such positive map Λ_1 necessarily satisfies $\||\Lambda_1|\|_\infty \leq 1$. Indeed, for all $X \in \mathcal{M}_{N_1}(\mathbb{C})$, $\|X\|_\infty \leq 1$ is equivalent to $\begin{cases} \mathbb{1}_{N_1} - X \geq \mathbb{0}_{N_1} \\ \mathbb{1}_{N_1} + X \geq \mathbb{0}_{N_1} \end{cases}$, which implies by positivity of Λ_1 that $\begin{cases} \Lambda_1(\mathbb{1}_{N_1} - X) \geq \mathbb{0}_p \\ \Lambda_1(\mathbb{1}_{N_1} + X) \geq \mathbb{0}_p \end{cases}$, i.e. by hypothesis on Λ_1 $\begin{cases} \mathbb{1}_p - \Lambda_1(X) \geq \mathbb{0}_p \\ \mathbb{1}_p + \Lambda_1(X) \geq \mathbb{0}_p \end{cases}$, which in turn is equivalent to $\|\Lambda_1(X)\|_\infty \leq 1$, and we are done.
Now, let δ an Hermitian on $\mathcal{H}$ satisfying $\|\delta\|_2 \leq 1$. Identifying $\mathcal{M}_{N_1 \times N_2}(\mathbb{C})$ to $\mathcal{M}_{N_2}(\mathcal{M}_{N_1}(\mathbb{C}))$, we may write it : $\delta = \big(\delta_{i,j}\big)_{1 \leq i,j \leq N_2}$ with $\delta_{i,j} = \big(\delta_{i,j}^{k,l}\big)_{1 \leq k,l \leq N_1}$ for all $1 \leq i,j \leq N_2$. Hence :

$$\begin{aligned} \|(\Lambda_1 \otimes \mathrm{Id}_2)(\delta)\|_\infty &= \big\|\big(\Lambda_1(\delta_{i,j}))_{1 \leq i,j \leq N_2)}\big\|_\infty \leq \big\|\big(\|\Lambda_1(\delta_{i,j})\|_\infty\big)_{1 \leq i,j \leq N_2}\big\|_\infty \leq \big\|\big(\|\Lambda_1(\delta_{i,j})\|_\infty\big)_{1 \leq i,j \leq N_2}\big\|_2 \\ &= \left(\sum_{1 \leq i,j \leq N_2} \|\Lambda_1(\delta_{i,j})\|_\infty^2\right)^{1/2} \leq \left(\sum_{1 \leq i,j \leq N_2} \|\delta_{i,j}\|_\infty^2\right)^{1/2} \leq \left(\sum_{1 \leq i,j \leq N_2} \|\delta_{i,j}\|_2^2\right)^{1/2} \\ &= \big\|\big(\|\delta_{i,j}\|_2\big)_{1 \leq i,j \leq N_2}\big\|_2 = \|\delta\|_2 \leq 1 \end{aligned}$$

So in the end $\begin{cases} (\Lambda_1 \otimes \mathrm{Id}_2)(\delta) \leq \mathbb{1}_{p \times N_2} = (\Lambda_1 \otimes \mathrm{Id}_2)(\mathbb{1}_{N_1 \times N_2}) \\ (\Lambda_1 \otimes \mathrm{Id}_2)(\delta) \geq -\mathbb{1}_{p \times N_2} = (\Lambda_1 \otimes \mathrm{Id}_2)(-\mathbb{1}_{N_1 \times N_2}) \end{cases}$ i.e. $\begin{cases} (\Lambda_1 \otimes \mathrm{Id}_2)(\mathbb{1}_{N_1 \times N_2} - \delta) \geq \mathbb{0}_{p \times N_2} \\ (\Lambda_1 \otimes \mathrm{Id}_2)(\mathbb{1}_{N_1 \times N_2} + \delta) \geq \mathbb{0}_{p \times N_2} \end{cases}$,
which implies as advertized that $\mathbb{1}_{N_1 \times N_2} - \delta$ and $\mathbb{1}_{N_1 \times N_2} + \delta$ are both separable.

Theorem 6.3 below follows from theorem 6.2 above by recursivity, and states that on K-partite Hilbert space, the ball of radius $\frac{2}{2^{K/2}}$ for the Hilbert-Schmidt norm centred on the identity operator contains only separable operators (see [22] for the subtleties of the proof, due mainly to the fact that we are dealing with complex rather than real vector spaces).

Theorem 6.3 *Let δ be an Hermitian matrix on $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_K$.*
If $\|\delta\|_2 \leq \dfrac{2}{2^{K/2}}$, then $\mathbb{1}_{\mathcal{H}} + \delta$ and $\mathbb{1}_{\mathcal{H}} - \delta$ are both separable Hermitian matrices on $\mathcal{H}$.

As a consequence, any 2-outcome POVM $\left(\dfrac{\mathbb{1}_{\mathcal{H}} + A}{2}, \dfrac{\mathbb{1}_{\mathcal{H}} - A}{2}\right)$ with $\|A\|_2 \leq \dfrac{2}{2^{K/2}}$ belongs to **SEP**.
Thus, for all traceless Hermitian matrix Δ on $\mathcal{H}$:

$$\|\Delta\|_{\mathbf{SEP}} = \max_{\left(\frac{\mathbb{1}_{\mathcal{H}}+A}{2}, \frac{\mathbb{1}_{\mathcal{H}}-A}{2}\right) \in \mathbf{SEP}} \big|\mathrm{Tr}(A\Delta)\big| \geq \max_{\|A\|_2 \leq \frac{2}{2^{K/2}}} \big|\mathrm{Tr}(A\Delta)\big| = \frac{2}{2^{K/2}}\|\Delta\|_2 \geq \frac{2}{2^{K/2}\sqrt{N}}\|\Delta\|_1 \quad (14)$$

with the next to last equality due to the self-duality of $\|\cdot\|_2$ and the last inequality due to the Cauchy-Schwarz inequality (*cf* appendix A.1).

And hence : $\lambda_0(\mathbf{SEP}) \geq \dfrac{2}{2^{K/2}\sqrt{N}}$.

Remark 6.4 *For a non necessarily traceless Hermitian matrix Δ, we have :*

$$\|\Delta\|_{\mathbf{SEP}} = \max_{(M, \mathbb{1}_{\mathcal{H}} - M) \in \mathbf{SEP}} \left(\max_{A \in [\mathbb{1}_{\mathcal{H}} - 2M; 2M - \mathbb{1}_{\mathcal{H}}]} \big|\mathit{Tr}(A\Delta)\big| \right) \geq \max_{\|A\|_2 \leq \frac{2}{2^{K/2}}} \big|\mathit{Tr}(A\Delta)\big|$$

So equation 14 still holds, and we actually have : $\lambda(\mathbf{SEP}) \geq \dfrac{2}{2^{K/2}\sqrt{N}}$.

6.2 Lower bound on $\lambda(\mathbf{PPT})$

Let us start by making the following simple but useful statement.

Theorem 6.5 *Let A be an Hermitian matrix on $\mathcal{H}$. Define $R(A)$ as $R(A) := \dfrac{Tr(A)}{\sqrt{Tr(A^2)}}$.*
If $R(A) \geq \sqrt{N-1}$, then A is positive.

Proof : A being Hermitian, we have : $\mathrm{Tr}(A) = \sum_{k=1}^{N} a_k$ and $\mathrm{Tr}(A^2) = \sum_{k=1}^{N} a_k^2$, where $a_1 \leq \cdots \leq a_N$ are the ordered (repeated) eigenvalues of A.
Yet, if A is not positive, which is equivalent to $a_1 < 0$, then :
$\sum_{k=1}^{N} a_k < \sum_{k=2}^{N} a_k \leq (N-1)^{1/2} \left(\sum_{k=2}^{N} a_k^2 \right)^{1/2} < (N-1)^{1/2} \left(\sum_{k=1}^{N} a_k^2 \right)^{1/2}$, and so : $R(A) < \sqrt{N-1}$.

Now, for all Hermitian matrix A on $\mathcal{H}$ and all partial transposition Γ on $\mathcal{H}$, $\mathrm{Tr}(A^\Gamma) = \mathrm{Tr}(A)$.
Hence, if A is an Hermitian matrix on $\mathcal{H}$ such that $R(A) \geq \sqrt{N-1}$, then $R(A^\Gamma) = R(A) \geq \sqrt{N-1}$ for all partial transposition Γ on $\mathcal{H}$, which implies that $A^\Gamma \geq \mathbb{0}_{\mathcal{H}}$ for all partial transposition Γ on $\mathcal{H}$, i.e. that A is a PPT matrix on $\mathcal{H}$.

We thus see that any 2-outcome POVM $\left(\dfrac{\mathbb{1}_{\mathcal{H}} + A}{2}, \dfrac{\mathbb{1}_{\mathcal{H}} - A}{2} \right)$ that is such that $R(\mathbb{1}_{\mathcal{H}} + A) \geq \sqrt{N-1}$ and $R(\mathbb{1}_{\mathcal{H}} - A) \geq \sqrt{N-1}$ automatically belongs to $\mathbf{PPT}$.
Yet, this criterion can be written as : $\dfrac{N \mp \mathrm{Tr}A}{\sqrt{N \mp 2\mathrm{Tr}A + \mathrm{Tr}A^2}} \geq \sqrt{N-1}$.
Which is equivalent to : $(N-1)\mathrm{Tr}A^2 \leq N + |\mathrm{Tr}A|(|\mathrm{Tr}A| - 2)$.
Which in turn is satisfied if : $\mathrm{Tr}A^2 \leq 1$ (since we always have $|\mathrm{Tr}A|(|\mathrm{Tr}A| - 2) \geq -1$).
So in the end : $\|A\|_2 \leq 1 \;\Rightarrow\; \left(\dfrac{\mathbb{1}_{\mathcal{H}} + A}{2}, \dfrac{\mathbb{1}_{\mathcal{H}} - A}{2} \right) \in \mathbf{PPT}$.

Consequently, for all traceless Hermitian matrix Δ on $\mathcal{H}$:

$$\|\Delta\|_{\mathbf{PPT}} = \max_{\left(\frac{\mathbb{1}_{\mathcal{H}}+A}{2}, \frac{\mathbb{1}_{\mathcal{H}}-A}{2}\right) \in \mathbf{PPT}} \left|\mathrm{Tr}(A\Delta)\right| \geq \max_{\|A\|_2 \leq 1} \left|\mathrm{Tr}(A\Delta)\right| = \|\Delta\|_2 \geq \frac{1}{\sqrt{N}} \|\Delta\|_1 \tag{15}$$

with the next to last equality due to the self-duality of $\|\cdot\|_2$ and the last inequality due to the Cauchy-Schwarz inequality (*cf* appendix A.1).

And hence : $\lambda_0(\mathbf{PPT}) \geq \dfrac{1}{\sqrt{N}}$.

Remark 6.6 *It may be pointed out that the condition $(M, \mathbb{1}_{\mathcal{H}} - M)$ being a 2-outcome PPT POVM is actually equivalent to the condition $(M, \mathbb{1}_{\mathcal{H}} - M)$ being bi-separable for any bi-partition of $\{1, \ldots, K\}$. So equation 15 is in fact nothing more than equation 14 applied in the particular 2-partite case.*

Remark 6.7 *Once again, for a non necessarily traceless Hermitian matrix Δ, we have :*

$$\|\Delta\|_{\mathbf{PPT}} = \max_{(M, \mathbb{1}_{\mathcal{H}} - M) \in \mathbf{PPT}} \left(\max_{A \in [\mathbb{1}_{\mathcal{H}} - 2M; 2M - \mathbb{1}_{\mathcal{H}}]} \left| Tr(A\Delta) \right| \right) \geq \max_{\|A\|_2 \leq 1} \left| Tr(A\Delta) \right|$$

So equation 15 still holds, and we actually have : $\lambda(\mathbf{PPT}) \geq \dfrac{1}{\sqrt{N}}$.

6.3 Upper bound on $\lambda_0(\mathbf{PPT})$

We previously showed that the global dimension dependence of $\lambda_0(U_{\mathcal{H}})$ is as $\frac{1}{\sqrt{N}}$ and that its number of parties dependence is as $\frac{1}{\alpha^{K/2}}$, with $2 \leq \alpha \leq 18$. We would now like to show that the factor of $\frac{1}{\sqrt{N}}$ does not go away when we go to the class of all PTT (and as a consequence all LOCC) measurements.

6.3.1 First special case

We first consider the situation when all the Hilbert spaces $\mathcal{H}_i$, $1 \leq i \leq K$, have same dimension d, so that $\mathcal{H} \equiv (\mathbb{C}^d)^{\otimes K}$.
In such case, we already have the following lower bound for $\lambda_0(\mathbf{PPT})$: $\lambda_0(\mathbf{PPT}) \geq \dfrac{1}{d^{K/2}}$.
The following theorem shows that this bound is close to being tight.

Theorem 6.8 *There exists a traceless Hermitian matrix $\Delta \neq \mathbb{0}_{\mathcal{H}}$ on $\mathcal{H} \equiv (\mathbb{C}^d)^{\otimes K}$ such that :*

$$\|\Delta\|_{\mathbf{PPT}} \leq \frac{2}{d^{\lfloor K/2 \rfloor} - 1}\|\Delta\|_1 = \frac{2\sqrt{d}^{\kappa}}{d^{K/2} - \sqrt{d}^{\kappa}}\|\Delta\|_1 \leq \frac{3\sqrt{d}^{\kappa}}{d^{K/2}}\|\Delta\|_1$$

where $\kappa \equiv K$ [2] is the parity of K.

Proof : For all Hermitian matrix Δ on $\mathcal{H}$, we have by definition :

$$\|\Delta\|_{\mathbf{PPT}} = \max_{\left(\frac{\mathbb{1}_{\mathcal{H}}+A}{2}, \frac{\mathbb{1}_{\mathcal{H}}-A}{2}\right) \in \mathbf{PPT}} |\mathrm{Tr}(A\Delta)| = \max_{\forall I \subset \{1,\ldots,K\}, -\mathbb{1}_{\mathcal{H}} \leq A^{\Gamma_I} \leq \mathbb{1}_{\mathcal{H}}} |\mathrm{Tr}(A\Delta)|$$

Yet, if A is such that for all $I \subset \{1, \ldots, K\}$, $-\mathbb{1}_{\mathcal{H}} \leq A^{\Gamma_I} \leq \mathbb{1}_{\mathcal{H}}$, then we necessarily have :

$$\forall\ I \subset \{1, \ldots, K\},\ |\mathrm{Tr}(A\Delta)| = \left|\mathrm{Tr}\left(A^{\Gamma_I}\Delta^{\Gamma_I}\right)\right| \leq \left\|A^{\Gamma_I}\right\|_{\infty}\left\|\Delta^{\Gamma_I}\right\|_1 \leq \left\|\Delta^{\Gamma_I}\right\|_1$$

where the first inequality holds thanks to Hölder's inequality (*cf* appendix A.1).

Amongst operators on $\mathcal{H}$ for which we know how to evaluate the trace norm of any of their partial transpose are the permutation operators U_π, $\pi \in \mathfrak{S}_K$ (*cf* appendix B.2).
Indeed, for all $\pi \in \mathfrak{S}_K$: $U_\pi = \sum_{j_1,\ldots,j_K} |j_1, \ldots, j_K\rangle\langle j_{\pi(1)}, \ldots, j_{\pi(K)}|$ where $|j_1\rangle, \ldots, |j_K\rangle$ run through a basis of $\mathbb{C}^d$. So for all $1 \leq p \leq K$, we have :

$$U_\pi^{\Gamma_{\{1,\ldots,p\}}} = \sum_{j_1,\ldots,j_K} |j_{\pi(1)}, \ldots, j_{\pi(p)}, j_{p+1}, \ldots, j_K\rangle\langle j_1, \ldots, j_p, j_{\pi(p+1)}, \ldots, j_{\pi(K)}|$$

Hence : $\left\|U_\pi^{\Gamma_{\{1,\ldots,p\}}}\right\|_1 = d^{K-f(\{1,\ldots,p\},\pi)}$, with $f(\{1, \ldots, p\}, \pi) := \left|\{i \in \{1, \ldots, p\},\ \pi(i) \in \{p{+}1, \ldots, K\}\}\right|$.
More generally, for all $I \subset \{1, \ldots, K\}$, $I \neq \emptyset$: $\left\|U_\pi^{\Gamma_I}\right\|_1 = d^{K-f(I,\pi)}$ where $f(I, \pi) := \left|\{i \in I,\ \pi(i) \notin I\}\right|$.

Yet, let us denote by U the matrix of the permutation $\pi := (1, \lfloor K/2 \rfloor + 1) \ldots (\lfloor K/2 \rfloor, 2\lfloor K/2 \rfloor)$, that is the product of $\lfloor K/2 \rfloor$ disjoint transpositions (and that decomposes therefore into $\lceil K/2 \rceil$ disjoint cycles).
We now consider the two following density operators on $\mathcal{H}$:

$$\rho := \frac{1}{d^K + d^{\lceil K/2 \rceil}}(\mathbb{1}_{\mathcal{H}} + U) \quad \text{and} \quad \sigma := \frac{1}{d^K - d^{\lceil K/2 \rceil}}(\mathbb{1}_{\mathcal{H}} - U)$$

Indeed, $U^\dagger = U^{-1} = U$, so that ρ and σ are actually Hermitian, $-\mathbb{1}_{\mathcal{H}} \leq U \leq \mathbb{1}_{\mathcal{H}}$, so that ρ and σ are actually positive, and Tr $\mathbb{1}_{\mathcal{H}} = d^K$, Tr $U = d^{\lfloor K/2 \rfloor}$, so that ρ and σ actually have trace 1.
We then choose as traceless Hermitian matrix $\Delta \neq \mathbb{0}_{\mathcal{H}}$:

$$\Delta := \rho - \sigma = \frac{2}{d^{\lceil K/2 \rceil}(d^{\lfloor K/2 \rfloor} + 1)(d^{\lfloor K/2 \rfloor} - 1)}(d^{\lfloor K/2 \rfloor}U - \mathbb{1}_{\mathcal{H}})$$

Due to the fact that ρ and σ are additionally orthogonal (since $U^2 = \mathbb{1}_{\mathcal{H}}$), we have : $\|\Delta\|_1 = 2$.

Furthermore, $I := \{1, \ldots, \lfloor K/2 \rfloor\} \subset \{1, .., K\}$ is such that $f(I, \pi) = \lfloor K/2 \rfloor$, so $\left\|U^{\Gamma_I}\right\|_1 = d^{K - \lfloor K/2 \rfloor}$, and hence, after a straightforward calculation :

$$\left\|\Delta^{\Gamma_I}\right\|_1 \leq \frac{2}{d^{\lceil K/2 \rceil}(d^{\lfloor K/2 \rfloor} + 1)(d^{\lfloor K/2 \rfloor} - 1)} \left(d^{\lfloor K/2 \rfloor} \left\|U^{\Gamma_I}\right\|_1 + \left\|\mathbb{1}_{\mathcal{H}}^{\Gamma_I}\right\|_1 \right) \leq \frac{2}{d^{\lfloor K/2 \rfloor} - 1} \|\Delta\|_1$$

Thus : $\|\Delta\|_{\mathbf{PPT}} \leq \left\|\Delta^{\Gamma_I}\right\|_1 \leq \frac{2}{d^{\lfloor K/2 \rfloor} - 1} \|\Delta\|_1$, which is what we wanted to prove.

As a consequence of this result : $\lambda(\mathbf{PPT}) \leq \lambda_0(\mathbf{PPT}) \leq \frac{2}{d^{\lfloor K/2 \rfloor} - 1}$ on $(\mathbb{C}^d)^{\otimes K}$.

6.3.2 Second special case

Another situation we might consider is when the Hilbert spaces $\mathcal{H}_i$, $1 \leq i \leq K$, are such that there exists $I \subset \{1, \ldots, K\}$ with $\mathcal{K} := \bigotimes_{i \in I} \mathcal{H}_i$ and $\mathcal{L} := \bigotimes_{i \in \{1, \ldots, K\} \setminus I} \mathcal{H}_i$ that satisfy $\dim \mathcal{K} = \dim \mathcal{L} = \sqrt{N}$.
In such case, once again, the lower bound $\lambda_0(\mathbf{PPT}) \geq \frac{1}{\sqrt{N}}$ can be shown to be close to optimal.

Theorem 6.9 *There exists a traceless Hermitian matrix $\Delta \neq \mathbb{0}_{\mathcal{H}}$ on $\mathcal{H} \equiv \mathbb{C}^{\sqrt{N}} \otimes \mathbb{C}^{\sqrt{N}}$ such that :*

$$\|\Delta\|_{\mathbf{PPT}} \leq \frac{2}{\sqrt{N} + 1} \|\Delta\|_1$$

Proof : Let us denote by $\mathbb{F}_{\mathcal{H}}$ the swap operator between the Hilbert spaces $\mathcal{K}$ and $\mathcal{L}$, i.e. the matrix of the permutation $(12) \in \mathfrak{S}_2$ on $\mathbb{C}^{\sqrt{N}} \otimes \mathbb{C}^{\sqrt{N}}$ (*cf* appendix B.2).
We now consider the two density operators $\rho := \frac{1}{N + \sqrt{N}}(\mathbb{1}_{\mathcal{H}} + \mathbb{F}_{\mathcal{H}})$ and $\sigma := \frac{1}{N - \sqrt{N}}(\mathbb{1}_{\mathcal{H}} - \mathbb{F}_{\mathcal{H}})$, the normalised projectors onto the symmetric and antisymmetric subspaces of $\mathbb{C}^{\sqrt{N}} \otimes \mathbb{C}^{\sqrt{N}}$, respectively.
We then choose as traceless Hermitian matrix $\Delta \neq \mathbb{0}_{\mathcal{H}}$: $\Delta := \rho - \sigma = \frac{2}{\sqrt{N}(N-1)}(-\mathbb{1}_{\mathcal{H}} + \sqrt{N}\mathbb{F}_{\mathcal{H}})$.
ρ and σ being additionally orthogonal, $\|\Delta\|_1 = 2$.

Yet, if a POVM is PPT across all possible bipartitions of $\mathcal{H}$, it is in particular PPT across the bipartition $\mathcal{K} : \mathcal{L}$ of $\mathcal{H}$. As a consequence :

$$\|\Delta\|_{\mathbf{PPT}(\mathcal{H})} \leq \|\Delta\|_{\mathbf{PPT}(\mathcal{K}:\mathcal{L})} = \max_{\left(\frac{\mathbb{1}_{\mathcal{H}} + A}{2}, \frac{\mathbb{1}_{\mathcal{H}} - A}{2}\right) \in \mathbf{PPT}(\mathcal{K}:\mathcal{L})} |\mathrm{Tr}(A\Delta)| = \max_{\substack{-\mathbb{1}_{\mathcal{H}} \leq A \leq \mathbb{1}_{\mathcal{H}} \\ -\mathbb{1}_{\mathcal{H}} \leq A^{\Gamma_{\mathcal{K}}} \leq \mathbb{1}_{\mathcal{H}} \\ -\mathbb{1}_{\mathcal{H}} \leq A^{\Gamma_{\mathcal{L}}} \leq \mathbb{1}_{\mathcal{H}}}} |\mathrm{Tr}(A\Delta)|$$

Moreover, Δ is a so called *highly symmetric* or *Werner* matrix on $\mathbb{C}^{\sqrt{N}} \otimes \mathbb{C}^{\sqrt{N}}$, i.e. a matrix that commutes with all the matrices of the form $U \otimes U$ with $U \in \mathcal{U}(\sqrt{N})$ a unitary matrix on $\mathbb{C}^{\sqrt{N}}$. Thus, when looking for a matrix A such that $|\mathrm{Tr}(A\Delta)|$ is maximal, it will be sufficient to only consider matrices that have the same commutation properties as Δ. Those are known to be linear combinations of the permutation matrices U_π, $\pi \in \mathfrak{S}_2$, on $\mathbb{C}^{\sqrt{N}} \otimes \mathbb{C}^{\sqrt{N}}$, i.e. linear combinations of $\mathbb{1}_{\mathcal{H}}$ and $\mathbb{F}_{\mathcal{H}}$ (*cf* appendix C).

Now, for $A = \alpha\mathbb{1}_{\mathcal{H}} + \beta\mathbb{F}_{\mathcal{H}}$:
On the one hand : $-\mathbb{1}_{\mathcal{H}} \leq A \leq \mathbb{1}_{\mathcal{H}} \Leftrightarrow \begin{cases} |\alpha + \beta| \leq 1 \\ |\alpha - \beta| \leq 1 \end{cases}$ and $\begin{cases} -\mathbb{1}_{\mathcal{H}} \leq A^{\Gamma_{\mathcal{K}}} \leq \mathbb{1}_{\mathcal{H}} \\ -\mathbb{1}_{\mathcal{H}} \leq A^{\Gamma_{\mathcal{L}}} \leq \mathbb{1}_{\mathcal{H}} \end{cases} \Leftrightarrow |\alpha + \sqrt{N}\beta| \leq 1.$
So : $\left(\frac{\mathbb{1}_{\mathcal{H}} + A}{2}, \frac{\mathbb{1}_{\mathcal{H}} - A}{2}\right) \in \mathbf{PPT}(\mathcal{K} : \mathcal{L}) \Leftrightarrow \begin{cases} |\alpha| \leq 1 \\ |\beta| \leq \frac{2}{\sqrt{N}+1} \end{cases}$.

And on the other hand : $|\mathrm{Tr}(A\Delta)| = \frac{2}{\sqrt{N}(N-1)}\big|-(1+\alpha)N+\beta\sqrt{N}N-\beta\sqrt{N}+(1+\alpha)N\big| = 2|\beta|$.

So that in the end : $|\mathrm{Tr}(A\Delta)| \leq \frac{4}{\sqrt{N}+1}$.

Thus : $\|\Delta\|_{\mathbf{PPT}(\mathcal{K}:\mathcal{L})} = \frac{4}{\sqrt{N}+1} = \frac{2}{\sqrt{N}+1}\|\Delta\|_1$, which leads to the conclusion we wanted to draw.

As a consequence of this result : $\lambda(\mathbf{PPT}) \leq \lambda_0(\mathbf{PPT}) \leq \frac{2}{\sqrt{N}+1}$ on $\mathbb{C}^{\sqrt{N}} \otimes \mathbb{C}^{\sqrt{N}}$.

6.3.3 Link with Data-Hiding

In the two previously described situations, we exhibited density operators ρ and σ on a composite Hilbert space of global dimension N that were orthogonal, hence such that $\left\|\frac{1}{2}\rho - \frac{1}{2}\sigma\right\|_1 = 1$, but nevertheless verifying $\left\|\frac{1}{2}\rho - \frac{1}{2}\sigma\right\|_{\mathbf{PPT}} \sim \frac{1}{\sqrt{N}}$. Those are therefore said to be *data-hiding* in the sense of [24], [25] or [26] : they encode states between multiple parties that would be perfectly distinguishable by a suitable measurement, but as long as the parties are restricted to LOCC measurements (or even more generally PPT measurements), they have only a very slim chance of guessing which state they are given. Indeed, the probability of discriminating correctly ρ from σ with only LOCC measurements decreases as the inverse square root of the total dimension.

6.4 Value of $\mu_0(\mathbf{SEP})$ and $\mu_0(\mathbf{PPT})$

Theorem 6.10 $\mu_0(\mathbf{SEP}) = \mu_0(\mathbf{PPT}) = 1$

Proof : We already know that $\mu_0(\mathbf{SEP}) \leq \mu_0(\mathbf{PPT}) \leq 1$ so we just have to prove that there exists an Hermitian traceless matrix Δ on $\mathcal{H}$ such that $\|\Delta\|_{\mathbf{SEP}} = \|\Delta\|_{\mathbf{PPT}} = \|\Delta\|_1$.
Yet, denoting by $\{|k_i\rangle, 1 \leq k_i \leq N_i\}$ an orthonormal basis of $\mathcal{H}_i$ for all $1 \leq i \leq K$, and defining the unit vectors $|1\rangle := |1_1\rangle\otimes\cdots\otimes|1_K\rangle$ and $|2\rangle := |2_1\rangle\otimes\cdots\otimes|2_K\rangle$ on $\mathcal{H}$, the matrix $\Delta := \frac{1}{2}|1\rangle\langle 1| - \frac{1}{2}|2\rangle\langle 2|$ meets our requirements. Indeed, it is obvious that $\|\Delta\|_1 = 1$ and $\mathrm{Tr}\Delta = 0$. Furthermore, $A := |1\rangle\langle 1| - |2\rangle\langle 2|$ is such that $\frac{\mathbb{1}_{\mathcal{H}} + A}{2}$ and $\frac{\mathbb{1}_{\mathcal{H}} - A}{2}$ are both separable, hence even more so PPT, and $|\mathrm{Tr}(A\Delta)| = \frac{1}{2}+\frac{1}{2} = 1$.
So $\|\Delta\|_{\mathbf{SEP}} = \|\Delta\|_{\mathbf{PPT}} = 1$, and we are done.

7 Conclusion and open questions

7.1 Summary of the main results and directly related unsolved problems

Figure 2 shows a schematic summary of the new and previously known relations between the distinguishability norm of POVMs with various degrees of locality restrictions and some usual operator norms on a multi-partite quantum system.

On a single system, distinguishability norm and 2-norm were first directly related in [17], with an application in quantum algorithms. More specifically, it was shown that even approximate 4-design POVMs (in a sense specified is the above mentioned paper) are *derandomizing* (which, roughly speaking, means that they "behave as the uniform POVM"). The advantage of such approximate 4-design POVMs compared to exact ones is mainly from an implementation point of view : an explicit and efficient (i.e. with "few" POVM elements) construction is provided.
It was then first realised and formalised in [27] that on a single (N-dimensional) system, the distinguishability norm associated with a 4-design POVM $D(N,1,4)$ and the 2-norm are indeed dimension independently equivalent on traceless operators : $\frac{1}{3}\|\Delta\|_2 \leq \|\Delta\|_{D(N,1,4)} \leq \|\Delta\|_2$ if $\mathrm{Tr}\Delta = 0$.

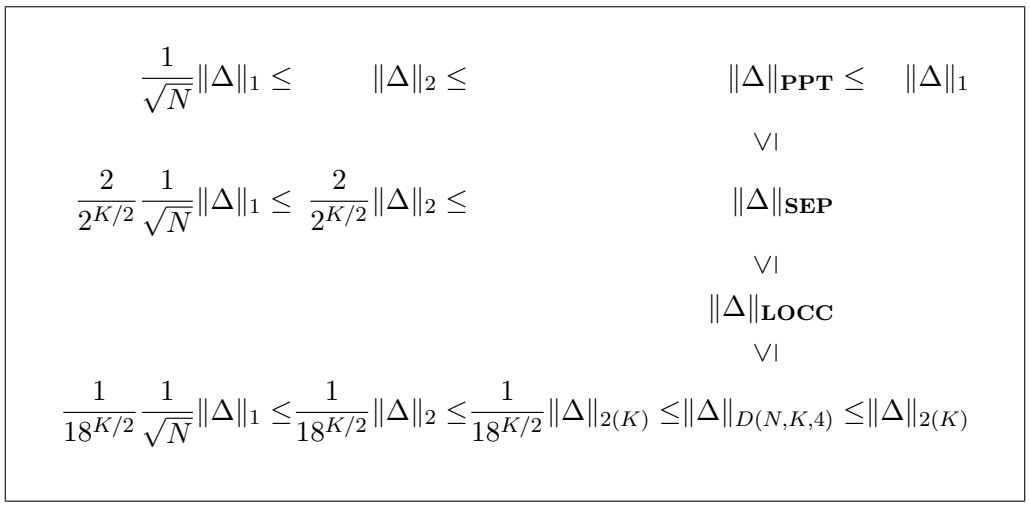


Figure 2: A summary of known relations linking several norms of any Hermitian Δ on a K-partite Hilbert space of global dimension N. $D(N, K, 4)$ denotes a generic tensor product of K local 4-design POVMs on the global N-dimensional Hilbert space.

The extension to two parties in [11], $\frac{1}{\sqrt{153}}\|\Delta\|_2 \leq \|\Delta\|_{D(N,2,4)}$ for $D(N, 2, 4)$ a tensor product of two 4-design POVMs (on a N-global dimensional system) and still assuming $\mathrm{Tr}\Delta = 0$, subsequently found applications in entanglement theory. In fact, this result was used in [30] to describe an algorithm that would decide in a quasipolynomial time whether a bi-partite state is separable or whether it is "far away" from the set of separable states.
We have now solved an open problem from [11], showing that, for any number K of parties, the distinguishability norm on Hermitian operators associated with a tensor product of local 4-design POVMs is actually equivalent to a certain K-partite relative of the Hilbert-Schmidt norm. The equivalence is in terms of constants of domination which depend only on the number of parties, not on the local dimensions.
The fact that the previously known results in the special cases of $K = 1$ and $K = 2$ parties found applications in very diverse fields of quantum information theory suggests that our latest extension to any number K of parties might be useful too.

It may be pointed out, though, that our constants appear worse compared to the known inequalities for $K = 1$ and $K = 2$ on traceless operators. In the former case, [17] gives $\frac{1}{3}$ whereas we get $\frac{1}{\sqrt{18}}$. In the latter, [11] gives $\frac{1}{\sqrt{153}}$ whereas we get $\frac{1}{18}$. While the gap is small, it might to some degree be explained by the fact that in both these cited papers the assumption $\mathrm{Tr}\Delta = 0$ was made, and exploited to simplify the fourth moment even more. One of the believes that motivated our investigation was that there was merit in transcending this restriction, as not in all applications it can be justified (recall that for two density operators ρ and σ, $\mathrm{Tr}(q\rho - (1-q)\sigma) \neq 0$ if $q \neq \frac{1}{2}$). In any case, it remains an open problem to find the optimal constants of domination with respect to the norm $\|\cdot\|_{2(K)}$.

Via the 2-norm we then obtained performance comparisons with the trace norm, revealing at most a factor of the order of the inverse square root of the dimension of the total Hilbert space between the distinguishability norm associated with a tensor product of local 4-design POVMs and the trace norm. Since such measurement is a particular LOCC strategy, we get lower bounds on the distinguishing power of LOCC measurements. The bounds can be shown to be optimal in their dimensional dependence, as two constructions of data-hiding states which attain these bounds (up to K-dependent factors) were exhibited. Here, one remaining question is whether for odd number K of parties, all of which have equal dimension, the additional factor of square root of the local dimension in theorem 6.8 can be removed. On a related note, regarding theorem 6.9, does there exist a universal constant $C > 0$ such that for all sufficiently large global dimension N one can find a Hermitian $\Delta \neq \mathbb{0}_{\mathcal{H}}$ with $\|\Delta\|_{\mathbf{PPT}} \leq \frac{C}{\sqrt{N}}\|\Delta\|_1$, irrespective of the local dimensions?

Even more interesting would be to quantify the performance of LOCC, or at least SEP, measurements. Indeed, notice that we have only exploited bi-separability in theorems 6.8 and 6.9, and we see that there remains only a factor of at most 2 to be gained as long as one is restricted to this weaker constraint. Is it possible to significantly improve this factor when judging the performance of SEP or LOCC measurements? In particular, do there exist constants $C > 0$ and $\alpha > 1$ such that for all number of parties K and all sufficiently large total dimensions N there is a Hermitian $\Delta \neq \mathbb{0}_{\mathcal{H}}$ with $\|\Delta\|_{\mathbf{LOCC}} \leq \frac{C}{\alpha^{K/2}\sqrt{N}}\|\Delta\|_1$, or even $\|\Delta\|_{\mathbf{SEP}} \leq \frac{C}{\alpha^{K/2}\sqrt{N}}\|\Delta\|_1$?

7.2 Distinguishing power of a tensor product of 2-design POVMs

A generic tensor product of 2-design POVMs has a distinguishing power that is, asymptotically in the local dimensions, much worse than the one of a generic tensor product of 4-design POVMs. It is indeed quite easy to find examples of tensor products of 2-design POVMs for which there exist state pairs whose distinguishability under the considered tensor product of 2-design POVMs behaves as $\frac{1}{N}$ rather than as $\frac{1}{\sqrt{N}}$ (which would be the order of magnitude of the worst distinguishability one could expect under a tensor product of 4-design POVMs).

Consider for instance on each $\mathcal{H}_i$, $1 \leq i \leq K$, a complete set of pairwise MUB (assuming that all the local dimensions N_i, $1 \leq i \leq K$, are such that there actually exists a complete set of pairwise MUB on $\mathcal{H}_i$) : $\Big\{\big\{|\phi(i)_k^j\rangle,\ 1 \leq j \leq N_i\big\},\ 1 \leq k \leq N_i + 1\Big\}$.
Now, define on each $\mathcal{H}_i$, $1 \leq i \leq K$, the 2-design POVM $M^{(i)} = \left(M(i)_k^j := \frac{1}{N_i+1}|\phi(i)_k^j\rangle\langle\phi(i)_k^j|\right)_{\substack{1\leq k\leq N_i+1\\ 1\leq j\leq N_i}}$.
And finally, take $M := M^{(1)} \otimes \cdots \otimes M^{(K)}$ as specific tensor product of 2-design POVMs on $\mathcal{H}$.
The state pair (ρ, σ) we will now consider for our purpose is the following : $\rho := \bigotimes_{i=1}^{K} \rho_i$ and $\sigma := \bigotimes_{i=1}^{K} \sigma_i$
where, for all $1 \leq i \leq K$, $\rho_i := |\phi(i)_1^1\rangle\langle\phi(i)_1^1|$ and $\sigma_i := |\phi(i)_1^2\rangle\langle\phi(i)_1^2|$.
Yet, for all $1 \leq i \leq K$, defining Δ_i as $\Delta_i := \rho_i - \sigma_i$ we have :

$$\|\Delta_i\|_1 = 2$$

$$\|\Delta_i\|_{M(i)} = \sum_{\substack{1\leq k\leq N_i+1\\ 1\leq j\leq N_i}} \big|\mathrm{Tr}\big(\Delta_i M(i)_k^j\big)\big| = \frac{1}{N_i+1} \sum_{\substack{1\leq k\leq N_i+1\\ 1\leq j\leq N_i}} \Big|\big|\langle\phi(i)_1^1|\phi(i)_k^j\rangle\big|^2 - \big|\langle\phi(i)_1^2|\phi(i)_k^j\rangle\big|^2\Big| = \frac{2}{d_i+1}$$

Indeed, $\big|\langle\phi(i)_1^l|\phi(i)_k^j\rangle\big|^2 = \begin{cases}\delta_{lj} \text{ if } k = 1\\ \frac{1}{N_i} \text{ if } k \neq 1\end{cases}$.
Hence, $\Delta := \rho - \sigma$ is such that $\|\Delta\|_1 = 2^K$ and $\|\Delta\|_M = \frac{2^K}{\prod_{i=1}^K (N_i+1)}$.
As a consequence : $\|\Delta\|_M = \frac{1}{\prod_{i=1}^K (N_i+1)}\|\Delta\|_1 \leq \frac{1}{N}\|\Delta\|_1$

From these considerations, a legitimate wonder would be : can one find a lower bound on $\lambda(D(\mathcal{H}, t))$ when only assuming $t \geq 2$ and not $t \geq 4$? It would obviously not behave as $\frac{1}{\sqrt{N}}$, but perhaps' as $\frac{1}{N}$...
Actually, we can answer this question in the one-partite case.

Theorem 7.1 *Let M be a 2-design POVM on $\mathcal{H} \equiv \mathbb{C}^N$. For all Hermitian Δ on $\mathcal{H}$, $\|\Delta\|_M \geq \frac{1}{2}\frac{1}{N+1}\|\Delta\|_1$.*

Proof : Let us first consider the case when $M := \left(\frac{N}{m}P_k\right)_{1\leq k\leq m}$ is a proper 2-design POVM.
Any Hermitian Δ may be written as $\Delta = A - B$ where A and B are two positive Hermitians with orthogonal supports (*cf* appendix A.1). Then, defining $(a_k)_{1\leq k\leq m}$ and $(b_k)_{1\leq k\leq m}$ as $a_k := \frac{N}{m}\mathrm{Tr}(AP_k)$

and $b_k := \frac{N}{m}\mathrm{Tr}(BP_k)$, we have : $\|\Delta\|_M = \sum_{k=1}^m |a_k - b_k| \geq \sum_{k=1}^m \big(a_k + b_k - 2\sqrt{a_k b_k}\big)$.

Yet, for all $\alpha > 0$: $2\sum_{k=1}^m \sqrt{a_k b_k} \leq \alpha + \frac{1}{\alpha}\left(\sum_{k=1}^m \sqrt{a_k b_k}\right)^2 \leq \alpha + \frac{m}{\alpha}\sum_{k=1}^m a_k b_k$.

And what is more, using the fact that $\left(\frac{1}{m}P_k\right)_{1\leq k\leq m}$ is a spherical 2-design, we have : $\sum_{k=1}^m \frac{1}{m}P_k = \frac{1}{N}\mathbb{1}_{\mathcal{H}}$ and $\sum_{k=1}^m \frac{1}{m}P_k \otimes P_k = \frac{1}{N(N+1)}\big(\mathbb{1}_{\mathcal{H}\otimes\mathcal{H}} + \mathbb{F}_{\mathcal{H}\otimes\mathcal{H}}\big)$. As a consequence :

$$\sum_{k=1}^m a_k = \sum_{k=1}^m \frac{N}{m}\mathrm{Tr}(AP_k) = N\mathrm{Tr}\left(A\sum_{k=1}^m \frac{1}{m}P_k\right) = \mathrm{Tr}(A) \quad \text{and likewise} \quad \sum_{k=1}^m b_k = \mathrm{Tr}(B)$$

$$\sum_{k=1}^m a_k b_k = \sum_{k=1}^m \frac{N^2}{m^2}\mathrm{Tr}(AP_k)\mathrm{Tr}(BP_k) = \frac{N^2}{m}\mathrm{Tr}\left(A\otimes B\sum_{k=1}^m \frac{1}{m}P_k\otimes P_k\right) = \frac{1}{m}\frac{N}{N+1}\big(\mathrm{Tr}(A)\mathrm{Tr}(B) + \mathrm{Tr}(AB)\big)$$

Now, by assumption on A and B, $\mathrm{Tr}(AB) = 0$. So putting all the above results together we eventually get : $\forall\ \alpha > 0,\ \|\Delta\|_M \geq \mathrm{Tr}(A) + \mathrm{Tr}(B) - \alpha - \frac{1}{\alpha}\frac{N}{N+1}\mathrm{Tr}(A)\mathrm{Tr}(B)$.

Hence, choosing $\alpha = \frac{1}{2}\big(\mathrm{Tr}(A) + \mathrm{Tr}(B)\big)$, and just using that $2\mathrm{Tr}(A)\mathrm{Tr}(B) \leq \frac{1}{2}\big(\mathrm{Tr}(A) + \mathrm{Tr}(B)\big)^2$, we have : $\|\Delta\|_M \geq \frac{1}{2}\left(1 - \frac{N}{N+1}\right)\big(\mathrm{Tr}(A) + \mathrm{Tr}(B)\big) = \frac{1}{2}\frac{1}{N+1}\big(\mathrm{Tr}(A) + \mathrm{Tr}(B)\big)$.

And since by definition of A and B, $\mathrm{Tr}(A) + \mathrm{Tr}(B) = \mathrm{Tr}|\Delta| = \|\Delta\|_1$, we come in the end to what we wanted to prove : $\|\Delta\|_M \geq \frac{1}{2}\frac{1}{N+1}\|\Delta\|_1$.

More generally, if $M = (Np_kP_k)_{1\leq k\leq m}$ is a weighted 2-design POVM, it may be approximated, better and better as $n \to +\infty$, by the proper 2-design POVM with more outcomes $\widetilde{M} = \left(\frac{N}{\sum_{q=1}^m \lfloor p_q n\rfloor}\widetilde{P}_{k,l_k}\right)_{\substack{1\leq k\leq m \\ 1\leq l_k\leq \lfloor p_k n\rfloor}}$,

where for each $1 \leq k \leq m$ all the $\widetilde{P}_{k,l_k}$, $1 \leq l_k \leq \lfloor p_k n\rfloor$, have same value P_k.

We thus see that in the one-partite case $\mathcal{H} \equiv \mathbb{C}^N$, $\lambda(D(\mathcal{H},2)) \geq \frac{1}{2}\frac{1}{N+1} \geq \frac{1}{4}\frac{1}{N}$. Unfortunately we are for now unable to provide an analogous result in the multi-partite case $\mathcal{H} \equiv \mathbb{C}^{N_1}\otimes\cdots\otimes\mathbb{C}^{N_K}$ with $K > 1$.

7.3 POVMs with "few" outcomes whose distinguishability norm is equivalent to $\|\cdot\|_{2(1)}$

We focus here on the one-partite case $\mathcal{H} \equiv \mathbb{C}^N$. What we know is that the distinguishability norm associated with any 4-design POVM M on $\mathcal{H}$ is essentially equivalent to the "one-partite modified 2-norm" on $\mathcal{H}$: $\frac{1}{\sqrt{18}}\|\cdot\|_{2(1)} \leq \|\cdot\|_M \leq \|\cdot\|_{2(1)}$. This is of course not true for any POVM on $\mathcal{H}$, even an informationally complete one. One could thus wonder what would be the "minimal" requirements on a POVM M on $\mathcal{H}$ that would guarantee that $\|\cdot\|_M = \Omega\big(\|\cdot\|_{2(1)}\big)$. In views of computations as well as experimental implementations, one important feature a POVM must hold to be useable is to have "few" outcomes. The previous question would hence more precisely become : what is the minimal number of outcomes a POVM M on $\mathcal{H}$ must have so that $\|\cdot\|_M = \Omega\big(\|\cdot\|_{2(1)}\big)$?

It seems it can actually be shown that certain randomly chosen POVMs with less than $O(N^3\log N)$ outcomes achieve this. Since a 4-design POVM must have at least $O(N^4)$ outcomes, those are not 4-design POVMs.

The idea is to start from a 4-design POVM and to construct the POVM elements of M by sampling rank-1 projectors independently from the probability distribution of the rank-1 projectors which make

the 4-design POVM. Yet, it turns out that, with high probability, drawing only $O(N^3 \log N)$ rank-1 projectors in this way (and then slightly modifying them so that they actually form a POVM in their whole with probability 1) will be sufficient for M to yield almost the same performance as the initial 4-design POVM. The proof requires bounds from large deviation theory, both "classic" results on real valued random variables (see for instance [8] and [9] for very general references on the matter) and their more "original" analogous on selfadjoint operator valued random variables (see [31] and [32] for a rigorous justification of the "natural" extension from the framework of the total ordering on real numbers to the one of the partial ordering on selfadjoint operators). It also makes essential use of a discretisation result ("net" argument).

Appendices

A Geometry of Hilbert spaces

The reader is referred to [14] or [7] (as two examples amongst many other) for a much more complete description of the results exposed in this section.

Let $(\mathcal{H}, \|\cdot\|)$ be a Hilbert space (with the norm $\|\cdot\|$ deriving from an inner product $\langle\cdot|\cdot\rangle$ on $\mathcal{H}$).

A.1 Linear operators on a Hilbert space

We denote by $\mathcal{F}(\mathcal{H})$ the set of linear operators on $\mathcal{H}$.

Definition/Proposition A.1 *For all $A \in \mathcal{F}(\mathcal{H})$, we denote by $A^\dagger$ its adjoint, defined as being the (existing and unique) element of $\mathcal{F}(\mathcal{H})$ such that : $\forall\ x, y \in \mathcal{H},\ \langle y|Ax\rangle = \langle A^\dagger y|x\rangle$.*
$A \in \mathcal{F}(\mathcal{H})$ is said to be Hermitian if $A^\dagger = A$.

Definition/Proposition A.2 *$A \in \mathcal{F}(\mathcal{H})$ is said to be positive if : $\forall\ x \in \mathcal{H},\ \langle x|Ax\rangle \geq 0$.*
This notion of positivity enables the definition of a partial ordering on $\mathcal{F}(\mathcal{H})$: for all $A, B \in \mathcal{F}(\mathcal{H})$, $A \leq B \ \Leftrightarrow\ B - A$ positive.
For all positive $A \in \mathcal{F}(\mathcal{H})$, there exists a unique positive $B \in \mathcal{F}(\mathcal{H})$ such that $B^2 = A$. We will denote such B by $A^{1/2}$ and call it the square root of A.
For all $A \in \mathcal{F}(\mathcal{H})$, $A^\dagger A$ is positive. We will denote by $|A|$ its square root and call it the absolute value of A.

Denoting by $\mathcal{T}(\mathcal{H})$ the class of linear operators on $\mathcal{H}$ which have finite trace, and by $\mathcal{B}(\mathcal{H})$ the class of linear operators on $\mathcal{H}$ which are bounded, we can then define the following subsets of $\mathcal{F}(\mathcal{H})$ (that all hold a Banach space structure for the associated norm) :

- For all $1 \leq p < \infty$, $\mathcal{S}_p(\mathcal{H}) := \{A \in \mathcal{F}(\mathcal{H}),\ |A|^p \in \mathcal{T}(\mathcal{H})\}$, equipped with the so-called *Schatten p-norm* $\|\cdot\|_p : A \in \mathcal{S}_p(\mathcal{H}) \mapsto \big(\mathrm{Tr}\big(|A|^p\big)\big)^{1/p}$.

- $\mathcal{S}_\infty(\mathcal{H}) := \mathcal{B}(\mathcal{H})$, the *Schatten ∞-norm* being the operator norm $\|\cdot\|_\infty := |||\cdot|||$.

$\mathcal{S}_2(\mathcal{H})$, equipped with the so-called *Hilbert-Schmidt inner product* $(A, B) \in \mathcal{S}_2(\mathcal{H}) \mapsto \mathrm{Tr}(B^\dagger A)$ (from which $\|\cdot\|_2$ derives) is a Hilbert space.

We furthermore have the following Hölder inequality for the Hilbert-Schmidt inner product :
$\forall\ 1 \leq p, q \leq \infty,\ \dfrac{1}{p} + \dfrac{1}{q} = 1\ \Rightarrow\ \forall\ (A, B) \in \mathcal{S}_p(\mathcal{H}) \times \mathcal{S}_q(\mathcal{H}),\ B^\dagger A \in \mathcal{S}_2(\mathcal{H})$ and $|\mathrm{Tr}(B^\dagger A)| \leq \|A\|_p \|B\|_q$
And the following duality theorem :
$\forall\ 1 \leq p \leq \infty,\ \forall\ A \in \mathcal{S}_p(\mathcal{H}),\ \|A\|_p = \sup\limits_{\substack{B \in \mathcal{S}_q(\mathcal{H}) \\ \|B\|_q \leq 1}} \big|\mathrm{Tr}(B^\dagger A)\big|$ where q is such that $\dfrac{1}{p} + \dfrac{1}{q} = 1$.

Remark A.3 *If $\mathcal{H} \equiv \mathbb{C}^N$ is of finite dimension N, then $\forall\ 1 \leq p \leq \infty,\ \mathcal{S}_p(\mathcal{H}) = \mathcal{F}(\mathcal{H})$.*
And we simply have for any $A \in \mathcal{F}(\mathcal{H})$: $\begin{cases} \forall\ 1 \leq p < \infty,\ \|A\|_p = \left(\sum\limits_{1 \leq i \leq N} \mu_i(A)^p\right)^{1/p} \\ \|A\|_\infty = \max\limits_{1 \leq i \leq N} \mu_i(A) \end{cases}$ *, with $\mu_1(A), \ldots, \mu_N(A)$ the eigenvalues of $|A|$ (which are indeed elements of $\mathbb{R}^+$).*

For an Hermitian A, with eigenvalues $\lambda_1(A), \ldots, \lambda_N(A)$, this reduces even more to :

$$\begin{cases} \forall\ 1 \leq p < \infty,\ \|A\|_p = \left(\sum\limits_{1 \leq i \leq N} |\lambda_i(A)|^p \right)^{1/p} \\ \|A\|_\infty = \max\limits_{1 \leq i \leq N} |\lambda_i(A)| \end{cases} .$$

A.2 Duality between norms and convex bodies

For any norm η on $\mathcal{H}$ and any $r > 0$ we will denote by $\mathcal{B}_r^\eta := \{x \in \mathcal{H},\ \eta(x) \leq r\}$ the closed ball of radius r for N.

Proposition A.4 *Let $K \subset \mathcal{H}$ be a closed convex (i.e. $x, y \in K \ \Rightarrow\ \forall\ 0 < \lambda < 1,\ \lambda x + (1-\lambda)y \in K$) balanced (i.e. $x \in K \ \Rightarrow\ -x \in K$) body of $\mathcal{H}$.*
Define $P_K : x \in \mathcal{H} \mapsto inf\ \{t > 0,\ x \in tK\} = inf\ \left\{t > 0,\ \frac{1}{t}x \in K\right\}$.
Then P_K is a norm on $\mathcal{H}$ that is such that $\mathcal{B}_1^{P_K} = K$.

Proof : The subadditivity of P_K is guaranteed by the convexity of K whereas its homogeneity is due to the fact that K is balanced.

Proposition A.5 *Conversely, for any norm η on $\mathcal{H}$ and any $r > 0$, $\mathcal{B}_r^\eta$ is a closed convex balanced body of $\mathcal{H}$ and $P_{\mathcal{B}_1^\eta} = \eta$.*

Definition/Proposition A.6 *For all set $K \subset \mathcal{H}$ we define its polar as $\widetilde{K} := \{x \in \mathcal{H},\ \forall\ y \in K,\ |\langle y|x\rangle| \leq 1\}$.*
If K is a closed convex balanced body, then so is $\widetilde{K}$, and $\widetilde{\widetilde{K}} = K$. In such case, $\widetilde{K}$ is the closed unit ball for P_K and K the one for $P_{\widetilde{K}}$, so that one has the important duality formulas :

$$\forall\ x \in \mathcal{H},\ P_K(x) = \sup_{y \in \widetilde{K}} |\langle y|x\rangle| \text{ and } P_{\widetilde{K}}(x) = \sup_{y \in K} |\langle y|x\rangle|$$

As an important example of such duality between norms and convex bodies in a Hilbert space, one has the following : In the Hilbert space $\mathcal{S}_2(\mathcal{H})$ (equipped with the Hilbert-Schmidt inner product), for all $1 \leq p, q \leq \infty$ such that $\frac{1}{p} + \frac{1}{q} = 1$, the closed unit balls for the Schatten p-norm $\mathcal{B}_1^{\|\cdot\|_p}$ and the Schatten q-norm $\mathcal{B}_1^{\|\cdot\|_q}$ are polar to each other.

B Linear representations of compact groups

For a general reference on the subject, see for instance [5], the account made in this section being far from exhaustive.

B.1 General definitions and properties

Definition B.1 *Let G be a group.*
A linear representation of G is given by a vector space $\mathcal{V}$ (the group's representation space) and a group morphism $\rho : G \to \mathcal{GL}(\mathcal{V})$ (the group's representation map).
$\dim \mathcal{V}$ is called the dimension of the representation $\big(\rho, \mathcal{V}\big)$.

Remark B.2 *Providing a linear representation $\big(\rho, \mathcal{V}\big)$ of a group G is equivalent to providing an action of the group G on the vector space $\mathcal{V}$. Such action is defined by : $a_\rho : (g, v) \in G \times \mathcal{V} \mapsto \rho(g)v \in \mathcal{V}$.*

Two specific (and of course non mutually exclusive) situations that will be of special interest are the following ones :

- If G is a topological group, it will be demanded of a linear representation $\big(\rho, \mathcal{V}\big)$ of G, first that $\mathcal{V}$ be a topological vector space, and second that the associated action a_ρ of G on $\mathcal{V}$ be continuous (for the considered topologies).

- If $\mathcal{V} := \mathcal{H}$ is a Hilbert space for an inner product $\langle\cdot|\cdot\rangle$, the representation $\big(\rho, [\mathcal{H}, \langle\cdot|\cdot\rangle]\big)$ is said to be unitary if : $\forall\ g \in G,\ \forall\ x, y \in \mathcal{H},\ \langle\rho(g)x|\rho(g)y\rangle = \langle x|y\rangle$ (i.e. if the inner product $\langle\cdot|\cdot\rangle$ is invariant under each of the maps $a_\rho(g,\cdot) : \mathcal{V} \to \mathcal{V}$, $g \in G : \forall\ g \in G,\ \forall\ x, y \in \mathcal{H},\ \langle a_\rho(g,x)|a_\rho(g,y)\rangle = \langle x|y\rangle$). This is actually equivalent to demanding that $\rho : G \to \mathcal{U}(\mathcal{H})$.

Theorem B.3 *Let G be a compact group and $\big(\rho, [\mathcal{H}, \langle\cdot|\cdot\rangle]\big)$ be a linear representation of G (where $\mathcal{H}$ is a Hilbert space for the inner product $\langle\cdot|\cdot\rangle$). Then there exists a unique inner product $\prec\cdot|\cdot\succ$ on $\mathcal{H}$ such that the linear representation $\big(\rho, [\mathcal{H}, \prec\cdot|\cdot\succ]\big)$ of G is unitary. What is more, $\prec\cdot|\cdot\succ$ provides $\mathcal{H}$ with the same topological structure as $\langle\cdot|\cdot\rangle$.*

Proof : G being compact, it may be equipped with a unique normalized left and right invariant Haar measure $d\mu_G$. The $\rho(G)$-invariant inner product $\prec\cdot|\cdot\succ$ may thus be defined from $\langle\cdot|\cdot\rangle$ by the following averaging procedure over G : $\forall\ x, y \in \mathcal{H},\ \prec x|y\succ := \displaystyle\int_G \langle\rho(g)x|\rho(g)y\rangle d\mu_G(g)$.

Remark B.4 *If G is a finite group, it clearly belongs to the above mentionned category since the discrete topology provides it with a compact group structure. In such case, the unique normalized left and right invariant Haar measure on G is the counting measure :* $\displaystyle\int_G f(g)d\mu_G(g) := \frac{1}{|G|}\sum_{g\in G} f(g)$.

Definition B.5 *Let G be a compact group and $\big(\rho, \mathcal{V}\big)$ be a linear representation of G.*
If $\mathcal{W} \subset \mathcal{V}$ is a closed subspace of $\mathcal{V}$ which is invariant under $\rho(G)$ (i.e. $\forall\ g \in G,\ \rho(g)(\mathcal{W}) \subset \mathcal{W}$), then it makes sense to talk about $\rho(G)_{|\mathcal{W}}$ the restriction of $\rho(G)$ to the subspace $\mathcal{W}$, and $\big(\rho_{|\mathcal{W}}, \mathcal{W}\big)$ is called a subrepresentation of $\big(\rho, \mathcal{V}\big)$.
If $\mathcal{V}$ has no proper subrepresentation space (i.e. exactly two subrepresentation spaces, namely $\{0\}$ and $\mathcal{V}$ itself) the representation $\big(\rho, \mathcal{V}\big)$ is said to be irreducible. It may otherwise be referred to as being decomposable.

Theorem B.6 *Any finite-dimensional linear representation of a compact group is completely reducible, i.e it may be written as a direct sum of irreducible representations.*

Proof : Let G be a compact group and $\big(\rho, [\mathcal{H}, \langle\cdot|\cdot\rangle]\big)$ be a finite-dimensional unitary representation of G. If it is irreducible, then we are done. Otherwise, there exists $\mathcal{K} \subset \mathcal{H}$ a non-trivial closed subspace of $\mathcal{H}$ invariant under $\rho(G)$. Defining $\mathcal{K}^\perp$ as the orthogonal supplementary of $\mathcal{K}$ in $\mathcal{H}$ for $\langle\cdot|\cdot\rangle$, it is immediate that $\mathcal{K}^\perp$ is also a non-trivial closed subspace of $\mathcal{H}$ invariant under $\rho(G)$. This provides the decomposition $\mathcal{H} = \mathcal{K} \oplus \mathcal{K}^\perp$ of $\mathcal{H}$ into a direct sum of subrepresentation spaces. Since by hypothesis $\dim\ \mathcal{K} < \dim\ \mathcal{H}$ and $\dim\ \mathcal{K}^\perp < \dim\ \mathcal{H}$, the result follows by recursivity.

Definition B.7 *Let G be a group and $\big(\rho, \mathcal{V}\big)$, $\big(\tau, \mathcal{W}\big)$ be two linear representations of G.*

- *$T \in \mathcal{L}(\mathcal{V}, \mathcal{W})$ is an entrelacing operator between $\big(\rho, \mathcal{V}\big)$ and $\big(\tau, \mathcal{W}\big)$ if :*

$$\forall\ g \in G,\ \forall\ v \in \mathcal{V},\ T(\rho(g)v) = \tau(g)T(v)$$

- *$\big(\rho, \mathcal{V}\big)$ and $\big(\tau, \mathcal{W}\big)$ are two equivalent linear representations of G if there exists an invertible entrelacing operator between them. Note that equivalence in the sense defined here is obviously an equivalence relation on the set of linear representations of G. This allows to define $\widehat{G}$, the so-called dual of G, as being the set of equivalence classes of the irreducible representations of G.*

Theorem B.8 *Let G be a group and T be an entrelacing operator between two finite-dimensional irreducible representations of G, $\big(\rho,\mathcal{V}\big)$ and $\big(\tau,\mathcal{W}\big)$.*

- *If $\big(\rho,\mathcal{V}\big)$ and $\big(\tau,\mathcal{W}\big)$ are not equivalent, then $T=0$.*
- *If $\big(\rho,\mathcal{V}\big)$ and $\big(\tau,\mathcal{W}\big)$ are equivalent, then $\mathcal{V}\cong\mathcal{W}$ and $\exists\ \alpha\neq 0:\ T=\alpha Id$.*

Proof : This follows directly from the fact that if $T:\mathcal{V}\to\mathcal{W}$ is an entrelacing operator, then on the one hand $\ker T$ and $\mathrm{Im}\ T$ are subspaces of $\mathcal{V}$ and $\mathcal{W}$ respectively which are invariant under $\rho(G)$ and $\tau(G)$ respectively, and on the other hand if $\mathcal{V}=\mathcal{W}$ any eigenspace of T is a subspace of $\mathcal{V}$ which is invariant under $\rho(G)$.

In the end, one thus get the so-called *canonical decomposition* of any finite-dimensional linear representation $\big(\rho,\mathcal{V}\big)$ of a given compact group G :

$$\big(\rho,\mathcal{V}\big)=\bigoplus_{\mathcal{Y}\in\widehat{G}}\big(\rho_{\mathcal{Y}},\mathcal{V}_{\mathcal{Y}}\big)$$

Definition/Proposition B.9 *Let G be a group.*
A function $\phi:G\to\mathbb{C}$ is said to be central if : $\forall\ g,h\in G,\ \phi(gh)=\phi(hg)$. This is equivalent to demanding that ϕ be constant on each conjugacy class $\mathcal{C}\in\overline{G}$ of G. Subsequently, a basis of the vector space of the central functions $G\to\mathbb{C}$ is provided by $\{\mathbb{1}_{\mathcal{C}},\ \mathcal{C}\in\overline{G}\}$, the set of indicative functions of the conjugacy classes of G.

An outstanding class of central functions on a group G is the one of the so-called *characters* of G :
One may associate to any linear representation $\big(\rho,\mathcal{V}\big)$ of G its character $\chi_{(\rho,\mathcal{V})}:g\in G\mapsto\mathrm{Tr}_{\mathcal{V}}\big(\rho(g)\big)$.
Two linear representations of G have same characters if and only if they are equivalent. This implies that $\{\chi_{(\rho_{\mathcal{Y}},\mathcal{V}_{\mathcal{Y}})},\ \mathcal{Y}\in\widehat{G}\}$ is another basis of the vector space of the central functions $G\to\mathbb{C}$.
Hence, one has the worth noticing fact : $|\overline{G}|=|\widehat{G}|:=N_G$.
The *character table* of the linear representation $\big(\rho,\mathcal{V}\big)$ of G can then be seen as the $N_G\times N_G$ matrix M such that : $\forall\ 1\leq i\leq N_G,\ \Pi^{\perp}_{\mathcal{V}_{\mathcal{Y}_i}}=\dfrac{1}{\sum\limits_{1\leq k\leq N_G}|M_{i,k}|}\sum\limits_{1\leq j\leq N_G}M_{i,j}\left(\sum\limits_{g\in\mathcal{C}_j}\rho(g)\right)$

B.2 Example : Representation of permutation groups on tensor products of Hilbert spaces

We consider here the particular case of the compact (actually even finite) group $\mathfrak{S}_t$ made of the $t!$ permutations of t elements.
For any Hilbert space $\mathcal{H}$, the tensor product Hilbert space $\mathcal{H}^{\otimes t}$ naturally holds a unitary representation of $\mathfrak{S}_t$, $\sigma\in\mathfrak{S}_t\mapsto U_\sigma\in\mathcal{U}(\mathcal{H}^{\otimes t})$, defined by :

$$\forall\ \sigma\in\mathfrak{S}_t,\ \forall\ |x_1\rangle,\ldots,|x_t\rangle\in\mathcal{H},\ U_\sigma|x_1\rangle\otimes\cdots\otimes|x_t\rangle=|x_{\sigma(1)}\rangle\otimes\cdots\otimes|x_{\sigma(t)}\rangle$$

If $\mathcal{H}\equiv\mathbb{C}^N$ is of finite dimension, so is $\mathcal{H}^{\otimes t}\equiv\mathbb{C}^{tN}$, so that the linear representation $\big(U,(\mathbb{C}^N)^{\otimes t}\big)$ of $\mathfrak{S}_t$ is completely reducible.
In this case, the U_σ, $\sigma\in\mathfrak{S}_t$, take the matrix form : $U_\sigma=\sum\limits_{1\leq i_1,\ldots,i_t\leq N}|i_1\rangle\otimes\cdots\otimes|i_t\rangle\langle i_{\sigma(t)}|\otimes\cdots\otimes\langle i_{\sigma(1)}|$,
where $\{|i\rangle,1\leq i\leq N\}$ denotes an orthonormal basis of $\mathbb{C}^N$.
The character of $\big(U,(\mathbb{C}^N)^{\otimes t}\big)$ can then easily be computed :

$$\forall\ \sigma\in\mathfrak{S}_t,\ \chi_{(U,(\mathbb{C}^N)^{\otimes t})}\big(U_\sigma\big)=\mathrm{Tr}_{(\mathbb{C}^N)^{\otimes t}}\big(U_\sigma\big)=N^{c(\sigma)}$$

where $c(\sigma)$ denotes the number of cycles in the permutation σ (including those of length 1).

Example B.10 $t = 2$

$\mathfrak{S}_2$	$\mathcal{C}_1 = (1^2)$	$\mathcal{C}_2 = (2^1)$
$\mathcal{Y}_1$	*1*	*1*
$\mathcal{Y}_2$	*1*	*-1*

In this most simple case, we have : $\begin{cases} \mathcal{C}_1 = \{id\} \\ \mathcal{C}_2 = \{(12)\} \end{cases}$ *, and* $\begin{cases} U_{id} = \mathbb{1}_{N\times N} \\ U_{(12)} = \mathbb{F}_{N\times N} \end{cases}$ *, where* $\mathbb{1}_{N\times N}$ *denotes the identity operator on* $\mathbb{C}^N \otimes \mathbb{C}^N$ *and* $\mathbb{F}_{N\times N}$ *the so-called swap operator between the two copies of* $\mathbb{C}^N$*.*

So : $\begin{cases} \Pi^{\perp}_{\mathcal{V}_{\mathcal{Y}_1}} = \frac{1}{2}\big(\mathbb{1}_{N\times N} + \mathbb{F}_{N\times N}\big) \\ \Pi^{\perp}_{\mathcal{V}_{\mathcal{Y}_2}} = \frac{1}{2}\big(\mathbb{1}_{N\times N} - \mathbb{F}_{N\times N}\big) \end{cases}$

Example B.11 $t = 3$

$\mathfrak{S}_3$	$\mathcal{C}_1 = (1^3)$	$\mathcal{C}_2 = (2^1, 1^1)$	$\mathcal{C}_3 = (3^1)$
$\mathcal{Y}_1$	*1*	*1*	*1*
$\mathcal{Y}_2$	*2*	*0*	*-1*
$\mathcal{Y}_3$	*1*	*-1*	*1*

Here : $\mathcal{C}_1 = \{id\}$*,* $\mathcal{C}_2 = \{(12), (13), (23)\}$ *and* $\mathcal{C}_3 = \{(123), (132)\}$*.*

So : $\begin{cases} \Pi^{\perp}_{\mathcal{V}_{\mathcal{Y}_1}} = \frac{1}{6}\big(\mathbb{1} + \big[U_{(12)} + U_{(13)} + U_{(23)}\big] + \big[U_{(123)} + U_{(132)}\big]\big) \\ \Pi^{\perp}_{\mathcal{V}_{\mathcal{Y}_2}} = \frac{1}{3}\big(2\mathbb{1} - \big[U_{(123)} + U_{(132)}\big]\big) \\ \Pi^{\perp}_{\mathcal{V}_{\mathcal{Y}_3}} = \frac{1}{6}\big(\mathbb{1} - \big[U_{(12)} + U_{(13)} + U_{(23)}\big] + \big[U_{(123)} + U_{(132)}\big]\big) \end{cases}$

Example B.12 $t = 4$

$\mathfrak{S}_4$	$\mathcal{C}_1 = (1^4)$	$\mathcal{C}_2 = (2^1, 1^2)$	$\mathcal{C}_3 = (2^2)$	$\mathcal{C}_4 = (3^1, 1^1)$	$\mathcal{C}_5 = (4^1)$
$\mathcal{Y}_1$	*1*	*1*	*1*	*1*	*1*
$\mathcal{Y}_2$	*3*	*1*	*-1*	*0*	*-1*
$\mathcal{Y}_3$	*2*	*0*	*2*	*-1*	*0*
$\mathcal{Y}_4$	*3*	*-1*	*-1*	*0*	*1*
$\mathcal{Y}_5$	*1*	*-1*	*1*	*1*	*-1*

In this last example : $\mathcal{C}_1 = \{id\}$*,* $\mathcal{C}_2 = \{(12), (13), (14), (23), (24), (34)\}$*,* $\mathcal{C}_3 = \{(12)(34), (13)(24), (14)(23)\}$*,*
$\mathcal{C}_4 = \{(123), (132), (124), (142), (134), (143), (234), (243)\}$ *and* $\mathcal{C}_5 = \{(1234), (1243), (1324), (1342), (1423), (1432)\}$*.*

B.3 Completely symmetric subspace of a tensor product of Hilbert spaces

For a given finite-dimensional Hilbert space $\mathcal{H} \equiv \mathbb{C}^N$, we denote by $\mathcal{S}(\mathcal{H}, t)$ the so-called *completely symmetric* subspace of $\mathcal{H}^{\otimes t}$, i.e. : $\mathcal{S}(\mathcal{H}, t) := \{X \in \mathcal{H}^{\otimes t},\ \forall\ \sigma \in \mathfrak{S}_t,\ U_\sigma X = X\}$.
In other words, $\mathcal{S}(\mathcal{H}, t) = \mathcal{V}_{\mathcal{Y}_1}$ is the invariant subspace of $\mathcal{H}^{\otimes t}$ that holds the trivial irreducible representation of $\mathfrak{S}_t$ on $\mathcal{H}^{\otimes t}$. So the orthogonal projector onto $\mathcal{S}(\mathcal{H}, t)$ is : $\Pi^{\perp}_{\mathcal{S}(\mathcal{H},t)} = \Pi^{\perp}_{\mathcal{V}_{\mathcal{Y}_1}} = \dfrac{1}{t!}\displaystyle\sum_{\sigma\in\mathfrak{S}_t} U_\sigma$.

Moreover, $\mathcal{S}(\mathcal{H}, t)$ has dimension $\binom{N+t-1}{t}$. Indeed, denoting by $\{|i\rangle, 1 \le i \le N\}$ an orthonormal basis of $\mathcal{H}$, $\{\Pi^{\perp}_{\mathcal{S}(\mathcal{H},t)}|i_1\rangle \otimes \cdots \otimes |i_t\rangle, 1 \le i_1 \le \cdots \le i_t \le N\}$ is an orthonormal basis of $\mathcal{S}(\mathcal{H}, t)$.

Now, let us consider the operator $P := \displaystyle\int_{\langle\psi|\psi\rangle=1} \big(|\psi\rangle\langle\psi|\big)^{\otimes t} d\psi$ on $\mathcal{H}^{\otimes t}$, where $d\psi$ denotes the uniform distribution on the unit vectors of $\mathcal{H}$, normalized by $\displaystyle\int_{\langle\psi|\psi\rangle=1} d\psi = 1$.
P is such that : $\forall\ X \in \mathcal{H}^{\otimes t},\ \forall\ \sigma \in \mathfrak{S}_t,\ U_\sigma P X = P X$, i.e. $\forall\ X \in \mathcal{H}^{\otimes t},\ PX \in \mathcal{S}(\mathcal{H}, t)$.
Thus : $\exists\ \alpha \in \mathbb{C} :\ P = \alpha \Pi^{\perp}_{\mathcal{S}(\mathcal{H},t)}$.

Yet : $\mathrm{Tr}(P) = \int_{\langle\psi|\psi\rangle=1} \big(\mathrm{Tr}\big(|\psi\rangle\langle\psi|\big)\big)^t d\psi = \int_{\langle\psi|\psi\rangle=1} d\psi = 1$. And : $\mathrm{Tr}\big(\Pi^{\perp}_{\mathcal{S}(\mathcal{H},t)}\big) = \dim \mathcal{S}(\mathcal{H},t) = \binom{N+t-1}{t}$.
So in the end : $P = \dfrac{1}{\binom{N+t-1}{t}} \Pi^{\perp}_{\mathcal{S}(\mathcal{H},t)} = \dfrac{1}{N \times \cdots \times (N+t-1)} \sum_{\sigma\in\mathfrak{S}_t} U_\sigma$ is the normalized orthogonal projector onto $\mathcal{S}(\mathcal{H},t)$.

C Von-Neumann algebras

C.1 General definitions and properties

Let $\mathcal{H}$ be a Hilbert space of finite dimension N and $\mathcal{M}(N)$ be the set of linear operators on $\mathcal{H}$. Let also G be a compact group of operators on $\mathcal{H}$ and $\mathcal{A} := \mathrm{Alg}(G)$ be the group algebra of G.

The compactness of G guarantees the existence and uniqueness of a normalized left and right invariant Haar measure on G, that we will denote by $d\mu_G$.
We can thus define the "twirl" of any $A \in \mathcal{M}(N)$ as :

$$P_G(A) := \int_G UAU^{-1} d\mu_G(U)$$

It is such that : $P_G(A) = A \;\Leftrightarrow\; \forall\, M \in \mathcal{A},\ [M,A] = 0$, which means that the "twirling" operation P_G is in fact the projection on the commutant algebra of $\mathcal{A}$, that we will denote by $\mathcal{A}'$.

One interesting property of the "twirling" operation is that, for all $A, B \in \mathcal{M}(N)$:

$$\begin{aligned}\mathrm{Tr}(P_G(A)B) =& \mathrm{Tr}\left(\int_G UAU^{-1} d\mu_G(U) B\right) = \int_G \mathrm{Tr}(UAU^{-1}B) d\mu_G(U)\\ =& \int_G \mathrm{Tr}(AU^{-1}BU) d\mu_G(U) = \mathrm{Tr}\left(A \int_G U^{-1}BU d\mu_G(U)\right) = \mathrm{Tr}(AP_G(B))\end{aligned}$$

As a consequence, if $A \in \mathcal{A}'$, i.e. if $P_G(A) = A$, then for all $B \in \mathcal{M}(N)$: $\mathrm{Tr}(AB) = \mathrm{Tr}(P_G(A)B) = \mathrm{Tr}(AP_G(B))$. This means that in order to calculate the traces $\mathrm{Tr}(AB)$ for all $B \in \mathcal{M}(N)$, we can actually restrict our attention to $B \in \mathcal{A}'$ without any loss of generality.

C.2 Example : Duality of $\mathcal{U}(N)$ and $\mathfrak{S}_t$

Let $\widetilde{\mathcal{H}} \equiv \mathbb{C}^N$ and $\mathcal{H} = \widetilde{\mathcal{H}}^{\otimes t} \equiv \mathbb{C}^{tN}$. We will denote by $\mathcal{U}(N)$ and $\mathcal{U}(tN)$ the groups of unitary operators on $\widetilde{\mathcal{H}}$ and $\mathcal{H}$ respectively.
We now consider the two following closed subgroups of $\mathcal{U}(tN)$ (and as such automatically compact) :

$$G := \{U^{\otimes t},\ U \in \mathcal{U}(N)\} \quad \text{and} \quad G' := \{U_\sigma,\ \sigma \in \mathfrak{S}_t\}$$

Note that $G \subset \mathcal{U}(tN)$ is the image of the unitary representation of $\mathcal{U}(N)$ on $\mathcal{H}$ and $G' \subset \mathcal{U}(tN)$ is the image of the unitary representation of $\mathfrak{S}_t$ on $\mathcal{H}$.

In this case, we have the following important result : The group algebras $\mathrm{Alg}(G)$ and $\mathrm{Alg}(G')$ are commutant to each other, i.e. $\mathrm{Alg}(G)' = \mathrm{Alg}(G')$ and $\mathrm{Alg}(G')' = \mathrm{Alg}(G)$. We say that the groups $\mathcal{U}(N)$ and $\mathfrak{S}_t$ *act dually* on $\mathcal{H}$ via the representations' images G and G'.

This implies that the so-called *highly symmetric* or *Werner* matrices, i.e. the matrices which commute with all the matrices from G, are actually the matrices which may be written as linear combinations of the matrices from G' :

$$\forall\, U \in \mathcal{U}(N),\ \Delta U^{\otimes t} = U^{\otimes t}\Delta \;\Leftrightarrow\; \Delta \in \mathrm{Alg}(G)' \;\Leftrightarrow\; \Delta \in \mathrm{Alg}(G') \;\Leftrightarrow\; \Delta = \sum_{\sigma\in\mathfrak{S}_t} \lambda_\sigma U_\sigma$$

And conversely the so-called *permutation invariant* matrices, i.e the matrices which commute with all the matrices from G', are actually the matrices which may be written as linear combinations of the matrices from G :

$$\forall\ \sigma \in \mathfrak{S}_t,\ \Delta U_\sigma = U_\sigma \Delta \ \Leftrightarrow\ \Delta \in \mathrm{Alg}(G')' \ \Leftrightarrow\ \Delta \in \mathrm{Alg}(G) \ \Leftrightarrow\ \Delta = \int_{U\in\mathcal{U}(N)} \lambda(U) U^{\otimes t}$$

D Alternative proof of a weaker version of theorem 5.3 and generalization of the method to obtain properties of a family of norms

In this section we first provide a way of demonstrating a slightly weaker result as the one given by theorem 5.3, but that has the advantage of being technically simpler. Furthermore, we will then be able to generalize quite straightforwardly the method to upper bound not only $\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(\left(\sum_{\sigma\in\mathfrak{S}_4^K} U_\sigma\right)\left(\Delta^{\otimes 4}\right)\right)$ but also $\mathrm{Tr}_{\mathcal{H}^{\otimes 2q}}\left(\left(\sum_{\sigma\in\mathfrak{S}_{2q}^K} U_\sigma\right)\left(\Delta^{\otimes 2q}\right)\right)$ for all $q \in \mathbb{N}*$, which will be turned into properties of an associated family of norms.

D.1 Alternative proof of a weaker version of theorem 5.3

Theorem D.1 *For all Hermitian matrix Δ on $\mathcal{H}$:*

$$Tr_{\mathcal{H}^{\otimes 4}}\left(\left(\bigotimes_{i=1}^K \sum_{\sigma_i\in\mathfrak{S}_4} U_{\sigma_i}\right)\left(\Delta^{\otimes 4}\right)\right) \leq 24^K \|\Delta\|_{2(K)}^4$$

For this it is enough to show that, for every K-tuple $\sigma \in \mathfrak{S}_4^K$, defining U_σ as $U_\sigma := \bigotimes_{i=1}^K U_{\sigma_i}$:

$$t(\sigma) := \left|\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(U_\sigma \Delta^{\otimes 4}\right)\right| \leq \max_{I\subset\{1,\ldots,K\}} \left[\mathrm{Tr}_{\mathcal{H}\setminus\mathcal{H}_I}\left(\mathrm{Tr}_{\mathcal{H}_I}\Delta\right)^2\right]^2 \tag{16}$$

We first have that for all $\sigma \in \mathfrak{S}_4^K$, applying the splitting map $\mathfrak{S}_4 \to \mathfrak{S}\times\mathfrak{S}$ to all the σ_i, $1 \leq i \leq K$, and using the Cauchy-Schwarz inequality (just as in the proof of theorem 5.3) and the arithmetic-geometric mean inequality :

$$t(\sigma) = \left|\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(U_\sigma \Delta^{\otimes 4}\right)\right| \leq \sqrt{\left|\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(U_{\sigma'}\Delta^{\otimes 4}\right)\right| \left|\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(U_{\sigma''}\Delta^{\otimes 4}\right)\right|} = \sqrt{t(\sigma')t(\sigma'')} \leq \frac{1}{2}t(\sigma') + \frac{1}{2}t(\sigma'') \tag{17}$$

Now, since $\Delta^{\otimes 4}$ is invariant under conjugation by elements of the form $(U_\sigma)^{\otimes K}$, $\sigma \in \mathfrak{S}_4$, we also have that t is invariant under conjugation by elements from the subgroup $G := \{(\sigma,\ldots,\sigma),\ \sigma\in\mathfrak{S}_4\}$ of $\mathfrak{S}_4^K$.
Yet, we can notice that the subset $\widetilde{\mathfrak{S}}$ of $\mathfrak{S}$ defined by $\widetilde{\mathfrak{S}} := \{id, (12)(34), (14)(23)\}$ is such that $\widetilde{\mathfrak{S}}^K$ is stable under conjugation by any element of G followed by splitting. And what is more, any given $\sigma \in \mathfrak{S}_4^K$ can be transformed into a tuple of elements of $\widetilde{\mathfrak{S}}^K$ by repeatedly conjugating by elements of G and splitting.

Thus, using equation 17, we get for all $\sigma \in \mathfrak{S}_4^K$ the upper bound : $t(\sigma) \leq \sum_\alpha p_\alpha t(\sigma^{(\alpha)})$, with certain $p_\alpha = \frac{1}{2^{k_\alpha}}$ that sum to 1, and the $\sigma^{(\alpha)}$ that belong to $\widetilde{\mathfrak{S}}^K$.

So eventually, for all $\sigma \in \mathfrak{S}_4^K$:

$$t(\sigma) \leq \max_{\pi \in \widetilde{\mathfrak{S}}^K} t(\pi) \tag{18}$$

In order to upper bound the traces on the right hand side of equation 18, let us deal with the following auxiliary problem.

Let $H = A \otimes B \otimes C$ be a finite dimensional 3-partite Hilbert space. For all hermitian matrix P on H and all unit vectors $|a\rangle, |a'\rangle \in A$, $|b\rangle, |b'\rangle \in B$ and $|c\rangle, |c'\rangle \in C$ we denote by $P_{a,b,c}^{a',b',c'}$ the matrix element $\langle c| \otimes \langle b| \otimes \langle a|P|a'\rangle \otimes |b'\rangle \otimes |c'\rangle$.

Let $\sigma = (\sigma_A, \sigma_B, \sigma_C) \in \mathfrak{S}_4^3$ be a 3-tuple of permutations.
For all hermitian matrix Δ on H, we have, with the $|a_q\rangle$, $|b_q\rangle$ and $|c_q\rangle$, $1 \leq q \leq 4$, respectively running through an orthonormal basis of A, B and C :

$$\mathrm{Tr}_{H^{\otimes 4}}\big((U_{\sigma_A} \otimes U_{\sigma_B} \otimes U_{\sigma_C})(\Delta^{\otimes 4})\big) = \sum_{\substack{a_1,b_1,c_1\\a_2,b_2,c_2\\a_3,b_3,c_3\\a_4,b_4,c_4}} \prod_{q=1}^{4} \Delta_{a_q,b_q,c_q}^{a_{\sigma_A(q)},a_{\sigma_B(q)},c_{\sigma_C(q)}}$$

We now consider the particular case $\sigma_A = id$, $\sigma_B = (12)(34)$ and $\sigma_C = (14)(23)$, in which we have :

$$\begin{aligned}\mathrm{Tr}_{H^{\otimes 4}}\big((U_{\sigma_A} \otimes U_{\sigma_B} \otimes U_{\sigma_C})(\Delta^{\otimes 4})\big) &= \sum_{\substack{a_1,b_1,c_1\\a_2,b_2,c_2\\a_3,b_3,c_3\\a_4,b_4,c_4}} \Delta_{a_1b_1c_1}^{a_1b_2c_4}\Delta_{a_2b_2c_2}^{a_2b_1c_3}\Delta_{a_3b_3c_3}^{a_3b_4c_2}\Delta_{a_4b_4c_4}^{a_4b_3c_1}\\ &= \sum_{\substack{b_1,c_1\\b_2,c_2\\b_3,c_3\\b_4,c_4}} \big[\mathrm{Tr}_A\Delta\big]_{b_1,c_1}^{b_2,c_4}\big[\mathrm{Tr}_A\Delta\big]_{b_2,c_2}^{b_1,c_3}\big[\mathrm{Tr}_A\Delta\big]_{b_3,c_3}^{b_4,c_2}\big[\mathrm{Tr}_A\Delta\big]_{b_4,c_4}^{b_3,c_1}\end{aligned}$$

Let us introduce the maximally entangled matrix on $C \otimes C$: $M_{C\otimes C} := \sum_{c,\widetilde{c}} |c\rangle \otimes |c\rangle\langle\widetilde{c}| \otimes \langle\widetilde{c}|$.

Now, let $R := (\mathrm{Tr}_A\Delta \otimes \mathbb{1}_C)(\mathbb{1}_B \otimes M_{C\otimes C})(\mathrm{Tr}_A\Delta \otimes \mathbb{1}_C)$.
We notice that, for all $b, b', c, c', \widetilde{c}, \widetilde{c}'$: $R_{b,c,\widetilde{c}}^{b',c',\widetilde{c}'} = \sum_{b''} \big[\mathrm{Tr}_A\Delta\big]_{b,c}^{b'',\widetilde{c}}\big[\mathrm{Tr}_A\Delta\big]_{b'',\widetilde{c}'}^{b',c'}$.
So that : $\mathrm{Tr}_{H^{\otimes 4}}\big((U_{\sigma_A} \otimes U_{\sigma_B} \otimes U_{\sigma_C})(\Delta^{\otimes 4})\big) = \sum_{\substack{b_1,b_3\\c_1,c_2,c_3,c_4}} R_{b_1,c_1,c_4}^{b_1,c_2,c_3} R_{b_3,c_2,c_3}^{b_3,c_1,c_4} = \mathrm{Tr}_{C\otimes C}\big(\mathrm{Tr}_B R\big)^2$.

Yet, defining P as $P := \big(\mathrm{Tr}_A\Delta \otimes \mathbb{1}_C\big)\left(\mathbb{1}_B \otimes \sum_c |c\rangle \otimes |c\rangle\right)$, we see that $R = PP^\dagger$. Hence R is a positive matrix, and so is $\mathrm{Tr}_B R$. Thus, using the fact that, for a positive matrix V, $\mathrm{Tr}\big(V^2\big) \leq \big(\mathrm{Tr}V\big)^2$, we get : $\mathrm{Tr}_{C\otimes C}\big(\mathrm{Tr}_B R\big)^2 \leq \big[\mathrm{Tr}_{B\otimes C\otimes C} R\big]^2 = \Big[\mathrm{Tr}_{B\otimes C}\big(\mathrm{Tr}_A\Delta\big)^2\Big]^2$.
So eventually : $\mathrm{Tr}_{H^{\otimes 4}}\big((U_{\sigma_A} \otimes U_{\sigma_B} \otimes U_{\sigma_C})(\Delta^{\otimes 4})\big) \leq \Big[\mathrm{Tr}_{H\setminus A}\left(\mathrm{Tr}_A\Delta\right)^2\Big]^2$.

We can now turn back to our initial problem.
For all $\pi \in \widetilde{\mathfrak{S}}^K$, we can define the following factors of the global Hilbert space $\mathcal{H}$:

- $\mathcal{A}(\pi) := \mathcal{H}_{i_1} \otimes \cdots \otimes \mathcal{H}_{i_a}$ with $\pi_{i_1}, \ldots, \pi_{i_a} = id$
- $\mathcal{B}(\pi) := \mathcal{H}_{i_{a+1}} \otimes \cdots \otimes \mathcal{H}_{i_b}$ with $\pi_{i_{a+1}}, \ldots, \pi_{i_b} = (12)(34)$
- $\mathcal{C}(\pi) := \mathcal{H}_{i_{b+1}} \otimes \cdots \otimes \mathcal{H}_{i_K}$ with $\pi_{i_{b+1}}, \ldots, \pi_{i_K} = (14)(23)$

$\mathcal{H}$ can then be written as : $\mathcal{H} = \mathcal{A}(\pi) \otimes \mathcal{B}(\pi) \otimes \mathcal{C}(\pi)$.
And hence : $t(\pi) = \left|\mathrm{Tr}_{\mathcal{H}^{\otimes 4}}\left(U_\pi \Delta^{\otimes 4}\right)\right| \leq \left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{A}(\pi)}\left(\mathrm{Tr}_{\mathcal{A}(\pi)}\Delta\right)^2\right]^2 \leq \max_{I\subset\{1,\ldots,K\}} \left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{H}_I}\left(\mathrm{Tr}_{\mathcal{H}_I}\Delta\right)^2\right]^2$.
Plugging this result in equation 18, we get equation 16 as wanted.

D.2 Generalization of the method to obtain properties of a family of norms

We consider, for simplicity, the case when $\mathcal{H} = \left(\mathbb{C}^d\right)^{\otimes K}$.
For all $p \in \mathbb{N}^*$ and all Hermitian matrix Δ on $\mathcal{H}$, we define :

$$\|\Delta\|_{p[K]} := \left(\int_{\substack{\langle\psi_i|\psi_i\rangle=1 \\ 1\leq i\leq K}} \left|\mathrm{Tr}\left(|\psi_1\rangle\langle\psi_1| \otimes \cdots \otimes |\psi_K\rangle\langle\psi_K|\Delta\right)\right|^p d\psi_1 \ldots d\psi_K\right)^{1/p}$$

Let us notice that if p is even, we have :

$$\left(\|\Delta\|_{p[K]}\right)^p = \frac{1}{\left[d \times \cdots \times (d+p-1)\right]^K} \mathrm{Tr}_{\mathcal{H}^{\otimes p}}\left(\left(\sum_{\sigma\in\mathfrak{S}_p^K} U_\sigma\right)\left(\Delta^{\otimes p}\right)\right)$$

So in particular by theorem 5.2 : $\|\Delta\|_{2[K]} = \frac{1}{\left[d(d+1)\right]^{K/2}}\|\Delta\|_{2(K)}$.
And by theorem D.1 above : $\|\Delta\|_{4[K]} \leq \frac{1}{\left[d(d+1)(d+2)(d+3)\right]^{K/4}}(4!)^{K/4}\|\Delta\|_{2(K)}$.
The norm $\|\cdot\|_{4[K]}$ is thus related to the norm $\|\cdot\|_{2[K]}$ by the inequality :

$$\|\Delta\|_{4[K]} \leq \left(\frac{d^2(d+1)^2}{d(d+1)(d+2)(d+3)}4!\right)^{K/4}\|\Delta\|_{2[K]}$$

By extending the method used to prove theorem D.1, we get more generally :

Theorem D.2 *For all $q \in \mathbb{N}^*$ and all Hermitian matrix Δ on $\mathcal{H}$:*

$$\|\Delta\|_{2q[K]} \leq \left(\frac{d^q(d+1)^q}{d \times \cdots \times (d+2q-1)}(2q)!\right)^{K/2q}\|\Delta\|_{2[K]} \underset{q\to\infty}{\sim} \left(\frac{2q}{e}\right)^K \|\Delta\|_{2[K]}$$

Proof : The only thing we actually have to show in order to prove theorem D.2 is that, for all $q \in \mathbb{N}^*$ and all Hermitian matrix Δ on $\mathcal{H}$:

$$\mathrm{Tr}_{\mathcal{H}^{\otimes 2q}}\left(\left(\sum_{\sigma\in\mathfrak{S}_{2q}^K} U_\sigma\right)\left(\Delta^{\otimes 2q}\right)\right) \leq \left((2q)!\right)^K \|\Delta\|_{2(K)}^{2q} \tag{19}$$

Let us define the following subset of $\mathfrak{S}_{2q}$, containing the identity and the permutations made of q disjoint transpositions that are invariant under the exchange $j \leftrightarrow 2q+1-j$, $1 \leq j \leq q$, i.e. under the conjugation by the product of transpositions $\prod_{j=1}^{q}(j, 2q+1-j)$:

$$\widetilde{\mathfrak{S}} := \left\{ id,\ \prod_{k=1}^{p}(i_k, i'_k)(2q+1-i_k, 2q+1-i'_k)\prod_{l=1}^{m}(j_l, 2q+1-j_l),\ 2p+m=q,\ 1 \leq i_k, i'_k, j_l \leq q \right\}$$

Just as in the special case $q=2$, letting $G := \{(\sigma,\ldots,\sigma), \sigma \in \mathfrak{S}_{2q}\}$, we have that $\widetilde{\mathfrak{S}}^K$ is stable under conjugation by an element of G followed by splitting, and that any element of $\mathfrak{S}_{2q}^K$ can be transformed into a tuple of elements of $\widetilde{\mathfrak{S}}^K$ by repeatedly conjugating by elements of G and splitting.
Thus, by repeated use of the Cauchy-Schwarz inequality and arithmetic-geometric mean inequality,

we get that for all $\sigma \in \mathfrak{S}_{2q}^K$: $\left|\mathrm{Tr}_{\mathcal{H}^{\otimes 2q}}\left(U_\sigma \Delta^{\otimes 2q}\right)\right| \leq \sum_\alpha p_\alpha \left|\mathrm{Tr}_{\mathcal{H}^{\otimes 2q}}\left(U_{\sigma^{(\alpha)}} \Delta^{\otimes 2q}\right)\right|$, with certain $p_\alpha = \dfrac{1}{2^{k_\alpha}}$ that sum to 1, and the $\sigma^{(\alpha)}$ that belong to $\widetilde{\mathfrak{S}}^K$.
So eventually, for all $\sigma \in \mathfrak{S}_{2q}^K$:

$$\left|\mathrm{Tr}_{\mathcal{H}^{\otimes 2q}}\left(U_\sigma \Delta^{\otimes 2q}\right)\right| \leq \max_{\pi \in \widetilde{\mathfrak{S}}^K} \left|\mathrm{Tr}_{\mathcal{H}^{\otimes 2q}}\left(U_\pi \Delta^{\otimes 2q}\right)\right| \tag{20}$$

Yet, once again similarly to the special case $q = 2$, for all $\pi \in \widetilde{\mathfrak{S}}^K$, we have the upper bound :

$$\begin{aligned}
\left|\mathrm{Tr}_{\mathcal{H}^{\otimes 2q}}\left(U_\pi \Delta^{\otimes 2q}\right)\right| &\leq \max_{I \subset \{1,\ldots,K\}} \left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{H}_I} \left(\mathrm{Tr}_{\mathcal{H}_I} \Delta\right)^2\right]^q \\
&\leq \sum_{I \subset \{1,\ldots,K\}} \left[\mathrm{Tr}_{\mathcal{H}\backslash\mathcal{H}_I} \left(\mathrm{Tr}_{\mathcal{H}_I} \Delta\right)^2\right]^q \\
&\leq \left[\sum_{I \subset \{1,\ldots,K\}} \mathrm{Tr}_{\mathcal{H}\backslash\mathcal{H}_I} \left(\mathrm{Tr}_{\mathcal{H}_I} \Delta\right)^2\right]^q
\end{aligned}$$

Since $\mathfrak{S}_{2q}^K$ contains $\left((2q)!\right)^K$ elements, we get equation 19 by simply plugging this result into equation 20 and suming over $\mathfrak{S}_{2q}^K$.

Theorem D.2 relates the norm $\|\cdot\|_{p[K]}$ to the norm $\|\cdot\|_{2[K]}$ whenever p is even. One might now wonder what can be said for p odd.
Yet, by Hölder's inequality, we have that for all Hermitian matrix Δ on $\mathcal{H}$:

$$\forall\ p, q, r \in \mathbb{N}^*,\ \frac{1}{p} + \frac{1}{q} = \frac{1}{r}\ \Rightarrow\ \|\mathbb{1}_{\mathcal{H}} \Delta\|_{r[K]} \leq \|\mathbb{1}_{\mathcal{H}}\|_{p[K]} \|\Delta\|_{q[K]} \text{ i.e. } \|\Delta\|_{r[K]} \leq \|\Delta\|_{q[K]}$$

Thus, for all Hermitian matrix Δ on $\mathcal{H}$:

$$\forall\ p, p' \in \mathbb{N}^*,\ p \leq p'\ \Rightarrow\ \|\Delta\|_{p[K]} \leq \|\Delta\|_{p'[K]}$$

Combining this monotonicity result for $p \mapsto \|\cdot\|_{p[K]}$ to theorem D.2, we finally get :

Theorem D.3 *For all $q \in \mathbb{N}^*$ and all Hermitian matrix Δ on $\mathcal{H}$:*

$$\|\Delta\|_{2q-1[K]} \leq \|\Delta\|_{2q[K]} \leq \left(\frac{d^q (d+1)^q}{d \times \cdots \times (d+2q-1)} (2q)!\right)^{K/2q} \|\Delta\|_{2[K]} \underset{q \to \infty}{\sim} \left(\frac{2q}{e}\right)^K \|\Delta\|_{2[K]}$$

Remark D.4 *It is actually possible to relate the norm $\|\cdot\|_{p[K]}$, $p \geq 2$, to the norm $\|\cdot\|_{2[K]}$ by a completely different approach described very recently in [28], following the submission of our results in [33]. Indeed, using a hypercontractive inequality of Beckner, one gets that for all $p \geq 2$ and all Hermitian matrix Δ on $\mathcal{H}$:*

$$\|\Delta\|_{p[K]} \leq (p-1)^K \|\Delta\|_{2[K]}$$

This upper bound is however asymptotically worse than the one obtained by our method.

These norms occur in many other issues related to quantum information theory than the one of distinguishing quantum states. One example amongst others appears in [29], with the description of a test which tells whether or not a multi-partite quantum state is a product state. The probability of acceptance of the generalized $2q$-copy product test on the K-partite state ρ described there is :

$$P_{(2q,K)}(\rho) := \left(\frac{d \times \cdots \times (d+2q-1)}{(2q)!}\right)^K \left(\|\rho\|_{2q[K]}\right)^{2q}$$

Using theorem D.2, the latter can be directly related to the probability of acceptance of the generalized 2-copy product test on the K-partite state ρ :

$$P_{(2q,K)}(\rho) \leq \left(2^q \frac{d \times \cdots \times (d+2q-1)}{d^q (d+1)^q}\right)^K P_{(2,K)}(\rho) \leq \left[(2q)!\right]^K P_{(2,K)}(\rho)$$

References

[1] **M.A. Nielsen, I.L. Chuang**, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[2] **W. Feller**, *An Introduction to Probability Theory and its Applications*, Wiley Series in Probability and Mathematical Statistics, New York, 1966.

[3] **A.S. Holevo**, "Statistical decision theory for quantum systems", J. Multivariate Analysis 3:337-394 (1973).

[4] **C.W. Helstrom**, *Quantum detection and estimation theory*, Academic Press, New York, 1976.

[5] **B. Simon**, *Representations of Finite and Compact Groups*, Graduate Studies in Mathematics Volume 10, American Mathematical Society, New York, 1996.

[6] **M. Reed, B. Simon**, *Methods of Modern Mathematical Physics - Functional Analysis*, Academic Press, New York, 1972.

[7] **I.C. Gohberg, M.G. Kreĭn**, *Introduction to the Theory of Linear Nonselfadjoint Operators in Hilbert Space*, Translations of Mathematical Monographs Volume 18, American Mathematical Society, Providence, 1969.

[8] **A. Dembo, O. Zeitouni**, *Large Deviations: Techniques and Applications*, Applications of Mathematics Volume 38, Springer-Verlag, Berlin Heidelberg, 2010.

[9] **M. Ledoux**, *The Concentration of Measure Phenomenon*, Mathematical Surveys and Monographs Volume 89, American Mathematical Society, Providence, 2001.

[10] **R. Penrose, W. Rindler**, *Spinors and Space-Time, Volume 1: Two-spinor calculus and relativistic fields*, Cambridge University Press, Cambridge, 1986.

[11] **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:0810.2327v2[quant-ph].

[12] **G. Zauner**, "Quantum designs: Foundations of a noncommutative design theory", International Journal of Quantum Information 9(1):445-507 (2011).

[13] **J.M. Renes, R. Blume-Kohout, A.J. Scott, C.M. Caves**, "Symmetric informationally complete quantum measurements", J. Math. Phys. 45.2171 (2004); arXiv:quant-ph/0310075v1.

[14] **A. Roy, A.J. Scott**, "Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements", J. Math. Phys. 48.072110 (2007); arXiv:quant-ph/0703025v2.

[15] **A.J. Scott**, "Tight informationally complete quantum measurements", J. Phys. A. 39.13507 (2006); arXiv:quant-ph/0604049v6.

[16] **A. Klappenecker, M. Roetteler**, "Mutually unbiased bases are complex projective 2-designs", Proc. ISIT 2005, pp.1740-1744, IEEE, Piscataway, NJ, 2005; arXiv:quant-ph/0502031v2.

[17] **A. Ambainis, J. Emerson**, "Quantum t-designs: t-wise independence in the quantum world", Proc. 22nd IEEE Conf. Computational Complexity (CCC007), pp.129-140, IEEE, Piscataway, NJ, 2007; arXiv:quant-ph/0701126v2.

[18] **R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki**, "Quantum entanglement", Rev. Mod. Phys. 81:865-942 (2009); arXiv:quant-ph/0702225v2.

[19] **M. Horodecki, P. Horodecki, R. Horodecki**, "Separability of mixed states: necessary and sufficient conditions"; arXiv:quant-ph/9605038v2.

[20] **C.H. Bennett, D.P. DiVicenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin, W.K. Wooters**, "Quantum Nonlocality without entanglement", Phys. Rev. A. 59.1070 (1999);arXiv:quant-ph/9804053v4.

[21] **H.N. Barnum, L. Gurvits**, "Largest separable balls around the maximally mixed bipartite quantum states", Phys. Rev. A. 66.062311 (2002); arXiv:quant-ph/0204159v2.

[22] **H.N. Barnum, L. Gurvits**, "Separable balls around the maximally mixed multipartite quantum states", Phys. Rev. A. 68.042312 (2003); arXiv:quant-ph/0302102v1.

[23] **K.G.H. Vollbrecht, R.F. Werner**, "Entanglement measures under symmetry", Phys. Rev. A. 64.062307; arXiv:quant-ph/0010095v2.

[24] **T. Eggeling, R.F. Werner**, "Hiding classical data in multi-partite quantum states", Phys. Rev. Lett. 89.097905; arXiv:quant-ph/0203004v2.

[25] **B.M. Terhal, D.P. DiVincenzo, D. Leung**, "Hiding Bits in Bell States", Phys. Rev. Lett. 86(25):5807-5810 (2001); arXiv:quant-ph/0011042v3.

[26] **D.P. DiVincenzo, D. Leung, B.M. Terhal**, "Quantum Data Hiding", IEEE Trans. Inf Theory 48(3):580-599 (2002); arXiv:quant-ph/0103098v1.

[27] **A.W. Harrow, A. Montanaro, A.J. Short**, "Limitations on quantum dimensionality reduction", Proc. ICALP'11, LNCS 6755, pp.86-97, Springer-Verlag, Berlin Heidelberg, 2011; arXiv[quant-ph]:1012.2262v2.

[28] **A. Montanaro**, "Some applications of hypercontractive inequalities in quantum information theory"; arXiv[quant-ph]:1208.0161v2.

[29] **A.W. Harrow, A. Montanaro**, "An efficient test for product states, with applications to quantum Merlin-Arthur games", Proc. 51st ASFCS, pp.633-642, 2010; arXiv:1001.0017.

[30] **F.G.S.L. Brandão, M. Christandl, J.T. Yard**, "Faithful Squashed Entanglement", Commun. Math. Phys. 306:805-830 (2011); arXiv[quant-ph]:1010.1750v5.

[31] **R. Ahlswede, A. Winter**, "Strong Converse for Identification Via Quantum Channels", IEEE Trans. Inf. Theory (2002); arXiv:quant-ph/001212v2.

[32] **J.A. Tropp**, "User-friendly tail bounds for sums of random matrices"; arXiv1004.4389v7.

[33] **C. Lancien, A. Winter**, "Distinguishing multi-partite states by local measurements"; arXiv[quant-ph]:1206.2884.

Acknowledgements

First and foremost, I have to say how immensely grateful I am towards Andreas Winter for having been so marvellous in supervising me. He managed indeed to find the perfect balance in the amount of autonomy he should leave me, questions being very precise at the start of the project when I really needed some guidance and becoming increasingly open as I was gaining in independence. Availability and receptiveness is another trait of his that would be worth pointing at : he could stop halfway through anything else he had been doing to listen to the account of my recent progress... as well as that of my long-lasting wanderings...! Eventually, how could I not mention the outstanding behaviour he had towards me regarding the whole results' release process? He in fact always considered the work as being *ours*, and therefore insisted, among other things, on my coming to AQIS'12 Conference in Suzhou at the end of August to present it myself. Being given such opportunity, three months only after having entered the field, was for sure quite unbelieveable.

Furthermore, never would I have imagined, before coming to Bristol, that I would grow so passionate for quantum information. This immediate keen interest, as mentioned above, is mainly due to Andreas' skills, both scientific and human. It nevertheless also has a lot to do with the general atmosphere in the Quantum Computation and Information Group at the University of Bristol. No sooner had I arrived than I was already considered as being an integral part of this cheerful team, that I therefore insist on thanking warmly here. A special thought goes to Steve Brierley for helpful explanations on t-designs and related topics, to Marcus Huber for a luminous introduction to some entanglement and separability problems, and to Milan Mosonyi for invaluable mathematical comments on the questions I was dealing with.

Eventually, I would like to assure Stéphane Attal, professor of Mathematics at the University Lyon 1, of my gratitude for having first thought about Andreas Winter as a possible placement supervisor for me, and then convinced him of accepting the job. All this project would not have seen the light of day without his help. Besides, neither would it have if the professors in the Mathematics Department at Polytechnique had not agreed to my going off from the path of "pure" mathematics. I thank them for the freedom they let me, which enabled me to truly blossom in a subject I am now definitely decided to continue in.