Generic local distinguishability and completely entangled subspaces

Jonathan Walgate[1] **and A J Scott**[2]

[1] Perimeter Institute for Theoretical Physics, 31 Caroline St N, Waterloo, Ontario N2L 2Y5, Canada
[2] Centre for Quantum Computer Technology and Centre for Quantum Dynamics, Griffith University, Brisbane, Queensland 4111, Australia

E-mail: jwalgate@perimeterinstitute.ca and andrew.scott@griffith.edu.au

Abstract

A subspace of a multipartite Hilbert space is *completely entangled* if it contains no product states. Such subspaces can be large with a known maximum size, s_{max}, approaching the full dimension of the system, D. We show that almost all subspaces with dimension $s \leqslant s_{max}$ are completely entangled and then use this fact to prove that n random pure quantum states are unambiguously locally distinguishable if and only if $n \leqslant D - s_{max}$. This condition holds for almost all sets of states of all multipartite systems and reveals something surprising. The criterion is identical for separable and nonseparable states: entanglement makes no difference.

PACS numbers: 03.67.−a, 03.65.Ta

1. Introduction

This paper addresses two broad questions. What properties characterize subspaces of multipartite quantum systems? How difficult is it to locally discriminate quantum states? These questions are fundamental to quantum information theory, but remarkably hard to answer in full. The sheer variety of quantum states makes a complete generalization difficult, and this is especially clear in multipartite Hilbert spaces, which confront us with a multitude of incompatible kinds of entanglement [1–3]. Amid such diversity, where exceptions abound to every rule of thumb, how can we form any intuition about typical quantum properties? Do typical properties even exist?

Yes, and this is thanks to the concentration of measure phenomenon expressed in Lévy's Lemma [4]. Loosely put, in Hilbert spaces of high dimension, pure quantum states chosen uniformly at random are likely to have average properties with probability approaching one. A property possessed by a random state with high probability might be regarded as typical;

a property possessed by a random state with unit probability, that is, by almost all states, is regarded as generic. When we characterize random states, and random subspaces, we are thus studying properties of which that can be regarded as typical or generic for all. In this paper we study generic properties. We will sketch some relevant facts concerning random states and subspaces in section 2, but for a thorough discussion, consider [5–8] and the references therein.

In section 3 we provide a complete answer to an important question: when are random subspaces of a multipartite quantum system completely entangled? That is, when are they void of product states? The answer: whenever any one subspace has this property. The same is found true for random subspaces of a bipartite system in relation to states of a given Schmidt rank. Highly entangled subspaces are relevant to quantum error-correcting codes [9, 10]. Random subspaces have been studied in a wide variety of contexts, such as entanglement measures [7], superdense coding [11] and enhancing the capacity of private quantum channels [12]. This list of applications is unlikely to be exhaustive; as we shall show, completely entangled subspaces are ubiquitous.

Three previous results are directly relevant to this paper. Hayden, Leung and Winter [7] have given a sufficient condition on the dimension of a random subspace of a bipartite system to typically contain only highly entangled states. Although only a small fraction of the overall Hilbert space is spanned, the subspace dimension can be made surprisingly large relative to the dimension of the subsystems. Wallach [13] and Parthasarathy [14] have independently proven that in a multipartite Hilbert space, $\mathcal{H} = \bigotimes_j \mathcal{H}_j$, the maximum dimension of a completely entangled subspace is $s_{\max} = D - \sum_j (d_j - 1) - 1$, where $d_j = \dim \mathcal{H}_j$ and $D = \dim \mathcal{H} = \prod_j d_j$. Parthasarathy also provides an explicit construction. Recently, Cubitt, Montanaro and Winter [21] have extended this result in the bipartite case and obtained maximal constructions of subspaces that are void of states with low Schmidt rank. We show that almost all subspaces have the same properties as these maximal constructions. Thus, for example, almost all multipartite subspaces with dimension $s \leqslant s_{\max}$ contain no product states.

In section 4 we answer a question intimately related to the above: when is a set of n random pure states unambiguously locally distinguishable? The answer: whenever $n \leqslant D - s_{\max} = 1 + \sum_j (d_j - 1)$. State discrimination is perhaps the most elementary physical task of all, and studying it under a restriction to local operations and classical communication (LOCC) provides insight into the local structure of quantum information. It has attracted much interest in recent years, but progress has been slowed by the abundance of special cases lurking in Hilbert space. Results have been restricted mostly to low dimensional systems, specific multipartite structures and small numbers of states [22–25]. These limitations are overcome for random states, which allow us to provide a complete generic solution for the unambiguous local distinguishability of pure states, over all multipartite quantum systems. A surprising fact then emerges: in almost all cases, entanglement makes no difference as to whether the states can be distinguished or not. Sets of random product states obey the exact same criterion as sets of random highly entangled states.

Our result recalls a recent discovery of Duan *et al* [26] that every complete basis for a multipartite Hilbert space contains some subset of exactly $1 + \sum_j (d_j - 1)$ locally unambiguously distinguishable states. One consequence of our result is that for almost all bases this is maximal. We also extend our analysis to the case of multiple copies, which allows some insight into the difficulties typically imposed by the restriction that separate measurements be performed on parts of a quantum system. To obtain the same information, separable measurements consume exponentially more copies of a system than are needed globally.

Finally, in section 5 we discuss some observations and open questions.

2. Randomness

Throughout this paper, we will use the adjectives 'random' and 'generic', and the adjectival phrases 'almost surely' and 'almost all', to describe pure quantum states and subspaces. By this we will mean the following.

Let $\mathcal{H} = \mathbb{C}^D$ be a Hilbert space of dimension D. A pure state ψ of $\mathcal{H}$ is represented by a unit vector $|\psi\rangle \in \mathcal{H}$, modulo a phase factor, $e^{i\theta}|\psi\rangle \sim |\psi\rangle$ and is thus a member of projective Hilbert space: $\psi \in P(\mathcal{H})$. This is just the space of lines passing through the origin in $\mathcal{H}$, or equivalently, the space of one-dimensional subspaces of $\mathcal{H}$. The space of s-dimensional subspaces of $\mathcal{H}$ is the Grassmannian $\mathrm{Gr}_s(\mathcal{H})$. Thus $P(\mathcal{H}) \cong \mathrm{Gr}_1(\mathcal{H})$.

There is a natural uniform probability measure on $\mathrm{Gr}_s(\mathcal{H})$ induced by the unit Haar measure ν [27] on the unitary group $\mathrm{U}(D)$. Explicitly, we fix a subspace $\mathcal{S} \in \mathrm{Gr}_s(\mathcal{H})$ and define $\mu_s(E) := \nu(\{U \in \mathrm{U}(D) : U\mathcal{S} \in E\})$ for any (Borel) subset $E \subseteq \mathrm{Gr}_s(\mathcal{H})$. This is the unique unitarily invariant probability measure on $\mathrm{Gr}_s(\mathcal{H})$. The probability measure induced on $P(\mathcal{H})$ in this way will be denoted by μ. We are now in a position to define random states and subspaces.

Definition 2.1. *A* random pure state *ψ of the Hilbert space $\mathcal{H}$ is a random variable that takes values in $P(\mathcal{H})$ and is distributed according to the uniform probability measure μ on $P(\mathcal{H})$.*

Definition 2.2. *A* random (s-dimensional) subspace *$\mathcal{S}$ of the Hilbert space $\mathcal{H}$ is a random variable that takes values in $\mathrm{Gr}_s(\mathcal{H})$ and is distributed according to the uniform probability measure μ_s on $\mathrm{Gr}_s(\mathcal{H})$.*

A random subspace (or random pure state) can thus be generated from a fixed subspace (of the same dimension), by applying a unitary chosen at random according to the Haar measure. A random pure state of a multipartite Hilbert space will, with probability one, have maximum Schmidt rank, and typically be highly entangled. A set of $s \leqslant D$ random pure states will, with probability one, be linearly independent. The span of these states is then a random s-dimensional subspace. This is because the measure induced on $\mathrm{Gr}_s(\mathcal{H})$ is unitarily invariant, and hence, can only be μ_s. If $\mathcal{S} \leqslant \mathcal{H}$ is a random s-dimensional subspace, then $\mathcal{S}^\perp$ is a random $(D - s)$-dimensional random subspace, where $\mathcal{S} \oplus \mathcal{S}^\perp = \mathcal{H}$.

We will occasionally use the terms 'generic', 'almost surely' and 'almost all'. When we say a random pure state *almost surely* has some specific property, then we mean that this property occurs with unit probability. This means the property is true for all pure states except those on a set of zero μ-measure. Thus, put simply, *almost all* pure states have this property; more precisely, μ-*almost all* pure states have this property. The property is then called *generic*. The same terminology is used for random subspaces and sets of random pure states, except that μ is replaced by μ_s or the product measure $\mu \times \cdots \times \mu$, respectively.

3. Completely entangled random subspaces

It is known that reasonably large subspaces of Hilbert spaces can be completely entangled. A dramatic demonstration of this fact was provided by Hayden *et al* [7]. Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ with $d_2 \geqslant d_1 \geqslant 3$, where $d_1 = \dim \mathcal{H}_1$, $d_2 = \dim \mathcal{H}_2$, and we set $D = d_1 d_2 = \dim \mathcal{H}$. Then for any $0 < c < 1$ there exists a subspace $\mathcal{S} \leqslant \mathcal{H}$ of dimension

$$ s = \left\lfloor \frac{c^{2.5}}{1753} D \right\rfloor, \tag{1} $$

containing only states with entanglement $E \geqslant (1 - c) \log d_1 - (1/\ln 2)d_1/d_2$ bits, where
$E(\psi) := -\mathrm{tr}\rho_A \log \rho_A$ with $\rho_A = \mathrm{tr}_B|\psi\rangle\langle\psi|$. Moreover, the probability for a random
subspace of dimension s to not have this property is bounded above by

$$\left(\frac{15}{c}\right)^{2s} \exp\left(-\frac{(D-1)c^2}{32\pi^2 \ln(2)}\right). \tag{2}$$

Thus, in increasing dimensions, random subspaces of dimension s (or smaller) are typically
completely entangled, with probability exponentially approaching one. These subspaces are
surprisingly large. For instance, if $\mathcal{H}_1$ and $\mathcal{H}_2$ are both n qubit systems, then $\mathcal{S}$ is a subspace
of dimension equal to that of a $2n - O(1)$ qubit system. Nevertheless, s is always a small
fraction of D.

Wallach [13] and Parthasarathy [14] independently showed that much larger dimensions
could be spanned without encompassing any product states. In particular, the following was
proven.

Theorem 3.1 (Wallach [13], Parthasarathy [14]). *Let $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ be a multipartite Hilbert
space with $\dim \mathcal{H}_j = d_j$ and $\dim \mathcal{H} = D = \prod_j d_j$. Then there exists a completely entangled
subspace $\mathcal{S} \leqslant \mathcal{H}$ of dimension s if and only if*

$$s \leqslant D - \sum_j (d_j - 1) - 1. \tag{3}$$

We thus define the maximum possible dimension of a completely entangled subspace:

$$s_{\max} := D - \sum_j (d_j - 1) - 1. \tag{4}$$

In comparison to the result of Hayden *et al* for bipartite systems (1), if $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, where $\mathcal{H}_1$
and $\mathcal{H}_2$ are both n qubit systems, then a completely entangled subspace can have a dimension
equal to that of a $2n - O(2^{-n})$ qubit system.

We extend theorem 3.1 in corollary 3.5 below, where we show that a random subspace of
dimension $s_{\max}$ or less is almost surely void of product states. Two different but equivalent
approaches will be taken. First, we use a theorem of differential geometry to give an explicit,
straightforward proof. Then a refined approach is taken, which is based on the theory of
algebraic geometry. While the latter method is arguably more obscure, given the conceptual
hurdles that must be overcome, it will ultimately prove to be more powerful.

3.1. Completely entangled random subspaces: a differential geometry approach

Consider the following variation of Sard's theorem of differential geometry [15–17]. A proof
was sketched by Chow *et al* [18], but consider Keerthi *et al* [19] for a guide to its use in
establishing genericity. Let $f : X \subseteq \mathbb{R}^M \to \mathbb{R}^N$ be $\mathcal{C}^1$, i.e. a differentiable function whose
first derivative is continuous. We say that $x \in X$ is a *regular point* of f if the Jacobian $\mathrm{D}f(x)$
has full row rank. If the set $f^{-1}(y)$, the preimage of $y \in \mathbb{R}^N$, contains only regular points,
then y is called a *regular value* of f. The phrase 'almost all' is used in the sense of the
Lebesgue measure in the following.

Theorem 3.2 (Parametrized Sard theorem). *Let $X \subseteq \mathbb{R}^L$ and $Y \subseteq \mathbb{R}^M$ be open, and let
$f : X \times Y \to \mathbb{R}^N$ be $\mathcal{C}^r$ with $r > \max\{0, L - N\}$. If $0 \in \mathbb{R}^N$ is a regular value of f, then for
almost all $y \in Y$, 0 is a regular value of $f(\cdot, y)$. In particular, $\tilde{X}(y) := \{x \in X : f(x, y) = 0\}$
is either empty or a differentiable manifold of dimension $L - N$, for almost all $y \in Y$.*

Corollary 3.3. *Let $X \subseteq \mathbb{R}^L$ and $Y \subseteq \mathbb{R}^M$ be open, and let $f : X \times Y \to \mathbb{R}^N$ be C^r with $r > \max\{0, L - N\}$. If $0 \in \mathbb{R}^N$ is a regular value of f and $L < N$, then $\tilde{X}(y) := \{x \in X : f(x, y) = 0\}$ is empty for almost all $y \in Y$.*

The parametrized Sard theorem, or more specifically corollary 3.3, is applied to the current problem by simply associating the variable x with an arbitrary product pure state, the variable y with an arbitrary set of n general pure states, and then defining f as the vector function of inner products between the product and general states. The trick is to choose x and y in such a way that 0 is guaranteed a regular value of f. The fact that this is so easily done is a feature of complex projective space. The problem then reduces to a parameter counting argument.

Theorem 3.4. *Let $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ be a multipartite Hilbert space with $\dim \mathcal{H}_j = d_j$. Then for μ-almost all pure states $\psi_1, \ldots, \psi_n \in P(\mathcal{H})$, if*

$$n > \sum_j (d_j - 1), \tag{5}$$

no product state is orthogonal to all of $|\psi_1\rangle, \ldots, |\psi_n\rangle$.

Proof. Let $\{|k_1\rangle \otimes \cdots \otimes |k_m\rangle\}_{k_j = 1, \ldots, d_j}$ be an orthonormal product basis for $\mathcal{H} = \bigotimes_{j=1}^m \mathcal{H}_j$. Parametrize an unnormalized product pure state of $\mathcal{H}$ as

$$|\xi(a^1, \ldots, a^m)\rangle\!\rangle := \sum_{k_1, \ldots, k_m} \left(a_{k_1}^1\right)^* \cdots \left(a_{k_m}^m\right)^* |k_1\rangle \otimes \cdots \otimes |k_m\rangle, \tag{6}$$

where each $a_{k_j}^j \in \mathbb{C}$, and thus, $a^j \in \mathbb{C}^{d_j}$. The notation $|\cdot\rangle\!\rangle$ will be used for the duration of this proof to emphasize that such vectors are generally unnormalized. Parametrize an unnormalized general pure state of $\mathcal{H}$ as

$$|\eta(b)\rangle\!\rangle := \sum_{k_1, \ldots, k_m} b_{k_1 \cdots k_m} |k_1\rangle \otimes \cdots \otimes |k_m\rangle, \tag{7}$$

where each $b_{k_1 \cdots k_m} \in \mathbb{C}$, and thus, $b \in \mathbb{C}^D$. Furthermore, define the polynomial functions

$$g_p(a^1, \ldots, a^m; b^1, \ldots, b^n) := \langle\!\langle \xi(a^1, \ldots, a^m) | \eta(b^p) \rangle\!\rangle \tag{8}$$

$$= \sum_{k_1, \ldots, k_m} a_{k_1}^1 \cdots a_{k_m}^m b_{k_1 \cdots k_m}^p, \tag{9}$$

for $p = 1, \ldots, n$. Thus there is a product state orthogonal to the subspace

$$\mathcal{S}(b^1, \ldots, b^n) := \text{span}\{|\eta(b^1)\rangle\!\rangle, \ldots, |\eta(b^n)\rangle\!\rangle\} \tag{10}$$

if and only if $g_1(a^1, \ldots, a^m; b^1, \ldots, b^n) = \cdots = g_n(a^1, \ldots, a^m; b^1, \ldots, b^n) = 0$ has a solution in the variables $a^1, \ldots, a^m$.

Now define the sets

$$A_{k_1 \cdots k_m} := \left\{ (a^1, \ldots, a^m) \in \mathbb{C}^{d_1} \times \cdots \times \mathbb{C}^{d_m} : a_{k_1}^1 = \cdots = a_{k_m}^m = 1 \right\}, \tag{11}$$

which specify subsets of product states,

$$\Xi_{k_1 \cdots k_m} := \left\{ |\xi(a^1, \ldots, a^m)\rangle\!\rangle : (a^1, \ldots, a^m) \in A_{k_1 \cdots k_m} \right\}, \tag{12}$$

whose union, $\Xi := \cup_{k_1 \cdots k_m} \Xi_{k_1 \cdots k_m}$, includes a representative of each normalized product state, i.e. every normalized product state can be written as $|\phi\rangle = c|\xi\rangle\!\rangle$ for some $|\xi\rangle\!\rangle \in \Xi$ and $c \in \mathbb{C}$.

First consider $\mathcal{S}^{\perp} \cap \Xi_{1\ldots1}$. Since

$$\frac{\partial g_p}{\partial b_{1\ldots1}^q} = \delta_{qp} a_1^1 \cdots a_1^m = \delta_{qp}, \tag{13}$$

if $(a^1, \ldots, a^m) \in A_{1\ldots1}$, the Jacobian $\mathrm{D}g(a^1, \ldots, a^m; b^1, \ldots, b^n)$ has full (complex) rank for all $(a^1, \ldots, a^m) \in A_{1\ldots1}$ and all $b^1, \ldots, b^n$. Now set

$$f(x, y) := (\mathrm{Re}(g_1), \ldots, \mathrm{Re}(g_n), \mathrm{Im}(g_1), \ldots), \tag{14}$$

where

$$x := \left(\mathrm{Re}(a_2^1), \ldots, \mathrm{Re}(a_{d_1}^1), \mathrm{Re}(a_2^2), \ldots, \mathrm{Re}(a_{d_m}^m), \mathrm{Im}(a_2^1), \ldots\right) \in \mathbb{R}^{2(d_1+\cdots+d_m-m)}, \tag{15}$$

$$y := \left(\mathrm{Re}(b_{1\ldots1}^1), \ldots, \mathrm{Re}(b_{d_1\ldots d_m}^1), \mathrm{Re}(b_{1\ldots1}^2), \ldots, \mathrm{Re}(b_{d_1\ldots d_m}^n), \mathrm{Im}(b_{1\ldots1}^1), \ldots\right) \in \mathbb{R}^{2nD}. \tag{16}$$

Since each g_p is an analytic function in its variables, the Jacobian $\mathrm{D}f(x, y)$ will also have full (real) rank for all x and y (consider the Cauchy–Riemann equations). Now with $X = \mathbb{R}^L$, $Y = \mathbb{R}^M$, $L = 2(d_1 + \cdots + d_m - m)$, $M = 2nD$ and $N = 2n$, by corollary 3.3, $\tilde{X}(y) := \{x \in X : f(x, y) = 0\} = \emptyset$ for almost all $y \in Y$ (in the sense of the Lebesgue measure) whenever $L < N$. Equivalently, $\mathcal{S}^{\perp}(y) \cap \Xi_{1\ldots1} = \emptyset$ for almost all $y \in Y$ whenever $n > \sum_j (d_j - 1)$.

Repeating the above argument for all sets $A_{k_1 \cdots k_m}$, and given that the finite union of sets of measure zero is again of measure zero, we conclude that $\mathcal{S}^{\perp}(y) \cap \Xi = \emptyset$ for almost all $y \in Y$ whenever $n > \sum_j (d_j - 1)$.

Finally, note that we can rewrite each $|\eta(b^j)\rangle\!\rangle = r_j \mathrm{e}^{\mathrm{i}\theta_j} |\psi_j\rangle$, where $r_j \geqslant 0$, $0 \leqslant \theta_j < 2\pi$ and $|\psi_j\rangle$ is a normalized pure state specified by $\psi_j \in \mathrm{P}(\mathcal{H})$. Now since the current measure on unnormalized pure states (essentially the Lebesgue measure on $\mathbb{R}^{2D}$) is related to the uniform probability measure μ on $\mathrm{P}(\mathcal{H})$ (described in section 2) through the differential

$$\mathrm{d}\,\mathrm{Re}(b_{1\ldots1}) \cdots \mathrm{d}\,\mathrm{Re}(b_{d_1\ldots d_m})\mathrm{d}\,\mathrm{Im}(b_{1\ldots1}) \cdots \mathrm{d}\,\mathrm{Im}(b_{d_1\ldots d_m}) = r^{2D-1}\,\mathrm{d}r\,\mathrm{d}\theta\,\mathrm{d}\mu(\psi), \tag{17}$$

and furthermore, $\mathcal{S}(b^1, \ldots, b^n) = \mathrm{span}\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$, independent of each r_j and θ_j, the above will be contradicted unless $\mathcal{S}^{\perp}$ contains no product states for μ-almost all $\psi_1, \ldots, \psi_n \in \mathrm{P}(\mathcal{H})$, whenever $n > \sum_j (d_j - 1)$. $\square$

Recall that the product measure $\mu \times \cdots \times \mu$ on $\mathrm{P}(\mathcal{H}) \times \cdots \times \mathrm{P}(\mathcal{H})$ (both n times) induces the uniform probability measure μ_n on $\mathrm{Gr}_n(\mathcal{H})$, since the former is unitarily invariant, and $n \leqslant D$ random pure states almost surely span n dimensions. The following is thus equivalent to theorem 3.4.

Corollary 3.5. *Let $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ be a multipartite Hilbert space with $\dim \mathcal{H}_j = d_j$ and $\dim \mathcal{H} = D = \prod_j d_j$. Then for μ_s-almost all subspaces $\mathcal{S} \in \mathrm{Gr}_s(\mathcal{H})$, if*

$$s \leqslant s_{\max} = D - \sum_j (d_j - 1) - 1, \tag{18}$$

$\mathcal{S}$ *contains no product states.*

Random subspaces do not contain product states unless they it have to, since if $s > s_{\max}$, then by theorem 3.1, *all* subspaces $\mathcal{S} \in \mathrm{Gr}_s(\mathcal{H})$ contain at least one product state. Wallach and Parthasarathy both proved this last fact using algebraic geometry. In fact, all of the above results are consequences of this theory, which we will explain next. We end this subsection with a straightforward corollary of theorem 3.4. This will be needed later in this paper.

Corollary 3.6. *Let $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ be a multipartite Hilbert space with $\dim \mathcal{H}_j = d_j$, and let c be any positive integer. Then for μ-almost all pure states $\psi_1, \ldots, \psi_n \in \mathrm{P}(\mathcal{H})$, if*

$$n > c \sum_j (d_j - 1), \tag{19}$$

no product state of $\mathcal{H}^{\otimes c} = (\bigotimes_j \mathcal{H}_j)^{\otimes c}$ (between all subsystems) is orthogonal to all of $|\psi_1\rangle^{\otimes c}, \ldots, |\psi_n\rangle^{\otimes c}$.

Proof. Let $n > c \sum_j (d_j - 1)$ and let ϕ be a product state of $\mathcal{H}^{\otimes c}$,

$$|\phi\rangle = |\phi_1\rangle \otimes \cdots \otimes |\phi_c\rangle, \tag{20}$$

where each ϕ_j is a product state of $\mathcal{H}$. Suppose that $\langle \phi | (|\psi_k\rangle^{\otimes c}) = 0$ for all k, i.e.,

$$\langle \phi_1 | \psi_k \rangle \langle \phi_2 | \psi_k \rangle \cdots \langle \phi_c | \psi_k \rangle = 0, \tag{21}$$

for $k = 1, \ldots, n$. To satisfy all n of these equations there must be at least one product state, $\phi_{j'}$ say, with $\langle \phi_{j'} | \psi_k \rangle = 0$ for $m > \sum_j (d_j - 1)$ values of k. But if the states ψ_k are chosen randomly, this is almost surely impossible, since otherwise we would contradict theorem 3.4. Thus there is no product state orthogonal to all of $|\psi_1\rangle^{\otimes c}, \ldots, |\psi_n\rangle^{\otimes c}$ for μ-almost all choices of $\psi_1, \ldots, \psi_n \in \mathrm{P}(\mathcal{H})$. □

3.2. Completely entangled random subspaces: an algebraic geometry approach

A *complex projective variety* X is an algebraic subset of $\mathrm{P}(\mathbb{C}^D)$, i.e., X can be specified as the common zero locus of a set $S \subset \mathbb{C}[x_1, \ldots, x_D]$ (which can be assumed finite) of homogeneous polynomials in the coordinates of $\mathbb{C}^D$,

$$X = V(S) := \{x \in \mathrm{P}(\mathbb{C}^D) : f(x_1, \ldots, x_D) = 0 \text{ for all } f \in S\}, \tag{22}$$

where $x_k := \langle k | x \rangle$ for some fixed basis $\{|k\rangle\}_{k=1,\ldots,D}$ of $\mathbb{C}^D$. This makes sense because a homogeneous polynomial satisfies $f(cx_1, \ldots, cx_D) = c^k f(x_1, \ldots, x_D)$ by definition, and thus, if f vanishes on any point of the line specified by x, then it vanishes for all. An example of a variety is a projective subspace, or $(s-1)$-*plane*:

$$\Lambda_{\mathcal{S}} := \mathrm{P}(\mathcal{S}) = \{x \in \mathrm{P}(\mathbb{C}^D) : |x\rangle \in \mathcal{S}\}, \tag{23}$$

where $\mathcal{S} \in \mathrm{Gr}_s(\mathbb{C}^D)$. This is of course the locus of solutions to $D - s$ homogeneous linear equations: $\mathcal{S}^\perp |x\rangle = 0$. In general, complex projective varieties are finite collections of submanifolds of $\mathrm{P}(\mathbb{C}^D)$. There are many good texts on algebraic geometry, of which, Harris [20] is perhaps the most readable introduction. We should remark, however, that some authors reserve the term 'variety' for what we will be calling an irreducible variety; we follow Harris and allow any algebraic set.

Note that the intersection of any two varieties is always another variety, since $V(S) \cap V(T) = V(S \cup T)$. In fact, because $\mathbb{C}[x_1, \ldots, x_D]$ is a Noetherian ring, we can show that the intersection of any number of varieties is another. Additionally, the union of any finite number of varieties is another variety, since for any two, $V(S) \cup V(T) = V(ST)$, where $ST = \{fg : f \in S, g \in T\}$. The empty set and entire space are also varieties: $\emptyset = V(\{1\})$ and $\mathrm{P}(\mathbb{C}^D) = V(\emptyset)$. These properties define a topology on $\mathrm{P}(\mathbb{C}^D)$, called the *Zariski topology*, where the subvarieties $X \subseteq \mathrm{P}(\mathbb{C}^D)$ are defined as the closed sets, or more formally, the *Zariski closed sets*. A *Zariski open set* X^c is then the complement in $\mathrm{P}(\mathbb{C}^D)$ of some variety X. We should remark here, however, that the Zariski topology is only a formal construct of algebraic geometry and reflects little of the usual topology of complex projective space. Any nonempty Zariski open set is both of full μ-measure and dense in the usual topology, being the complement of a finite collection of proper submanifolds of $\mathrm{P}(\mathbb{C}^D)$.

A variety X is called *irreducible* if for each pair of subvarieties $Y, Z \subseteq X$ such that $Y \cup Z = X$, either $Y = X$ or $Z = X$. Any $(s-1)$-plane, for example, from a single point up to the entire space itself is an irreducible variety. The concept of dimension can be defined for irreducible varieties. There are various equivalent definitions, three of which are as follows.

Definition 3.7 (Harris [20, p 134]). *The dimension of an irreducible complex projective variety $X \subseteq P(\mathbb{C}^D)$, denoted by* dim X, *can be defined in three equivalent ways:*

(1) dim X *is the smallest integer d such that there exists a $(D - d - 2)$-plane disjoint from X.*
(2) dim X *is the smallest integer d such that the general $(D - d - 2)$-plane is disjoint from X.*
(3) dim X *is that integer d such that the general $(D - d - 1)$-plane intersects X in a finite set of points.*

This means dim $\Lambda_{\mathcal{S}} = \dim \mathcal{S} - 1$, and in particular, dim $P(\mathbb{C}^D) = D - 1$. The equivalence of these definitions should be shown, but we will take them as fact. All three indirectly imply something important about the number of product pure states contained in a subspace of multipartite Hilbert space.

Consider definition 3.7.1 for example. Define $\sigma : P(\mathbb{C}^{d_1}) \times P(\mathbb{C}^{d_2}) \to P(\mathbb{C}^{d_1 d_2})$ by $\sigma(x, y) = z$ where $z_{jk} = x_j y_k$. The image of this map $\Sigma_{d_1, d_2} := \sigma(P(\mathbb{C}^{d_1}) \times P(\mathbb{C}^{d_2}))$ is then a variety, called the *Segre variety*. It is the locus of solutions to the quadratic equations $z_{ij} z_{kl} - z_{il} z_{kj} = 0$. Importantly, σ defines the *Segre embedding* of the Cartesian product of two projective spaces into a larger projective space. It shows how the Cartesian product of two varieties, $X \times Y \subseteq P(\mathbb{C}^{d_1}) \times P(\mathbb{C}^{d_2})$, can be considered another variety in the larger space, $\sigma(X \times Y) \subseteq P(\mathbb{C}^{d_1 d_2})$. If X and Y are irreducible, then so is $\sigma(X \times Y)$, with dim $\sigma(X \times Y) = \dim X + \dim Y$. In particular, Σ_{d_1, d_2} is irreducible with dimension

$$\dim \Sigma_{d_1, d_2} = \dim P(\mathbb{C}^{d_1}) + \dim P(\mathbb{C}^{d_2}) = (d_1 - 1) + (d_2 - 1). \tag{24}$$

Now define the general Segre variety $\Sigma_{d_1, \dots, d_m} := \sigma\left(\Sigma_{d_1, \dots, d_{m-1}} \times P(\mathbb{C}^{d_m})\right)$ recursively. Then

$$\dim \Sigma_{d_1, \dots, d_m} = \sum_j (d_j - 1). \tag{25}$$

Finally, given that $\Sigma_{d_1, \dots, d_m} \subseteq P(\mathbb{C}^D)$, $D = \prod_j d_j$ is really just the set of product states for the multipartite Hilbert space $\mathcal{H} = \bigotimes_j \mathbb{C}^{d_j}$, theorem 3.1 is a straightforward consequence of definition 3.7.1.

Now consider definition 3.7.2. We first need to describe what is meant by a 'general' $(s-1)$-plane. An algebraic subset of the Grassmannian $\text{Gr}_s(\mathbb{C}^D)$ can be viewed as a projective variety under the Plücker embedding. We refer to Harris [20] for the details, but for our purposes, simply note that there is a Zariski topology on $\text{Gr}_s(\mathbb{C}^D)$ analogous to that for $P(\mathbb{C}^D)$. Now when we say that the *general* $(s-1)$-plane has some property, we mean that the subset of $(s-1)$-planes with this property, $\{\Lambda_{\mathcal{S}}\}_{\mathcal{S} \in S}$, is specified by a parameter set $S \subseteq \text{Gr}_s(\mathbb{C}^D)$ that contains a nonempty Zariski open subset of $\text{Gr}_s(\mathbb{C}^D)$. This means S has full μ_s-measure. Thus, given the dimension of the Segre variety (25), corollary 3.5 (and theorem 3.4) becomes a straightforward consequence of definition 3.7.2.

Finally, consider the last definition of dimension, definition 3.7.3. As implied by this variation, for any irreducible variety X, the general $(D - \dim X - 1)$-plane intersects X at a finite nonzero number of points. This number is the degree of the variety.

Definition 3.8 (Harris [20, p 225]). *The* degree *of an irreducible complex projective variety $X \subseteq P(\mathbb{C}^D)$, denoted by* deg X, *is the number of points at which the general $(D - \dim X - 1)$-plane intersects X.*

It is in fact a feature of complex projective space that any two irreducible varieties, $X, Y \subseteq P(\mathbb{C}^D)$, must intersect whenever $\dim X + \dim Y \geqslant D - 1$ (theorem 3.1 is partly based on this fact). In the case of the Segre variety,

$$\deg \Sigma_{d_1,\ldots,d_m} = \frac{(\sum_j (d_j - 1))!}{\prod_j (d_j - 1)!}, \tag{26}$$

which is derived recursively with the help of Harris [20, Ex 19.2]. The following now generalizes corollary 3.5.

Corollary 3.9. *Let* $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ *be a multipartite Hilbert space with* $\dim \mathcal{H}_j = d_j$ *and* $\dim \mathcal{H} = D = \prod_j d_j$. *Then for* μ_s-*almost all subspaces* $\mathcal{S} \in \mathrm{Gr}_s(\mathcal{H})$, *the number of product states contained in* $\mathcal{S}$ *is exactly*

$$\begin{cases} 0, & \text{if} \quad s \leqslant s_{\max} = D - \sum_j (d_j - 1) - 1; \\ \dfrac{(\sum_j (d_j - 1))!}{\prod_j (d_j - 1)!}, & \text{if} \quad s = s_{\max} + 1; \\ \infty, & \text{otherwise.} \end{cases} \tag{27}$$

3.3. Random subspaces void of states with low Schmidt rank

Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ be a bipartite Hilbert space of dimension $D = d_1 d_2$, where $\dim \mathcal{H}_j = d_j$. A pure state $|\psi\rangle \in \mathcal{H}$ is said to have *Schmidt rank* r if the $d_1 \times d_2$ matrix $M(\psi)$ with components $[M(\psi)]_{jk} = (\langle j| \otimes \langle k|)|\psi\rangle$ has rank r. This means the Schmidt decomposition of $|\psi\rangle$, defined by the singular value decomposition of $M(\psi)$, has r terms:

$$|\psi\rangle = \sum_{l=1}^{r} \sqrt{\lambda_l} |u_l\rangle \otimes |v_l\rangle, \tag{28}$$

given the singular value decomposition $[M(\psi)]_{jk} = \sum_{l=1}^{r} \sqrt{\lambda_l} \langle j|u_l\rangle \langle v_l^*|k\rangle$ (conjugation in the standard basis). All bipartite entanglement measures are functions of the Schmidt coefficients λ_l, one of which is the Schmidt rank.

Theorem 3.1 gives the maximum dimension of a subspace $\mathcal{S} \leqslant \mathcal{H}$ containing no states of Schmidt rank 1. What about subspaces void of states with Schmidt rank r or less? This scenario was studied by Cubitt, Montanaro and Winter [21]. We will now briefly mention what algebraic geometry implies.

The *determinantal variety* is defined as

$$M_r := \{x \in P(\mathbb{C}^{d_1 d_2}) : \mathrm{rank}\, M(x) \leqslant r\}, \tag{29}$$

which is the common zero locus of the $(r + 1) \times (r + 1)$ minor determinants of $M(x)$. Note that $M_1 = \Sigma_{d_1, d_2}$, the Segre variety. In general, M_r is the set of states with Schmidt rank r or less. From Harris [20, pp 151 and 243],

$$\dim M_r = d_1 d_2 - (d_1 - r)(d_2 - r) - 1, \tag{30}$$

and for $d_2 \geqslant d_1 > r$,

$$\deg M_r = \prod_{j=0}^{d_1 - r - 1} \frac{(d_2 + j)! \, j!}{(r + j)! (d_2 - r + j)!}. \tag{31}$$

The following can thus be deduced.

Corollary 3.10 (Cubitt *et al* [21])**.** *Let* $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ *be a bipartite Hilbert space with* $\dim \mathcal{H}_j = d_j$. *Then there exists a subspace* $\mathcal{S} \leqslant \mathcal{H}$ *of dimension s, completely void of states with Schmidt rank r or less, if and only if*

$$s \leqslant (d_1 - r)(d_2 - r). \tag{32}$$

Corollary 3.11. *Let* $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ *be a bipartite Hilbert space with* $\dim \mathcal{H}_j = d_j$, *where* $d_2 \geqslant d_1$. *Then for* μ_s-*almost all subspaces* $\mathcal{S} \in \mathrm{Gr}_s(\mathcal{H})$, *the number of states with Schmidt rank r or less contained in* $\mathcal{S}$ *is exactly*

$$\begin{cases} 0, & \text{if } s \leqslant s'_{\max} = (d_1 - r)(d_2 - r), \\ \prod_{j=0}^{d_1-r-1} \dfrac{(d_2 + j)!\, j!}{(r + j)!\,(d_2 - r + j)!}, & \text{if } s = s'_{\max} + 1, \\ \infty, & \text{otherwise.} \end{cases} \tag{33}$$

4. Local unambiguous state discrimination

Pure state discrimination is the task of identifying the state of a quantum system, $\psi_?$, given that it is one of a finite known set of possibilities, $\Psi = \{\psi_1, \ldots, \psi_n\}$. Measurements may be performed on the system, and its state deduced from the results. If the system is multipartite, we can restrict these measurements to local operations on each subsystem, coordinated via classical communication. This restriction is abbreviated LOCC, and is particularly important in quantum information theory, providing the context in which entanglement is a useful resource.

'Unambiguous' state discrimination is the task of obtaining *certain knowledge* of the state [28–30]. When the states in Ψ are nonorthogonal, this certainty when successful involves a commensurate risk of failure. The risk is significant: educated guesswork is correct more often than an unambiguous discrimination yields a definite answer. But guesses can be wrong, whereas unambiguous identifications are infallible. It is not obvious *a priori* that unambiguous discrimination should be possible at all. If physical states cannot be perfectly distinguished, why should we expect to separate them with *any* probability? The classical analogues of nonorthogonal quantum states are overlapping probability distributions on phase space, and these cannot be unambiguously distinguished. In this sense, unambiguous state discrimination is inherently nonclassical.

Linearly independent quantum states can always be globally unambiguously distinguished, but this is not the case locally. (For example, the Bell states can be perfectly distinguished globally, but cannot be unambiguously distinguished using LOCC.) Nevertheless, Ji, Cao and Ying [32] showed that any pair of pure states is equally unambiguously distinguishable locally and globally. Bandyopadhay and one of us [33] showed that triplets of quantum states always contain at least one locally identifiable state. Duan *et al* [26] showed that any basis of a multipartite Hilbert space, $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ where $\dim \mathcal{H}_j = d_j$, always contains some locally unambiguously distinguishable subset with $1 + \sum_j (d_j - 1)$ members. They have also presented a fascinating construction for complete bases of entangled states that are locally unambiguously distinguishable. Generalizing from these specific results is difficult, as the class of LOCC operations is mathematically complicated. We aim at the next best thing: a solution for *almost all* sets of quantum states.

Every LOCC protocol amounts to some general quantum operation applied to a multipartite Hilbert space $\mathcal{H}$. Since state discrimination is concerned only with the outcomes

of this operation, whose probabilities are described by a positive operator valued measure (POVM), unambiguous local distinguishability can be defined in the following way.

A POVM is a set of positive operators $\{E_k\}_k$ which sum to the identity: $\sum_k E_k = 1$. POVMs describe the outcome statistics of general quantum operations. The outcomes are labeled by the integer k. An *LOCC decomposable POVM* is one which describes an operation on $\mathcal{H}$ that can be implemented by local operations and classical communication.

Definition 4.1. *The n pure states $\psi_1, \ldots, \psi_n$ of the multipartite Hilbert space $\mathcal{H}$ are unambiguously locally distinguishable if and only if there exists an LOCC decomposable POVM $\{E_k\}_{k=0,\ldots,n}$ on $\mathcal{H}$ with the property that,*

$$\langle \psi_j | E_k | \psi_j \rangle = 0 \text{ if and only if } j \neq k, \tag{34}$$

whenever $k > 0$.

An outcome $k > 0$ unambiguously identifies the state ψ_k, since no other member of Ψ can produce this result. The outcome 0 identifies no state. For any LOCC protocol, every operator E_k is separable, and can be expressed as a weighted sum of projectors onto pure product states: $E_k = \sum_l w_{kl} P_{kl}$. The set of all these projectors $\{w_{kl} P_{kl}\}_{k,l}$ is a POVM describing a separable quantum measurement on $\mathcal{H}$, but not necessarily one that can be implemented using LOCC. However, for any finite set of product state projectors $\{P_l\}_l$, we can assign nonzero weights w'_l such that the POVM $\{w'_l P_l, 1 - \sum_l w'_l P_l\}_l$ *does* describe an LOCC protocol. The following condition is then a consequence, first observed by Chefles:

Condition 4.2 (Chefles [31]). *Any n pure states $\psi_1, \ldots, \psi_n$ of a multipartite Hilbert space $\mathcal{H}$ are unambiguously locally distinguishable if and only if there exist n product states $\phi_1, \ldots, \phi_n$ of $\mathcal{H}$ with the property that*

$$\langle \phi_j | \psi_k \rangle = 0 \text{ if and only if } j \neq k. \tag{35}$$

This condition addresses whether a set of states is unambiguously locally distinguishable or not. It does not indicate the probability with which this might be achieved, only whether or not this probability is nonzero. This qualitative question is all that we will consider in this section. We discuss the quantitative problem in section 5.

Clearly, for any Ψ, searching the set of all product states on $\mathcal{H}$ for states with the necessary properties is far from trivial. However, with the aid of theorem 3.4 it is simple to prove that the local unambiguous distinguishability of almost all sets of states can be judged solely by their number in relation to their multipartite structure.

Theorem 4.3. *Let $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ be a multipartite Hilbert space where $\dim \mathcal{H}_j = d_j$. Then the members of almost all sets of n pure states of $\mathcal{H}$ are locally unambiguously distinguishable, if and only if*

$$n \leqslant 1 + \sum_j (d_j - 1). \tag{36}$$

Proof. Let $\Psi = \{\psi_1, \ldots, \psi_n\} \subset P(\mathcal{H})$. Define $\Psi_1 := \Psi \backslash \{\psi_1\}$, the subset of Ψ including all members but ψ_1, and $\mathcal{S}_1 := \text{span}\{|\psi\rangle : \psi \in \Psi_1\}$, the subspace of $\mathcal{H}$ spanned by members of Ψ_1. Now let $\mathcal{S}_1^\perp$ be the complement of $\mathcal{S}_1$ in $\mathcal{H}$, i.e. $\mathcal{H} = \mathcal{S}_1 \oplus \mathcal{S}_1^\perp$, and define $\Phi_1 \subset P(\mathcal{S}_1^\perp)$ to be the set of all product states orthogonal to $\mathcal{S}_1$.

Suppose $n > 1 + \sum_j (d_j - 1)$. From theorem 3.4, $\Phi_1 = \emptyset$ for almost all choices of $\Psi \subset P(\mathcal{H})$. In such cases there is no product state ϕ_1 with $\langle \phi_1 | \psi_k \rangle = 0$ for all $k \neq 1$. Thus Ψ cannot satisfy condition 4.2 and is therefore not locally unambiguously distinguishable.

Now suppose $n \leqslant 1 + \sum_j (d_j - 1)$. From theorem 3.1, $\Phi_1 \neq \emptyset$ for all choices of Ψ. Now since ψ_1 was chosen at random, independently from the members of Ψ_1, and therefore independently from the members of Φ_1, for any product state $\phi_1 \in \Phi_1$ we almost surely have $\langle \phi_1 | \psi_1 \rangle \neq 0$, and moreover, $\langle \phi_1 | \psi_k \rangle = 0$ if and only if $k \neq 1$. By symmetry, similar product states can be found for all members of Ψ, which means condition 4.2 is satisfied. The members of Ψ are therefore almost surely locally unambiguously distinguishable. $\square$

4.1. General versus product pure states

The members of Ψ, since they are chosen at random, will be highly entangled in large dimensions. It is interesting to compare this situation with a more restricted case: sets of randomly chosen *product* states. We define a random product state as follows. For a given Hilbert space $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ with $\dim \mathcal{H}_j = d_j$, a random product state ϕ of $\mathcal{H}$ is a tensor product state $|\phi\rangle = \bigotimes_j |\phi_j\rangle$ where each state ϕ_j is an independently chosen random pure state of $\mathcal{H}_j$.

It has been known for some time that almost all sets of n random product states form a (nonorthogonal) unextendible product basis if and only if $n \geqslant 1 + \sum_j (d_j - 1)$ (see, e.g., DiVincenzo *et al* [34]). An unextendible product basis is a set of product states with a span whose complementary subspace contains no product states. The following is then an immediate consequence of Chefles' condition.

Theorem 4.4. *Let $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ be a multipartite Hilbert space where $\dim \mathcal{H}_j = d_j$. Then the members of almost all sets of n product pure states of $\mathcal{H}$ are locally unambiguously distinguishable, if and only if*

$$n \leqslant 1 + \sum_j (d_j - 1). \tag{37}$$

Comparing this criterion with that for random general pure states we see something striking: they are identical. Random general pure states are near-maximally entangled; one might reasonably expect that this makes them harder to distinguish using LOCC. At least in respect of unambiguous distinguishability, this is not the case.

4.2. Multiple separated copies

There may be more than one copy of the system whose state we are trying to identify. Suppose there are c identical copies of an unknown state $\psi_? \in \Psi$. The larger c gets, the easier distinguishing members of Ψ becomes.

The LOCC constraint prohibits joint quantum operations between parties but not between copies, so a party with access to multiple copies of the same subsystem could measure them all jointly. It is interesting to impose an additional constraint on the parties, however, and insist that separate operations be performed on every subsystem from every copy—subsystems from different copies may not be measured jointly. The copies are then called *separated copies*. Equivalently, we extend the scenario of one copy shared between m parties to that of c copies shared between cm parties, all communicating freely.

This constraint is natural from a practical perspective, especially in a laboratory context. Copies of a system might be generated and studied at different times. Even if not, whatever technical restriction forbids joint measurements within a copy could similarly restrict measurements between copies. A relevant example is quantum state tomography, which is almost exclusively performed on many copies of a system using completely separable measurements [35, 36].

Theorem 4.5. *Let* $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ *be a multipartite Hilbert space with* $\dim \mathcal{H}_j = d_j$, *and let* c *be any positive integer. Then the members of almost all sets of n pure states of* $\mathcal{H}$ *are locally unambiguously distinguishable, given c separated copies of the unknown member, if and only if*

$$n \leqslant 1 + c \sum_j (d_j - 1). \tag{38}$$

Proof. Simply consider $\mathcal{H}^{\otimes c} = \left(\bigotimes_{j=1}^m \mathcal{H}_j \right)^{\otimes c}$ as the Hilbert space of cm separate parties. The proof is then exactly the same as that for theorem 4.3, except theorem 3.4 needs to be replaced by corollary 3.6. $\qquad\square$

How good are separable measurements at producing unambiguous data? We have seen that above a low threshold size, the members of almost all sets Ψ are locally unambiguously indistinguishable. With sufficiently many copies, however, the members of any finitely large Ψ can be unambiguously distinguished. The minimum number of copies this requires gives a measure of *how* indistinguishable Ψ is. Contrasting the minima for separable and global measurements shows how poor the former are at obtaining that 'quintessentially quantum' unambiguous data. As the dimension of the measured system increases, separable measurements consume exponentially more copies.

Corollary 4.6. *Let* $\mathcal{H} = \bigotimes_j \mathcal{H}_j$ *be a multipartite Hilbert space with* $\dim \mathcal{H}_j = d_j$. *Then for almost all sets of n pure states of* $\mathcal{H}$,

$$c \geqslant \frac{n-1}{\sum_j (d_j - 1)} \tag{39}$$

identical copies are required to locally unambiguously identify an unknown member, if these copies are separated.

What does this imply about the feasibility of unambiguous discrimination on higher dimensional multipartite systems? Suppose we grow the number of subsystems, m. For any fixed number of copies, the number of random states that can be unambiguously distinguished globally grows exponentially with m. But far from being fixed, the number of copies required to emulate these global measurements *separably* also grows exponentially. A linearly independent set of m-qubit states, for example, has up to 2^m members. To unambiguously distinguish this many states using single qubit measurements requires $\left\lceil \frac{2^m - 1}{m} \right\rceil$ copies of the system. Globally, one is always enough!

Of course with many copies of a quantum system, a great deal can be learned about its state without using unambiguous protocols. As measurement results accumulate, analysis of Ψ will reveal most states becoming increasingly unlikely and a select few candidates becoming highly probable. What will remain elusive is certainty. In theory (if admittedly not in practice) absolute certainty is obtainable by global measurements, and exponentially harder to reach with separable operations.

5. Discussion

Almost all subspaces of multipartite Hilbert spaces are completely entangled, provided they are small enough. We have precisely quantified 'small enough', and it is very large (18). For any m-qubit system, almost all subspaces of dimension $2^m - m - 1$ or less are completely

entangled. Random and entangled subspaces are useful in a number of contexts, and we hope our result will find application elsewhere. It should certainly make them easier to find! One application we have pursued ourselves, obtaining a simple rule governing the local unambiguous distinguishability of almost all sets of quantum states.

We have only discussed pure states, but our results have implications for random mixed states as well. Hayden *et al* [7] showed that general mixed states of rank equal to the span of a 'maximally entangled' random subspace, have near maximal entanglement of formation but near zero distillable entanglement, making them nearly bound entangled. Cubitt *et al* [21] observe their constructions can be used to create similar mixed states of much greater rank with high Schmidt measure. Our results suggest this property of mixed states is generic.

Of the many questions left open, the most obvious concerns quantification. Precisely *how* entangled are the states in a completely entangled random subspace? The Schmidt rank provides one measure in bipartite situations. What of other measures, such as the entanglement of formation, or of distillation? Whereas the maximally entangled subspaces of Hayden *et al* contain only states with high entropy of entanglement, our much larger subspaces sacrifice this property as they grow. The largest completely entangled subspaces contain states that are only slightly entangled. Thanks to corollary 3.11, we can chart the stepwise descent of random subspaces' Schmidt rank as their dimension increases. It would be interesting to see how other entanglement measures behaved.

Distinguishability can be quantified as well. If a set of random states can be locally unambiguously discriminated, with what probability of success? If not, how many copies would provide a better than even odds chance? Unfortunately, we still do not have good bounds on the probability with which *global* unambiguous discrimination can be performed on random states, so answers to these local questions remain out of reach. Good progress has been made on the optimal global distinguishability of random states [8], however; so both the unambiguous global problem and the optimal local problems are tantalizing.

We can make one locally unambiguous observation, however. If the members of a set of pure states can be locally unambiguously discriminated with nonzero probability, then they can certainly be locally unambiguously discriminated with some finite, nonnegligible probability. The probability overlap of a random state ψ_i with some arbitrary product state that identifies it, ϕ_i, will have mean $\overline{|\langle\phi_i|\psi_i\rangle|^2} = 1/D$, where D is the dimension of the overall system. (To see this, consider writing the random state in an independently fixed product basis.) As D becomes large, concentration of measure effects transform this average into a very reliable estimate. Thus selecting an arbitrary set of product states, $\{\phi_i\}$, satisfying Chefles' condition 4.2, we can build an LOCC protocol around them that stands a finite chance of success: $\{w_i|\phi_i\rangle\langle\phi_i|, 1 - \sum_i w_i|\phi_i\rangle\langle\phi_i|\}_i$. The weights w_i must be considered because the measurement must be LOCC implementable, but these can be quite large. For instance if for all i, $w_i = \frac{1}{n}$, the POVM is automatically LOCC decomposable irrespective of $\{\phi_i\}$. Such a protocol simply guesses the state's identity in advance, then performs binary local measurements to confirm or refute this hypothesis. This yields a success probability of about $\frac{1}{Dn}$. There will be much better choices of measurement, of course, but even arbitrary successful protocols succeed a noticeable fraction of the time.

If n random product pure states are locally unambiguously distinguishable then so are n random general pure states, and vice versa. Entanglement does not matter for determining whether or not the states are distinguishable, but perhaps the two sets can be distinguished with different probabilities of success. If the probability for general states were lower, we might recover some of our intuition about entanglement. We cannot judge this question now, but observe that *arbitrary* successful protocols show no sign of favoring separable states. This is not conclusive evidence one way or the other, but it reinforces that there is no evidence

for random highly entangled states being harder to locally unambiguously distinguish than random product states.

Acknowledgments

References

[1] Horodecki M 2001 *Quantum Inf. Comput.* **1** 3
[2] Vedral V, Plenio M B, Rippin M A and Knight P L 1997 *Phys. Rev. Lett.* **78** 2275
[3] Christandl M 2006 *PhD Thesis* University of Cambridge
[4] Ledoux M 2001 The concentration of Measure Phenomenon (Providence, RI: American Mathematical Society)
[5] Wootters W K 1990 *Found. Phys.* **20** 1365
[6] Życzkowski K and Sommers H 2005 *Phys. Rev.* A **71** 032313
[7] Hayden P, Leung D and Winter A 2006 *Comm. Math. Phys.* **265** 95117
[8] Montanaro A 2007 *Commun. Math. Phys.* **273** 619
[9] Scott A J 2004 *Phys. Rev.* A **69** 052330
[10] Gour G and Wallach N R 2007 *Phys. Rev.* A **76** 042309
[11] Abeyesinghe A, Hayden P, Smith G and Winter A 2006 *IEEE Trans. Inform. Theory* **52** 3635
[12] Bartlett S D, Hayden P and Spekkens R W 2005 *Phys. Rev.* A **72** 052329
[13] Wallach N R 2002 *Contemp. Math.* **305** 291
[14] Parthasarathy K R 2004 *Proc. Indian Acad. Sci.* **114** 365
[15] Abraham R and Robbin J 1967 *Transversal Mappings and Flows* (New York: Benjamin)
[16] Abraham R, Marsden J E and Ratiu T 1983 *Manifolds, Tensor Analysis, and Applications* (New York: Springer)
[17] Hirsch M W 1976 *Differential Topology* (New York: Springer)
[18] Chow S-N, Mallet-Paret J and Yorke J A 1978 *Math. Comp.* **32** 887
[19] Keerthi S S, Sancheti N K and Dattasharma A 1992 *Proc. of the 31st IEEE Conf. on Decision and Control (Tucson, AZ, Dec. 1992)* p 96
[20] Harris J 1992 *Algebraic Geometry: A First Course* (New York: Springer)
[21] Cubitt T S, Montanaro A and Winter A 2008 *J. Math. Phys.* **49** 022107
[22] Walgate J, Short A J, Hardy L and Vedral V 2000 *Phys. Rev. Lett.* **85** 4972
[23] Virmani S, Sacchi M F, Plenio M B and Markham D 2001 *Phys. Lett.* A **288** 62
[24] Ghosh S, Kar G, Roy A, Sen(De) A and Sen U 2001 *Phys. Rev. Lett.* **87** 277902
[25] Xin Y and Duan R 2008 *Phys. Rev.* A **77** 012315
[26] Duan R, Feng Y, Ji Z and Ying M 2007 *Phys. Rev. Lett.* **98** 230502
[27] Halmos P R 1974 *Measure Theory* (New York: Springer)
[28] Ivanović I D 1987 *Phys. Lett.* A **123** 257
[29] Dieks D 1988 *Phys. Lett.* A **126** 303
[30] Peres A 1988 *Phys. Lett.* A **128** 19
[31] Chefles A 2004 *Phys. Rev.* A **69** 050307
[32] Ji Z, Cao H and Ying M 2005 *Phys. Rev.* A **71** 032323
[33] Bandyopadhyay S and Walgate J 2006 *Preprint* quant-ph/0612013
[34] DiVincenzo D P, Mor T, Shor P W, Smolin J A and Terhal B M 2003 *Comm. Math. Phys.* **238** 379
[35] James D F V, Kwiat P G, Munro W J and White A G 2001 *Phys. Rev.* A **64** 052312
[36] Rehacek J, Hradil Z and Jezek M 2001 *Phys. Rev.* A **63** 040303