IS A RANDOM STATE ENTANGLED ?

G. AUBRUN

Institut Camille Jordan, Université Claude Bernard Lyon 1
43 boulevard du 11 novembre 1918, 69622 Villeurbanne cedex, France
E-mail: aubrun@math.univ-lyon1.fr

For a random quantum state on $\mathcal{H} = \mathbf{C}^d \otimes \mathbf{C}^d$ obtained by partial tracing a random pure state on $\mathcal{H} \otimes \mathbf{C}^s$, we consider the question whether it is typically separable or typically entangled. We show the existence of a sharp threshold $s_0 = s_0(d)$ of order roughly d^3. More precisely, for any $\varepsilon > 0$ and for d large enough, such a random state is entangled with very large probability when $s \leqslant (1-\varepsilon)s_0$, and separable with very large probability when $s \geqslant (1+\varepsilon)s_0$.

Keywords: Random states, entanglement

1. Random states

If all that we know about a quantum system is its dimension n (the number of levels) and that it is well isolated from the environment, a reasonable model for the state of the system—or at least a reasonable first guess—is a unit vector selected at random from the sphere of an n-dimensional complex Hilbert space $\mathcal{H}$. If the system interacts with some part of the environment, represented by an ancilla space $\mathcal{H}_a$, the quantum formalism suggests as a model the so-called (random) *induced state*, obtained after partial tracing, over $\mathcal{H}_a$, a random pure state on the space $\mathcal{H} \otimes \mathcal{H}_a$. The same description applies if we are primarily interested in a *subsystem* of an isolated system.

The above is just one example of how a random paradigm arises naturally in the quantum context. Another important aspect is that the objects studied in quantum information theory usually live in very large dimensions. For example, the quantum state of 8 qubits (a "qubyte") is described by a operator on $(\mathbf{C}^2)^{\otimes 8}$, leading to $2^{16}-1$ degrees of freedom. As opposed to numerical methods, which face the curse of dimensionality, probabilistic considerations are usually boosted by large dimensions and enjoy the blessing of dimensionality.

The use of high-dimensional random states has become a very fruitful approach in quantum information theory [1]. A highlight was Hastings's proof [2] that suitably chosen random channels provide a counterexample to the additivity conjecture for the classical capacity of quantum channels.

Although random states have been considered for many years, their properties remained elusive. In this article, we answer in a very precise way the most fundamental question one may ask about a random state: is it entangled ? Understanding how prevalent is entanglement is certainly of importance. We note that detecting and exploiting entanglement—originally discovered in the 1930's [3]—is a central problem in quantum information and quantum computation at least since Shor's work [4] on integer factoring.

For simplicity, we focus on the study of entanglement in bipartite balanced systems. We assume that a random state is shared between two parties (Alice and Bob), which play a symmetric role. Mathematically, we are going to consider states on $\mathcal{H} = \mathbf{C}^d \otimes \mathbf{C}^d$, with $d \geqslant 2$.

Let us first comment on the (trivial) case where Alice and Bob share a random pure state, described by a uniformly distributed unit vector $|\psi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d$. Such a pure state is separable if and only if $|\psi\rangle$ factorizes as $|\psi_A\rangle \otimes |\psi_B\rangle$. This happens with proability zero: the set of product vectors is a manifold of lower dimension (the Segré maniford) inside the projective space. Henceforth, random pure states are almost surely entangled.

The situation becomes interesting when we consider random mixed states. The "open system" paradigm mentioned earlier suggests to incorporate the influence of the environment. We assume that the state shared by Alice and Bob is the partial trace (over the environment $\mathcal{H}_a = \mathbf{C}^s$) of a pure state $|\phi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d \otimes \mathbf{C}^s$. When $|\phi\rangle$ is uniformly distributed on the unit sphere, we say that the reduced state $\rho = \mathrm{tr}_{\mathbf{C}^s} |\phi\rangle\langle\phi|$ is a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$, induced by $\mathbf{C}^s$. The distribution of such random induced states enjoys nice properties [5]: for $s \geqslant d^2$, it has a density with respect to the Lebesgue measure which is proportional to $(\det \rho)^{s-d^2}$. In particular, for $s = d^2$, random induced states are uniformly distributed on the set of states.

Other models of random mixed states have been proposed. For example, given s indepedent Haar distributed pure states $\{|\psi_i\rangle\}$ on $\mathbf{C}^d \otimes \mathbf{C}^d$, one may consider their uniform mixture

$$\rho = \frac{1}{s} \sum_{i=1}^{s} |\psi_i\rangle\langle\psi_i|. \tag{1}$$

This models shares many properties with random induced states, and all results stated here are true for both models, where s is understood either has the dimension of the environment, or the number of terms in the mixture.

In the limit case when d is fixed and s tends to ∞, the random states concentrate towards the maximally mixed state $\rho_* = \mathbb{I}/d^2$. This can be seen from the density, since the maximally mixed state is the unique state with maximal determinant. This is mathematically a manifestation of the law of large numbers, and physically can be related to decoherence. Since ρ_* lies in the interior of the set of separable states, it follows that, with d fixed and $s \to \infty$, the probability that induced states are separable tends to 1.

From the two extreme cases $s = 1$ (pure states) and $s = \infty$, we may infer that induced states are more likely to be separable when the environment has larger dimension. As it turns out, a phase transition takes place (at least when d is sufficiently large): the generic behavior of ρ "flips" to the opposite one when s changes from being a little smaller than certain threshold dimension s_0 to being larger than s_0. We now state our main theorem in this direction.

Theorem 1.1. *There exists a function $s_0(d)$ satisfying*

$$d^3 \lesssim s_0(d) \lesssim d^3 \log^2 d \tag{2}$$

such that, if ρ is a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ induced by $\mathbf{C}^s$, for any $\varepsilon > 0$,

(1) if $s \leqslant (1-\varepsilon)s_0(d)$, we have

$$\mathbf{P}(\rho \text{ is entangled}) \geqslant 1 - 2\exp(-c(\varepsilon)d^3),$$

(2) is $s \geqslant (1+\varepsilon)s_0(d)$, we have

$$\mathbf{P}(\rho \text{ is separable}) \geqslant 1 - 2\exp(-c(\varepsilon)s),$$

where $c(\varepsilon)$ is a constant depending only on ε.

Here and it what follows, the notation $a \lesssim b$ means that there exists a numeric constant C such that $a \leqslant Cb$. The value of this constant is not specified, although it could be retrieved from the proofs. Note that the theorem is meaningful only for large enough d.

Theorem 1.1 was proved in Ref. 6, and a non-technical high-level overview of the proof can be found in Ref. 7. The sequel of this article is organized as follows: in Sec. 2 we reformulate the main theorem, measuring local dimensions by numbers of qubits. In Sec. 3, we compare with related results. Section 4 presents basic concepts from convex geometry on which we rely. In Sec. 5, we sketch a proof of the "easy" half of the theorem, and Sec. 6 covers the complete proof.

2. Threshold on the number of shared qubits

Here is a more appealing reformulation of the main theorem. Suppose Alice and Bob are given a quantum state, prepared in the following way. We start with a system of N qubits, which is in a global pure state. This state is described by a unit vector in $(\mathbf{C}^2)^{\otimes N}$, and we assume that this unit vector is chosen at random, with respect to the uniform measure on the 2^N-dimensional sphere. Give k of these qubits to Alice, k other qubits to Bob, and forget about the remaning $N-2k$ qubits (by taking the partial trace over the corresponding subsystem). Do Alice and Bob typically share entanglement ? In this formulation, the answer also exhibits a threshold property: there is a critical value $k_0(N)$, equivalent to $N/5$ as N tends to infinity, such that

(1) If $k > k_0(N)$, then with overwhelming probability Alice and Bob do share some entanglement.
(2) If $k < k_0(N)$, then with overwhelming probability Alice and Bob do not share any entanglement.

What we mean by "overwhelming probability" is that the probability of failure tends to 0 exponentially fast (as N tends to ∞).

3. Related works

Let ρ be a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ induced by $\mathbf{C}^s$. The following is an immediate consequence of Theorem 1.1.

(i) If $s \leqslant cd^3$, then ρ is typically entangled, while if $s \geqslant d^3\text{polylog } d$, ρ is typically separable.

Instead of the qualitative "entanglement vs. separability" dichotomy, we could ask for a quantitative version of the problem: how much is a random state entangled ? A popular way to quantify entanglement is the *entanglement of formation*, defined for a pure state $|\psi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d$ as $E_f(|\psi\rangle\langle\psi|) := -\sum \lambda_i \log \lambda_i$, where λ_i are the Schmidt coefficients of ψ, and extended to mixed states ρ by the convex roof construction

$$E_f(\rho) = \min \left\{ \sum \lambda_k E_f(|\psi_k\rangle\langle\psi_k|) \ : \ \rho = \sum \lambda_k |\psi_k\rangle\langle\psi_k| \right\}.$$

The following result was proved by Hayden–Leung–Winter [1].

(ii) If $s \leqslant d^2/\text{polylog } d$, then the entanglement of formation of ρ is typically close to maximal, while if $s \geqslant d^2\text{polylog } d$, the entanglement of formation of ρ is typically close to minimal.

A useful test to detect entanglement is the Peres criterion [8], which involves the partial transposition ρ^Γ of a state ρ. A state which is separable must be PPT (Positive Partial Transpose, i.e. with $\rho^\Gamma \geqslant 0$), and the converse is false except in very low dimensions. A natural question is when random states are PPT. In that case, the value of the threshold is known [9] to be precisely equal to $4d^2$.

(iii) If $s < 4d^2$, then ρ id typically non-PPT, while if $s > 4d^2$, then ρ is typically PPT.

Comparing these results yields new insights on the behaviour of entanglement in large-dimensional systems. A particularly interesting case is when $s = d^\alpha$ with $2 < \alpha < 3$. By (i), in this range, random states are entangled. However, by (ii), their entanglement of formation is close to minimal ! Moreover, by (iii), these states are non-PPT. Such states are called "bound entangled" and cannot be distilled [10], i.e. local operations cannot transform them into entangled qubits, making them useless for purposes such as teleportation or superdense coding [11]. Our results show that bound entangled states are not an anomaly: they are, in some sense, generic.

Another efficient criterion which parallels the Peres criterion is the realignment criterion, also called computable cross-norm criterion [12, 13]. The realignment ρ^R of a state ρ is obtained by applying a permutation to the indices of ρ. It has the following property: a separable state ρ satisfies the inequality $\|\rho^R\|_1 \leqslant 1$. This yields to a criterion to detect entanglement which is known to be neither stronger nor weaker than the Peres criterion. We can prove [14] that the threshold for that criterion equals $(\frac{8}{3\pi})^2 d^2$

(iv) If $s < (\frac{8}{3\pi})^2 d^2$, then typically $\|\rho^R\|_1 > 1$, while if $s > (\frac{8}{3\pi})^2 d^2$, then typically $\|\rho^R\|_1 \leqslant 1$.

Note that $(\frac{8}{3\pi})^2 \approx 0.72$. By comparing (iii) and (iv), we learn than in an asymptotic sense, the realignment criterion is weaker than the Peres criterion: for $s = \beta d^2$ with $(\frac{8}{3\pi})^2 < \beta < 4$, then typically the Peres criterion detects entanglement while the realignment criterion does not. This range includes the case $\beta = 1$ ($s = d^2$), which corresponds to the Lebesgue measure.

4. Background from convex geometry

In this section, we introduce basic concepts associated to a convex body $K \subset \mathbf{R}^N$ containing the origin in the interior. The *gauge* of K is the function $\|\cdot\|_K$ defined for $x \in \mathbf{R}^N$ by

$$\|x\|_K = \inf\{t \geqslant 0 \ : \ x \in tK\}.$$

The *polar* (or dual) body of K is defined as

$$K^\circ = \{y \in \mathbf{R}^N \ : \ \langle x, y\rangle \leqslant 1 \ \ \forall x \in K\}.$$

The bipolar theorem states that $(K^\circ)^\circ = K$. If $u \in \mathbf{R}^N$, the *support function* of K in the direction u is $h_K(u) := \max_{x\in K} \langle x, u\rangle = \|u\|_{K^\circ}$. Note that when u is a unit vector, $h_K(u) + h_K(-u)$ is the distance between the two hyperplanes tangent to K and normal to u. The mean width of K is then defined as

$$w(K) := \int_{S^{N-1}} h_K(u)\, d\sigma(u) = \int_{S^{N-1}} \|u\|_{K^\circ} d\sigma(u),$$

where $d\sigma$ is the normalized spherical measure on the unit sphere S^{N-1}.

In our setting, $K = \mathcal{S}$ is the set of separable states on $\mathbf{C}^d \otimes \mathbf{C}^d$, and the ambient space $\mathbf{R}^N$ is the space of self-adjoint trace 1 operators on $\mathcal{H}$ (hence $N = d^4 - 1$), where the maximally mixed state plays the role of the origin. The Euclidean structure is induced by the Hilbert–Schmidt inner product, and the support function of $\mathcal{S}$ is given, for a self-adjoint traceless operator W, by

$$h_{\mathcal{S}}(W) = \max_{\sigma\in\mathcal{S}} \operatorname{tr}(W\sigma) = \max_{|x\rangle,|y\rangle\in\mathbf{C}^d} \langle x\otimes y|W|x\otimes y\rangle.$$

By the Hahn–Banach separation theorem, a state ρ is entangled if and only if there exists an entanglement witness, i.e. a self-adjoint traceless operator W such that

$$h_{\mathcal{S}}(W) < \operatorname{tr}(W\rho). \tag{3}$$

As we will see, the mean width of $\mathcal{S}$ and the mean width of $\mathcal{S}^\circ$ play a central role in our arguments.

5. A single witness is enough

In this section we sketch an elementary proof of the "easy" part of the main theorem: if $s \lesssim d^3$ and ρ is a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ induced by $\mathbf{C}^s$, then with large probability, ρ is entangled. It is known [15] that the problem of deciding whether a state is entangled is algorithmically hard, and we have to seek the entanglement witness among a huge group of candidates. We are going to bypass this issue by *testing only a single witness*. This idea looks naive from a low-dimension perspective, but becomes reasonable when dimension gets higher.

The most naive choice for a witness is $W_0 := \rho - \mathbb{I}/d^2$. Geometrically, this amounts to checking whether some hyperplane orthogonal to the segment joining ρ to the maximally mixed state separates ρ from $\mathcal{S}$. The following lemma estimates the support function of $\mathcal{S}$ in the (random) direction W_0.

Lemma 5.1. *If $s \geqslant d^2$, then with large probability,*

$$h_{\mathcal{S}}(W_0) \lesssim \frac{1}{d^{3/2} s^{1/2}}$$

For $W = W_0$, the right-hand side of Eq. (3) can be estimated easily: $\operatorname{tr}(W_0 \rho)$ is the square of the Hilbert–Schmidt distance between ρ and the maximally mixed state, and is of order $1/s$. Together with Lemma 5.1, this implies whenever $s \lesssim d^3$, Eq. (3) is satisfied and therefore ρ is entangled.

Proof of Lemma 5.1. We proceed via an elementary discretization argument. Consider an ε-net $\mathcal{N}$ inside the unit sphere of $\mathbf{C}^d$. Denote also $\mathcal{N} \otimes \mathcal{N}$ the set of tensor products of two elements from $\mathcal{N}$. If ε is small enough (e.g. $\varepsilon = 1/24$), we obtain [16]

$$h_{\mathcal{S}}(W_0) \leqslant 2 \max_{\psi \in \mathcal{N} \otimes \mathcal{N}} |\langle \psi | W_0 | \psi \rangle|.$$

For fixed ε, it is well-known (e.g. Lemma 4.10 in Ref. 17) that one can choose $\mathcal{N}$ with exponentially many points, i.e. $\operatorname{card}(\mathcal{N} \otimes \mathcal{N}) \leqslant \operatorname{card}(\mathcal{N})^2 \leqslant C_0^d$ for some constant C_0. We now use an union bound argument. For a fixed unit vector $|\psi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d$, the deviations of the random variable $|\langle \psi | W_0 | \psi \rangle|$ can be estimated by Lévy's lemma (see e.g. Ref. 6). Indeed, recall that ρ was obtained as $\operatorname{tr}_{\mathbf{C}^s} |\phi\rangle\langle\phi|$, where $|\phi\rangle$ is a vector uniformly distributed on the unit sphere in $\mathbf{C}^d \otimes \mathbf{C}^d \otimes \mathbf{C}^s$. Using the fact that the function $|\phi\rangle \mapsto \langle \psi | \operatorname{tr}_{\mathbf{C}^s} |\phi\rangle\langle\phi| | \psi \rangle^{1/2}$ is 1-Lipshitz on the unit sphere, we obtain the following bound for any $0 < \eta < 1$ (here C and c denote numerical constants)

$$\mathbf{P}\left(|\langle \psi | W_0 | \psi \rangle| > \frac{\eta}{d^2} \right) \leqslant C \exp(-cs\eta^2). \tag{4}$$

By the union bound, we obtain

$$\mathbf{P}\left(h_{\mathcal{S}}(W_0) > \frac{2\eta}{d^2} \right) \leqslant \operatorname{card}(\mathcal{N} \otimes \mathcal{N}) C \exp(-cs\eta^2) \leqslant C C_0^d \exp(-cs\eta^2).$$

This estimate is much smaller than 1 whenever η is proportional to $\sqrt{d/s}$. It follows that, with high probability, $h_{\mathcal{S}}(W_0)$ is bounded by a multiple of $1/\sqrt{d^3 s}$. □

The proof of Lemma 5.1 depends crucially on the subgaussian behaviour in the upper bound in Eq. (4). Other models of random states which satisfy the same behaviour will enjoy the same conclusion. This includes the uniform mixtures of independent pure states considered in Eq. (1) (the analogue of Eq. (4) appears as Lemma II.3 in Ref. 18). This also includes the uniform measure on the Hilbert–Schmidt sphere centered around the maximally mixed state. In that case, the argument yields an upper bound on the mean width of the convex body $\mathcal{S}$, which reads as

$$w(\mathcal{S}) \lesssim \frac{1}{d^{3/2}}. \tag{5}$$

This upper bound is known to be sharp [16].

6. Gaussian approximation and the MM^*-estimate

The previous section presented an elementary argument for the easy part of Theorem 1.1. However, the fact that random states are separable beyond the threshold require more sophisticated ideas which we now sketch.

Let ρ be a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ induced by $\mathbf{C}^s$. The separability of ρ is equivalent to $\|\rho\|_{\mathcal{S}} \leqslant 1$, or (since $(\mathcal{S}^\circ)^\circ = \mathcal{S}$) to $h_{\mathcal{S}^\circ}(\rho) \leqslant 1$ — a problem about the width of $\mathcal{S}^\circ$. To compute the expected value of $\|\rho\|_{\mathcal{S}}$, we are going to approximate ρ by a simpler probabilistic model, using a quantitative version of a central limit theorem for random induced states. The Gaussian approximation suggests that a random state ρ on $\mathbf{C}^d \otimes \mathbf{C}^d$, induced by $\mathbf{C}^s$, should be compared to

$$\rho \approx \frac{\mathbb{I}}{d^2} + \frac{1}{d^2\sqrt{s}} G,$$

where G is a GUE random matrix conditioned to have trace zero. We prove that, in the regime when d and s/d^2 tend to infinity, this approximation is valid and allows to compute the expected value of $\|\rho\|_{\mathcal{S}}$ using Gaussian matrices. Once this is known, the threshold function appearing in Theorem 1.1 is naturally defined as

$$s_0(d) = w(\mathcal{S}^\circ)^2.$$

and assertions (i) and (ii) in Theorem 1.1 can be derived using concentration of measure.

The heart of the proof is showing Eq. (2), especially the upper bound. Determining the threshold $s_0(d)$ requires finding the typical value of the gauge associated to $\mathcal{S}$, computing which—as we mentioned—is a hard problem. We take an indirect route and find the order of magnitude of the threshold using the machinery of high-dimensional geometry, in particular the so-called MM^*-estimate.

The MM^*-estimate [17, 19] is a general theorem which relates the mean width of a convex body and the mean width of its polar. While the abstract formulation may require an affine change of coordinates, in the present situation, because of the symmetries of $\mathcal{S}$ (invariance under local unitary conjugations), we can deduce via simple representation theory the inequalities

$$1 \leqslant w(\mathcal{S})w(\mathcal{S}^\circ) \lesssim \log d. \quad (6)$$

The left inequality is obvious and corresponds to what we did in the previous section: detecting entanglement using a single witness. The MM^*-estimate guarantees that this trivial lower bound is sharp, up to logarithmic factors. Once Eq. (6) is obtained, the rest of the proof follows: the mean width $w(\mathcal{S})$ was computed in the previous section (see Eq. (5)), and the inequalities (6) then allow to establish the order of magnitude of $w(\mathcal{S}^\circ)$ (and hence of $s_0(d)$) up to polylog factors. Whether these logarithmic factors can be removed is an interesting open problem.

Acknowledgement

Our research was supported in part by the *Agence Nationale de la Recherche* grants ANR-08-BLAN-0311-03 and ANR 2011-BS01-008-02.

References

[1] P. Hayden, D. W. Leung and A. Winter, *Comm. Math. Phys.* **265**, 95 (2006).
[2] M. Hastings, *Nature Physics* **5**, 255 (2009).
[3] A. Einstein, B. Podolsky and N. Rosen, *Physical review* **47**, p. 777 (1935).
[4] P. Shor, *SIAM Journal on Computing* **26**, p. 1484 (1997).
[5] K. Zyczkowski and H. Sommers, *Journal of Physics A: Mathematical and General* **34**, p. 7111 (2001).
[6] G. Aubrun, S. Szarek and D. Ye, *Arxiv preprint arXiv:1106.2264* (2011).
[7] G. Aubrun, S. J. Szarek and D. Ye, *Phys. Rev. A* **85**, p. 030302(Mar 2012).
[8] A. Peres, *Physical Review Letters* **77**, 1413 (1996).
[9] G. Aubrun, *Random Matrices: Theory and Applications* **1**, p. 1250001 (2012).
[10] M. Horodecki, P. Horodecki and R. Horodecki, *Physical Review Letters* **80**, 5239 (1998).
[11] P. Shor, J. Smolin and B. Terhal, *Physical Review Letters* **86**, 2681 (2001).
[12] K. Chen and L. Wu, *Quantum Information & Computation* **3**, 193 (2003).
[13] O. Rudolph, *Quantum Information Processing* **4**, 219 (2005).
[14] G. Aubrun and I. Nechita, *Arxiv preprint arXiv:1203.3974* (2012).
[15] L. Gurvits, Classical deterministic complexity of Edmond's problem and quantum entanglement, in *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, (ACM, New York, 2003).
[16] G. Aubrun and S. Szarek, *Physical Review A* **73**, p. 022109 (2006).
[17] G. Pisier, *The volume of convex bodies and Banach space geometry*, Cambridge Tracts in Mathematics, Vol. 94 (Cambridge University Press, Cambridge, 1989).
[18] P. Hayden, D. Leung, P. Shor and A. Winter, *Communications in Mathematical Physics* **250**, 371 (2004).
[19] T. Figiel and N. Tomczak-Jaegermann, *Israel J. Math.* **33**, 155 (1979).