One-dimensional steering from keychain models

Carl A. Miller
National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899, USA and
Joint Center for Quantum Information and Computer Science,
University of Maryland, College Park, MD 20742, USA[*]

Roger Colbeck
Department of Mathematics, University of York, York, YO10 5DD, UK[†]

Yaoyun Shi
Department of Electrical Engineering and Computer Science,
University of Michigan, Ann Arbor, MI, 48109, USA[‡]

(Dated: May 31, 2017)

If a measurement is made on one half of a bipartite system then, conditioned on the outcome, the other half achieves a new reduced state. If these reduced states defy classical explanation — that is, if shared randomness cannot produce these reduced states for all possible measurements — the bipartite state is said to be *steerable.* Classifying the steerability of states is a challenging problem even for low dimensions. In the case of two-qubit systems a criterion is known for T-states (that is, 2-qubit states that have a maximally mixed marginal on the first subsystem) under projective measurements. In the current work we introduce the concept of *keychain models* — a special class of local hidden state models — which allows us to study steerability outside the set of T-states. We use keychain models to give a complete classification steering within the set of partially entangled Werner states. We also give a partial classification of steering for states that arise from applying uniform noise to pure two-qubit states.

I. INTRODUCTION

In his 1964 paper [1] John Bell made the fundamental observation that measurement correlations exhibited by some entangled quantum states cannot be explained by any local causal model. Specifically, if ρ_{AB} is the state of a bipartite system shared by Alice and Bob, and Alice is given a private message $x \in \mathcal{X}$ and Bob is given a private message $y \in \mathcal{Y}$, then it is possible for Alice and Bob to measure ρ_{AB} and produce output messages $a \in \mathcal{A}$ and $b \in \mathcal{B}$ such that the conditional probability distribution $\mathbf{P}(ab \mid xy)$ cannot be simulated by any local hidden variable (LHV) model.

This can be interpreted as a fundamental confirmation of the models for nonlocality used in quantum physics, and it also has important applications in information processing. Device-independent quantum cryptography is based on the observation that if two untrusted input-output devices exhibit nonlocal correlations, their internal processes must be quantum. With correctly chosen protocols and mathematical proof, this observation allows a classical user to manipulate the devices to perform basic cryptographic tasks and at the same time verify their security [2].

In 2007, the related notion of quantum steering was distilled [3], in which, rather than having Bob make a measurement, we directly consider the subnormalized marginal states $\tilde{\rho}_B^{x,a}$ that occur when Alice receives input x and produces output a. A local hidden state (LHS) model attempts to generate these via shared randomness. Denoting the shared randomness λ, distributed according to probability density $\mu(\lambda)$, Bob can output quantum state σ_λ, while Alice outputs a according to a probability distribution $\mathbf{P}_{x,\lambda}(a)$. A LHS model produces a faithful simulation if $\tilde{\rho}_B^{x,a} = \int_\lambda \mathbf{P}_{x,\lambda}(a)\sigma_\lambda \mathrm{d}\mu(\lambda)$.

If these states cannot be simulated with an LHS model, then we say that the state ρ is steerable. One can think of steering as an analogue of non-locality for the case where one party (Bob) trusts their measurement device (and hence in principle could do tomography to determine his marginal state after being told Alice's measurement and outcome). It is hence a useful intermediate between entanglement witnessing (both measurement devices trusted) and Bell violations (neither trusted) and has applications such as one-sided device-independent quantum cryptography [4] and channel discrimination [5]. Exhibiting new steerable states offers an expanded toolbox for such problems.

[*] Electronic address: camiller@umd.edu
[†] Electronic address: roger.colbeck@york.ac.uk
[‡] Electronic address: shiyy@umich.edu

But while simple to state, the steering classification problem has proved to be difficult even for 2-qubit systems. We consider why this is so. Let ρ_{AB} be a two-qubit state. If Alice were to measure $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ on input 0 and $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ on input 1 (where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$), then it is possible for Bob to obtain one of four subnormalized states which we denote $\tilde{\rho}_B^0, \tilde{\rho}_B^1, \tilde{\rho}_B^+, \tilde{\rho}_B^-$ (where, for example, $\tilde{\rho}_B^0 = \mathrm{Tr}_A[(|0\rangle\langle 0| \otimes \mathbb{1}_B)\rho]$). Determining whether a local hidden state model exists for these four states is a search over a finite-dimensional space and is not difficult. Next suppose Alice additionally performs the measurement $\{|\pi/4\rangle\langle\pi/4|, |5\pi/4\rangle\langle 5\pi/4|\}$ on a third input letter, where

$$|\theta\rangle := \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle\,, \tag{1}$$

leading to states $\tilde{\rho}_B^{\pi/4}, \tilde{\rho}_B^{5\pi/4}$. There is no guarantee that a local hidden state model that simulates the previous four states will simulate this new pair as well (generally, the states $\tilde{\rho}_B^{\pi/8}, \tilde{\rho}_B^{5\pi/8}$ are not in the convex hull of the former states). A new search for local hidden state models is required, and the search space increases exponentially with each new measurement. Thus a direct approach — even when just dealing with measurements of the form $\{|\theta\rangle\langle\theta|, |\theta+\pi\rangle\langle\theta+\pi|\}$ — is unlikely to be feasible.

Previous work on steering classification has achieved success by exploiting the symmetries of certain classes of states. For the class of Werner states $\{\Phi_\eta \mid \eta \in [0,1]\}$ given by

$$\Phi_\eta \;=\; \eta|\Phi^+\rangle\langle\Phi^+| + (1-\eta)\mathbb{1}/4, \tag{2}$$

an exact classification of P-steerability (i.e., steerability under projective measurements) has been performed (see Subsection II B in the current paper for a summary of results on Werner states). More recently a complete classification of P-steerability for T-states (i.e., states for which ρ_A is a maximally mixed state) has been given [6, 7]. In both cases the methods depended critically on the symmetry of the marginal state on Alice's side.

In the current work, we develop new techniques that allow us to step beyond T-states and consider the case where ρ_A is not maximally mixed. We study the simple case of RP-steerability (i.e., steerability by measurements in the span of $\{X, Z\}$). We give a complete classification of RP-steerability within the class of partially entangled Werner states $\{\Phi_{\alpha,\eta}\}$, which is given by

$$|\phi_\alpha\rangle \;:=\; \cos\alpha\,|00\rangle + \sin\alpha\,|11\rangle\,, \tag{3}$$
$$\Phi_{\alpha,\eta} \;:=\; \eta|\phi_\alpha\rangle\langle\phi_\alpha| + (1-\eta)\mathbb{1}/4. \tag{4}$$

The classification is shown in Figure 1, where the shaded/unshaded region represents the states that are unsteerable/steerable for real projective measurements. Our classification also applies to a larger class of real 2-qubit states (specifically, all states whose steering ellipse is tilted at an angle less than $\pi/4$). See Theorem 9 and Corollary 10 for the formal statement. To achieve this classification we introduce the concept of *keychain models*, which are a geometrically motivated class of local hidden state models for one-dimensional families of measurements. We explain this in more detail in the next subsection.

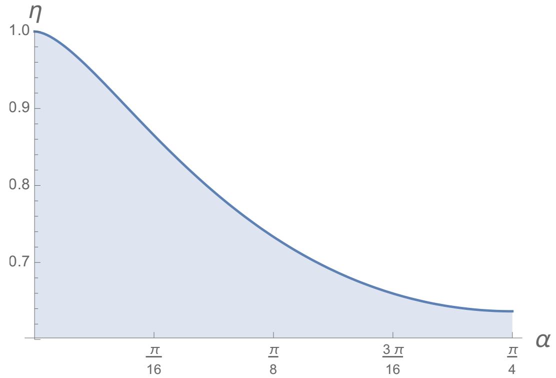

FIG. 1: RP-unsteerable partially entangled Werner states

Our approach invites generalizations. In its current form we have a criterion for steerability among all real 2-qubit states whose steering ellipse is tilted at an angle less than $\pi/4$. With additional work one may be able to generalize the classification to all real 2-qubit states. Additionally, the keychain approach could be applied in more general scenarios where steering is attempted with any one-dimensional family of measurements.

Studying the behavior of qubit states under real projective measurements is a natural problem, since, for example, it models measuring the polarizations of entangled photons. However, another future goal would be to extend our methods to arbitrary complex measurements on 2-qubit states. This looks more challenging — steering with a 2-dimensional family of measurements is considerably harder than with a 1-dimensional family of measurements — but if it can be accomplished, it would be an important step towards a complete criterion for steering among 2-qubit states.

A. Proof techniques

The difficulty in establishing steerability for a given set of measurements is that the space of LHS models is intractably large. Our proof begins with the observation that, in the case of real 2-qubit states and real projective measurements, a more tractable (though still infinite dimensional) class of LHS models suffices. Specifically, we consider the class of LHS models that we call "keychain models." Let $\mathbb{RP}^1$ denote the set of all real one-dimensional projectors on $\mathbb{C}^2$. A key chain model is a pair $(\mu, \{f_\theta\}_\theta)$, where μ is a probability distribution on S^1, and $f_\theta \colon S^1 \to [0,1]$ is a two-step function (meaning, roughly, a function that is constant at all but two points of S^1 — see Definition 4). We show that ρ_{AB} is RP-steerable if and only if it can be computed by a key chain model, i.e.,

$$\tilde{\rho}_B(\theta) \;=\; \int_{x \in S^1} x f_\theta(x) d\mu. \tag{5}$$

(This is similar to the model of [6, 7], which is based on functions on S^2 that are supported on half-spheres.) From this we can conclude that that if the circumference of the steering ellipse $\{\tilde{\rho}_B(\theta)\}$ is greater than 2, i.e.,

$$\int_{S^1} \left\| \frac{d}{d\theta} \tilde{\rho}_B(\theta) \right\|_1 d\theta \;>\; 2, \tag{6}$$

then the state ρ_{AB} has no local hidden state model.

At this point our proof diverges from that of [6, 7], since the converse of the above statement is not true in our case: if (6) fails to hold, there could still be no local hidden state model. However, the following stronger claim does guarantee the existence of a local hidden state model:

$$\int_{S^1} \left| \frac{d}{d\theta} \tilde{\rho}_B(\theta) \right| d\theta \;\leq\; 2\rho_B. \tag{7}$$

Moreover, the state ρ_{AB} is steerable if and only if

$$\rho'_{AB} := (\mathbb{1}_A \otimes Y)\rho_{AB}(\mathbb{1}_B \otimes Y) \tag{8}$$

is steerable for all positive definite Y, and by substituting in ρ'_{AB} for ρ_{AB} in (6) and (7) we obtain an infinite family of criterion for RP-steerability and RP-unsteerability. We thus need to find a Y such that one of (6) and (7) holds for ρ'_{AB}.

The most technically difficult part of our proof then shows that there must exist a positive definite density matrix Y such that

$$Y^{-1} \left[\int_{S^1} \left| Y \left(\frac{d}{d\theta} \tilde{\rho}_B(\theta) \right) Y \right| d\theta \right] Y^{-1} \tag{9}$$

is a scalar multiple of ρ_B. This compels (9) to either be greater than, or less than or equal to ρ_B, and thus we achieve a criterion for steering which is both necessary and sufficient. We prove this by demonstrating that if we let Y tend to any projector P in $\mathbb{RP}^1$, the normalization of (9) must tend to the orthogonal projector $P^\perp$. Any map from a 2-dimensional disc to itself which rotates the boundary of the disc must be an onto map, and this gives the desired result. (The proof of the aforementioned limit assertion is surprisingly subtle – the rate at which the normalization of (9) approaches $P^\perp$ turns out to be only logarithmic.)

Theorem 9 gives a formal statement of our main result. Figure 1 is then obtained by numerical computations to find appropriate operators Y for each partially entangled Werner state.

II. PRELIMINARIES

A. Notation and Definitions

For any Hilbert space $\mathcal{H}$, let $\mathcal{A}(\mathcal{H})$ denote the set of all Hermitian operators on $\mathcal{H}$, $\mathcal{P}_{\geq}(\mathcal{H})$ be the set of positive semidefinite operators on $\mathcal{H}$, $\mathcal{P}_{>}(\mathcal{H})$ be the set of positive definite operators on $\mathcal{H}$, $\mathcal{D}(\mathcal{H})$ denote the set of all density operators on $\mathcal{H}$, and $\mathcal{D}_{>}(\mathcal{H})$ denote the set of all positive definite density operators on $\mathcal{H}$. Let $\mathcal{RA}(\mathcal{H}), \mathcal{RP}_{\geq}(\mathcal{H})$ etc. denote the respective subsets of real operators (operator X is real if $\langle i|A|j\rangle \in \mathbb{R}$ for all i, j, where $\{|i\rangle\}$ is the standard basis). For an operator X on $\mathcal{H}$ we use $|X| := \sqrt{X^\dagger X}$ and $\|X\|_1 := \mathrm{tr}|X|$, the latter being the *trace norm* of X.

Throughout this paper, we let $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$ denote qubit systems possessed by Alice and Bob. Let let $\mathbb{RP}^1 \subseteq \mathcal{RD}(\mathcal{H})$ denote the set of one-dimensional real projectors on $\mathbb{C}^2$.

1. The steering ellipse

Any operator $\lambda \in \mathcal{RP}_{\geq}(\mathbb{C}^2)$ can be expressed uniquely as

$$\lambda = \frac{1}{2}(n\mathbb{1} + r_1\sigma_1 + r_3\sigma_3)\,, \tag{10}$$

where $\sigma_1 = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $\sigma_3 = |0\rangle\langle 0| - |1\rangle\langle 1|$ are the usual Pauli operators. If $\lambda \in \mathbb{RP}^1$ then $r_0 = 1$.

The *tilt* of λ, denoted $\mathrm{Tilt}(\lambda)$, is the quantity $\sqrt{r_1^2 + r_3^2}/n$. The *tilt angle* of λ is $\arctan(\mathrm{Tilt}(\lambda))$. If we think of (n, r_1, r_3) as 3-dimensional Cartesian coordinates, then the tilt angle of λ is angle that it forms with the $(1, 0, 0)$ axis. We will use these coordinates when we sketch ellipses later in this work. Note that an operator is positive semidefinite if and only if its tilt is less than or equal to 1. It is useful to note that

$$\|\lambda\|_1 = \begin{cases} |n| & \text{if } \mathrm{Tilt}(\lambda) \leq 1 \\ \sqrt{r_1^2 + r_3^2} & \text{if } \mathrm{Tilt}(\lambda) > 1 \end{cases} \tag{11}$$

Let $\rho_{AB} \in \mathcal{RD}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Then, the *steering ellipse* of ρ_{AB} on B is the function $\tilde{\rho}_B \colon \mathbb{RP}^1 \to \mathcal{P}_{\geq}(\mathbb{C}^2)$ given by

$$\tilde{\rho}_B(\theta) \ := \ \mathrm{Tr}_A\left[(|\theta\rangle\langle\theta| \otimes \mathbb{1}_B)\,\rho_{AB}\right]\,, \tag{12}$$

where $|\theta\rangle$ is defined in (1). Note that $\{|\theta\rangle, |\theta + \pi\rangle\}$ form an orthonormal basis, so $\rho_B = \tilde{\rho}_B(\theta) + \tilde{\rho}_B(\theta + \pi)$ for any θ. (In the more general case of arbitrary projective measurements, the states on Bob's side are a two-parameter family that define an ellipsoid rather than an ellipse [6].)

Definition 1. Let $\rho_{AB} \in \mathcal{RD}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Then, the *tilt of the steering ellipse of* ρ_{AB} is the equal to the tilt of any nonzero vector that is normal to the 2-dimensional affine space that contains the steering ellipse of ρ_{AB}.[1]

Note that if the tilt of the steering ellipse is less than or equal to 1, then no element of the steering ellipse is strictly greater (in the positive semidefinite sense) than any other.

2. Local hidden state models

In the most general sense, a local hidden state model for an indexed set of real 2-qubit subnormalized states $\{\tilde{\tau}_a\}_{a\in A}$ is a probability distribution μ on $\mathcal{D}(\mathbb{C}^2)$ and functions $\{f_a \colon \mathcal{D}(\mathbb{C}^2) \to [0, 1]\}_a$ such that

$$\tilde{\tau}_a \ = \ \int_{x\in\mathcal{D}(\mathbb{C}^2)} x f_a(x) d\mu \tag{13}$$

However, via the map $\mathcal{D}(\mathbb{C}^2) \to \mathcal{RD}(\mathbb{C}^2)$ given by $x \mapsto (x + \overline{x})/2$, we may assume μ, f_a are supported on $\mathcal{RD}(\mathbb{C}^2)$, and by decomposing each operator in $\mathcal{RD}(\mathbb{C}^2)$ into a convex combination of one-dimensional projectors, we may further assume that μ, f_a are supported in $\mathbb{RP}^1$. We are thus led to the following definition.

[1] If the steering ellipse does not span a 2-dimensional affine space (i.e., it is degenerate) then we say that its tilt is equal to ∞.

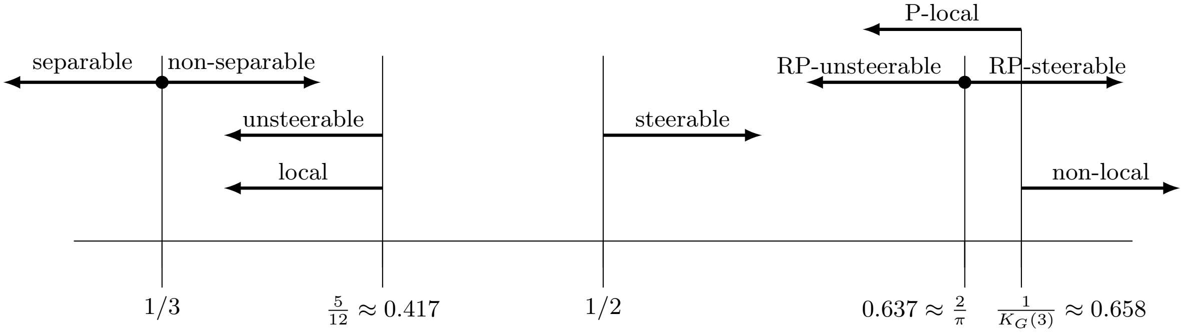

FIG. 2: Summary of known results for Werner states. The boundary of $2/\pi$ for RP-(un)steerability is new to the present paper.

Definition 2. A *local hidden state model* for an indexed set $\{\tilde{\tau}_a\}_{a\in A} \subseteq \mathcal{RP}_{\geq}(\mathbb{C}^2)$ is a pair $(\mu, \{f_a\}_a)$ such that μ is a probability distribution on $\mathbb{RP}^1$, $f_a \colon \mathbb{RP}^1 \to [0,1]$, and

$$\tilde{\tau}_a \;=\; \int_{x\in\mathbb{RP}^1} x f_a(x) d\mu. \tag{14}$$

A real 2-qubit state ρ_{AB} is *RP-steerable* if its steering ellipse, $\{\tilde{\rho}_B(\theta)\}_{\theta\in[0,2\pi)}$, does not have a local hidden state model.

Remark 3. The property of having a LHS model is convex, i.e., if ρ_{AB} and ρ'_{AB} have LHS models (for some set of measurements), then so does $p\rho_{AB} + (1-p)\rho'_{AB}$ for all $0 \leq p \leq 1$ (and the same set of measurements).

B. Known results for Werner states

Werner states (cf. (2)) are separable if and only if $\eta \leq \frac{1}{3}$ [8], are steerable if $\eta > \frac{1}{2}$ [3] and are non-local if $\eta > 1/K_G(3)$ [9], where $K_G(3)$ is Grothendieck's constant of order 3 [10], which is known to be below 1.52 (so that $1/K_G(3) > 0.658$) [9]. They are local for projective measurements if $\eta \leq 1/K_G(3)$ and are local for all measurements for $\eta \leq \frac{5}{12}$ [11] and also have a LHS model in this range [12]. For $1/3 < \eta \leq \frac{5}{12}$ the states are non-separable and unsteerable. For $\frac{1}{2} < \eta \leq \frac{1}{K_G(3)}$ the states are local for projective measurements and steerable. It is unknown whether these states are local for all measurements anywhere in this range, which would show steerability $\not\Rightarrow$ non-locality, however, this non-implication is known using another family of states [12].

The above is summarized in Figure 2, which also includes the new result about Werner states from the present paper.

III. KEYCHAIN MODELS

Next we formalize the class of keychain models. We begin with some preliminary definitions. Drawing from [7], if μ is a probability distribution on $\mathbb{RP}^1$, let $\mathrm{Box}(\mu)$ denote the convex set of all operators of the form

$$\int_{x\in\mathbb{RP}^1} x f(x) \; d\mu, \tag{15}$$

where f is a function from $\mathbb{RP}^1$ to the interval $[0,1]$. Note that $\mathrm{Box}(\mu) \subset \mathcal{RA}(\mathbb{C}^2)$ with $\mathrm{tr}(z) \leq 1$ for $z \in \mathrm{Box}(\mu)$ and that an ellipse has a local hidden state model if and only if it is contained in $\mathrm{Box}(\mu)$ for some probability distribution μ.

Note that there is a natural identification between $\mathbb{RP}^1$ and the unit circle $S^1 \subseteq \mathbb{R}^2$ which is given by $\frac{1}{2}(\mathbb{1} + r_1\sigma_1 + r_3\sigma_3) \leftrightarrow (r_1, r_3)$ with $r_1^2 + r_3^2 = 1$. We say that a sequence $s_1, s_2, s_3 \in \mathbb{RP}^1$ is a *clockwise* sequence if the images of s_1, s_2, s_3 form a clockwise sequence in S^1, and *counterclockwise* if the images of s_1, s_2, s_3 form a counterclockwise sequence in S^1. (If any of the points s_1, s_2, s_3 are the same, then we will say that the sequence is both clockwise and counterclockwise.) We say that a sequence $t_1, \ldots, t_n \in \mathbb{RP}^1$ is clockwise (resp. counterclockwise) if every 3-term subsequence of $t_1, t_2, \ldots, t_n, t_1$ is clockwise (resp. counterclockwise).

For any $x, y \in \mathbb{RP}^1$, let $[x, y]$ denote the set of all $z \in \mathbb{RP}^1$ such that x, y, z is a clockwise sequence. Let $(x, y) = \mathbb{RP}^1 \smallsetminus [y, x]$.

Definition 4. A function $f\colon \mathbb{RP}^1 \to [0,1]$ is a *two-step function* if there are (not necessarily distinct) elements $x, y \in \mathbb{RP}^1$ and $q \in [0, 1/2]$ such that

$$f(z) = \begin{cases} 1-q & \text{if} \quad z \in (x,y) \\ q & \text{if} \quad z \in (y,x), \end{cases} \tag{16}$$

and

$$q \leq f(x) \leq 1-q, \tag{17}$$
$$q \leq f(y) \leq 1-q. \tag{18}$$

We refer to q as the *bias* of the function and to x, y as the the *endpoints* of the function. If $q < 1/2$, then we refer specifically to x as the *left endpoint* and to y as the *right endpoint*.

We prove the following. Our method is very similar to that in [7].

Proposition 5. *Let μ be a probability distribution on $\mathbb{RP}^1$. Any element of $z \in \mathrm{Box}(\mu)$ can be written*

$$z = \int_{\mathbb{RP}^1} x g(x) d\mu, \tag{19}$$

where g is a two-step function (cf. Definition 4). If z is on the boundary of $\mathrm{Box}(\mu)$*, then such a function g exists with bias $q = 0$.*

Proof. The proof will be divided into two cases: (1) the case where z lies on the boundary of $\mathrm{Box}(\mu)$, and (2) the case where z lies in the interior of $\mathrm{Box}(\mu)$.

(1) In the case where z lies on the boundary of $\mathrm{Box}(\mu)$, there must exist $H \in \mathcal{RA}(\mathbb{C}^2)$ such that the function $x \mapsto \langle x, H \rangle$ on $\mathrm{Box}(\mu)$ is maximized at z. We subdivide into three cases depending on H.

Case 1a: The element z is on the boundary and $H > 0$.

The operator

$$\rho = \int_{\mathbb{RP}^1} x \, d\mu \tag{20}$$

is greater than or equal to z, so $\langle \rho - z, H \rangle \geq 0$. But this quantity cannot exceed 0 by assumption, so $\langle \rho - z, H \rangle = 0$, which yields $\rho = z$. Since the constant function $\mathbb{RP}^1 \to \{1\}$ satisfies the definition of a two-step function, we are done.

Case 1b: The element z is on the boundary and $H \not\geq 0$.

In this case, there are unique distinct elements $y, w \in \mathbb{RP}^1$ such that $\langle y, H \rangle = \langle w, H \rangle = 0$, $\langle x, H \rangle > 0$ for all $x \in (y, w)$, and $\langle x, H \rangle < 0$ for all $x \in (w, y)$. Choose a function $f\colon \mathbb{RP}^1 \to [0,1]$ such that

$$z = \int_{\mathbb{RP}^1} x f(x) \, d\mu \tag{21}$$

(such a function must exist because $z \in \mathrm{Box}(\mu)$). Let g be the two step-function

$$g(x) = \begin{cases} 1 & \text{if} \quad x \in (y,w) \\ 0 & \text{if} \quad x \in (w,y) \\ f(y) & \text{if} \quad x = y \\ f(w) & \text{if} \quad x = w. \end{cases} \tag{22}$$

and let

$$r = \int_{x \in \mathbb{RP}^1} x g(x) \, d\mu \, . \tag{23}$$

Since $r \in \mathrm{Box}(\mu)$, $\langle r, H \rangle \leq \langle z, H \rangle$. Hence we have

$$0 \geq \langle r - z, H \rangle = \left\langle \int_{x \in (y,w)} (1 - f(x)) x d\mu, H \right\rangle - \left\langle \int_{x \in (w,y)} f(x) x d\mu, H \right\rangle \geq 0 \, , \tag{24}$$

where the final inequality follows because any operator $x \in (y, w)$ has positive inner product with H and any operator $x \in (w, y)$ has negative inner product with H. It follows that $z = r$, which completes this case.

Case 1c: The element z is on the boundary and H is positive semidefinite and rank-one.

Let $y \in \mathbb{RP}^1$ be the unique element such that $\langle H, y \rangle = 0$. Let

$$g(x) \;=\; \begin{cases} 1 & \text{if} \quad x \neq y \\ f(y) & \text{if} \quad x = y\,, \end{cases} \tag{25}$$

where $f \colon \mathbb{RP}^1 \to [0,1]$ is a function such that (21) holds. By similar reasoning as in Case 1b, this function also computes z.

Case 2: The element z is in the interior of $\mathrm{Box}(\mu)$.

Let

$$c \;=\; \int_{\mathbb{RP}^1} (1/2) x d\mu. \tag{26}$$

Since z is interior it can be written as $z = tc + (1-t)b$, where $t \in [0,1]$ and b is an element on the boundary of $\mathrm{Box}(\mu)$. Let g be a two-step function which computes b, which must exist from the first part of the proof. Then, the function $t/2 + (1-t)g$ computes z. □

A *keychain* model for a set $\{\sigma_a\} \subseteq \mathcal{RP}_{\geq}(\mathbb{C}^2)$ of subnormalized states is a local hidden state model $(\mu, \{f_a\})$ in which the functions are all two-step functions. The previous proposition shows that any set that has a local hidden state model also has a keychain model.

Next we will use the foregoing techniques to prove a geometric fact about steerability. Let us say that the *length* of a piecewise differentiable curve $S \colon [0,1] \to \mathcal{RA}(\mathbb{C}^2)$ is its length under the trace norm:

$$\int_0^1 \left\| \frac{\mathrm{d}}{\mathrm{d}t} S(t) \right\|_1 dt. \tag{27}$$

Proposition 6. *Let $\rho_{AB} \in \mathcal{RD}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be a two-qubit state whose steering ellipse has tilt < 1 and whose steering ellipse $\{\tilde{\rho}_B(\theta)\}_\theta$ has a local hidden state model. Then, the length of $\{\tilde{\rho}_B(\theta)\}_\theta$ is no more than 2.*

Note that, using (11), the length of this curve is the Euclidean length of the projection of the ellipse onto the $r_0 = 0$ plane in Bloch representation. It can be calculated using

$$\int_0^{2\pi} \sqrt{\left(\frac{\mathrm{d}}{\mathrm{d}\theta} r_1(\theta)\right)^2 + \left(\frac{\mathrm{d}}{\mathrm{d}\theta} r_3(\theta)\right)^2}\, \mathrm{d}\theta\,.$$

For the proof of Proposition 6, we will need the following definition.

Definition 7. A probability distribution on $\mathbb{RP}^1$ is *discrete* if it supported at a finite number of points.

Any probability distribution on $\mathbb{RP}^1$ can be approximated to an arbitrary degree of accuracy by discrete probability distributions.

The next lemma asserts that if μ is a discrete probability distribution, certain slices of $\mathrm{Box}(\mu)$ must have circumference ≤ 2 under the trace norm.

Lemma 8. *Let μ be a discrete probability distribution on $\mathbb{RP}^1$ with $\int_{\mathbb{RP}^1} x d\mu = \rho$, and $H \in \mathcal{RP}_{>}(\mathbb{C}^2)$. Then, the set*

$$\{M \in \mathrm{Box}(\mu) \mid \langle M, H \rangle = (1/2) \langle \rho, H \rangle\} \tag{28}$$

is enclosed by a curve of length ≤ 2.

Proof. We will construct an explicit curve which is the boundary of (28). Let $S = \{s_1, \ldots, s_n\}$ be the support of μ, where the points $|0\rangle\langle 0|, s_1, \ldots, s_n$ are in clockwise order, and define $\tilde{\rho}_m := \sum_{i=1}^m \mu_{s_i} s_i$.

For any $t \in [0, \langle H, \rho \rangle]$, define a two-step function $h_t \colon \mathbb{RP}^1 \to [0,1]$ as follows: if

$$t \in [\langle \rho_m, H \rangle, \langle \rho_{m+1}, H \rangle)\,, \tag{29}$$

then

$$h_t(x) \;=\; 1 \quad \text{for } x \in [|0\rangle\langle 0|, s_{m+1}) \tag{30}$$

$$h_t(s_{m+1}) \;=\; \left(\frac{t - \langle \rho_m, H \rangle}{\mu(s_{m+1}) \langle s_{m+1}, H \rangle}\right) \tag{31}$$

and h_t is zero elsewhere. Note that, by construction,

$$\int_{x\in\mathbb{RP}^1} h_t(x)\left\langle x,H\right\rangle d\mu \;=\; t. \tag{32}$$

Also define a two-step function $\overline{h}_t\colon \mathbb{RP}^1 \to [0,1]$ by

$$\overline{h}_t \;=\; \begin{cases} h_{(t+\langle\rho,H\rangle/2)} - h_t & \text{if } t < \left\langle \rho,H\right\rangle/2 \\ 1 - h_t + h_{(t-\langle\rho,H\rangle/2)} & \text{otherwise,} \end{cases} \tag{33}$$

so that for any t,

$$\int_{x\in\mathbb{RP}^1} \overline{h}_t(x)\left\langle x,H\right\rangle d\mu \;=\; \left\langle \rho,H\right\rangle/2. \tag{34}$$

Let

$$G(t) \;=\; \int_{x\in\mathbb{RP}^1} \overline{h}_t(x)x\; d\mu. \tag{35}$$

The image of G is then the boundary of (28).

Note that for any fixed i, the function $t \mapsto \overline{h}_t(s_i)$ is bitonic (in the sense that it only increases once and decreases once, modulo $\left\langle\rho,H\right\rangle$) and has extreme values $0,1$, and thus

$$\int_0^{\langle\rho,H\rangle} \left|\frac{d}{dt}\left(\overline{h}_t(s_i)\right)\right| dt = 2. \tag{36}$$

Therefore, the length of the curve G is given by

$$\begin{aligned}
\int_0^{\langle\rho,H\rangle}\left\|\frac{d}{dt}G(t)\right\|_1 dt \;&=\; \int_0^{\langle\rho,H\rangle}\left\|\frac{d}{dt}\int_{x\in\mathbb{RP}^1}\overline{h}_t(x)x d\mu\right\|_1 dt &(37)\\
&=\; \int_0^{\langle\rho,H\rangle}\left\|\frac{d}{dt}\sum_{i=1}^n \overline{h}_t(s_i)s_i\mu(s_i)\right\|_1 dt &(38)\\
&\le\; \int_0^{\langle\rho,H\rangle}\sum_{i=1}^n\left|\frac{d}{dt}\left(\overline{h}_t(s_i)\right)\right|\mu(s_i)dt &(39)\\
&=\; \sum_{i=1}^n 2\mu(s_i) &(40)\\
&=\; 2, &(41)
\end{aligned}$$

as desired. □

Proof of Proposition 6. Let $(\mu,\{f_\theta\})$ be a keychain local hidden state model for the steering ellipse of ρ_{AB}. Let H be a (non-zero) positive semidefinite operator which is normal to the steering ellipse of ρ_{AB} (such an operator exists because the tilt of the steering ellipse of ρ_{AB} is at most 1 by assumption). Because it is normal to the ellipse, $\left\langle\tilde{\rho}_B(\theta),H\right\rangle = u$ (independent of θ). Choose a sequence $\mu_1,\mu_2,\ldots$ of discrete probability distributions on $\mathbb{RP}^1$ which converges to μ. Then, the sets

$$\left\{M\in \mathrm{Box}(\mu_i)\mid \left\langle M,H\right\rangle = (1/2)\left\langle\rho_B,H\right\rangle\right\}, \tag{42}$$

each of which is enclosed by some curve of circumference ≤ 2, converge to the set

$$\left\{M\in \mathrm{Box}(\mu)\mid \left\langle M,H\right\rangle = (1/2)\left\langle\rho_B,H\right\rangle\right\}. \tag{43}$$

Because $\left\langle\tilde{\rho}_B,H\right\rangle = \left\langle\tilde{\rho}_B(\theta),H\right\rangle + \left\langle\tilde{\rho}_B(\theta+\pi),H\right\rangle = 2u$, this set contains $\tilde{\rho}_B(\theta)$. The desired result follows. □

IV. A CRITERION FOR *RP*-STEERABILITY

The previous section gave a necessary condition for RP-steeraibility. Our next goal is to create a criterion that is both necessary and sufficient.

We now state our main result.

Theorem 9. *Let $\rho_{AB} \in \mathcal{RD}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be a two-qubit state whose steering ellipse has tilt < 1. Then, ρ_{AB} is RP-unsteerable if and only if there exists $Y \in \mathcal{RP}_{>}(\mathbb{C}^2)$ such that*

$$Y\rho_B Y - \int_0^{\pi} \left| Y \frac{\mathrm{d}}{\mathrm{d}\theta}\left(\tilde{\rho}_B\left(\theta\right)\right) Y \right| \mathrm{d}\theta \geq 0\,. \tag{44}$$

Corollary 10. *Let $\rho_{AB} \in \mathcal{RD}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be a two-qubit state whose steering ellipse has tilt < 1. Then ρ_{AB} is RP-steerable if and only if there exists $Y \in \mathcal{RP}_{>}(\mathbb{C}^2)$ such that*

$$Y\rho_B Y - \int_0^{\pi} \left| Y \frac{\mathrm{d}}{\mathrm{d}\theta}\left(\tilde{\rho}_B\left(\theta\right)\right) Y \right| \mathrm{d}\theta \leq 0\,, \tag{45}$$

with the left-hand-side not equal to 0.

* * * Some definitions removed since in preliminaries; we could consider whether the definition below could be removed with a little rewriting of the appendix. * * *

For the proofs of Theorem 9 and Corollary 10, we begin with the following definition.

Definition 11. For $Y \in \mathcal{A}(\mathcal{H})$ with $Y > 0$, define

$$\left|X\right|_Y \ := \ Y^{-1}\left|YXY\right|Y^{-1} \tag{46}$$

and $\|X\|_{1,Y} := \mathrm{Tr}(|X|_Y)$.

Note that (52) can be rewritten as

$$\rho_B - \int_0^{\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\theta}\left(\tilde{\rho}_B\left(\theta\right)\right) \right|_Y \mathrm{d}\theta \geq 0\,. \tag{47}$$

We proceed by developing various components for the proof of Theorem 9. The following result found in [12] will be useful.

Lemma 12. *If ρ_{AB} has a LHS model (for any set of measurements), then so does*

$$(\mathcal{I} \otimes \mathcal{M})(\rho_{AB})/\mathrm{tr}((\mathcal{I} \otimes \mathcal{M})(\rho_{AB})) \tag{48}$$

for any positive linear map $\mathcal{M}$.

Additionally, we need the following lemma about the asymptotic behavior of the integral in inequality (47). For any ϵ and any real unit vector $v \in \mathbb{C}^2$, let

$$D_{\epsilon,v} \ = \ \epsilon(\mathbb{1} - |v\rangle\langle v|) + |v\rangle\langle v|. \tag{49}$$

For any nonzero positive semidefinite matrix A, we use $\langle A \rangle$ to denote the normalization of A, i.e., $\langle A \rangle := A/\mathrm{tr}(A)$.

Lemma 13. *Let $\rho_{AB} \in \mathcal{RD}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be a two-qubit state whose steering ellipse has tilt < 1. Let $\{v, w\}$ be an orthogonal basis for $\mathbb{C}^2$. Then,*

$$\lim_{\epsilon \to 0} \left\langle \int_0^{2\pi} \Bigg(\left| \frac{d}{d\theta} \tilde{\rho}_B(\theta) \right|_{D_{\epsilon,v}} d\theta \right\rangle \Bigg(= \ |w\rangle\langle w|. \tag{50}$$

Proof. This is given by Corollary 26 in the Appendix. □

As a consequence of Lemma 13, the function $\mathcal{RD}_{>}(\mathbb{C}^2) \to \mathcal{RD}(\mathbb{C}^2)$ given by

$$Y \mapsto \left\langle \int_0^{2\pi} \left| \frac{d}{d\theta} \tilde{\rho}_B(\theta) \right|_{D_{\epsilon,v}} d\theta \right\rangle . \tag{51}$$

extends continuously to a map $\mathcal{RD}(\mathbb{C}^2) \to \mathcal{RD}(\mathbb{C}^2)$ which has the effect of mapping each element of $\mathbb{RP}^1$ to its orthogonal complement. By Lemma 18 in the appendix, the function given by (51) is onto. In particular, its image contains ρ_B. We therefore have the following.

Lemma 14. *Let $\rho_{AB} \in \mathcal{RD}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be a two-qubit state whose steering ellipse has tilt < 1. Then, there exists $Y \in \mathcal{RD}_{>}(\mathbb{C}^2)$ such that*

$$\int_0^{2\pi} \left| \frac{d}{d\theta} \tilde{\rho}_B(\theta) \right|_{Y} d\theta \tag{52}$$

is a scalar multiple of ρ_B.

Proof of Theorem 9. For any Hermitian operator X, define $|X|_{\pm} := (|X| \pm X)/2$, and $\|X\|_{\pm} = \operatorname{tr} |X|_{\pm}$.

Case 1: Suppose

$$\rho_B \ \geq \ \rho' := \int_0^{\pi} \left| \frac{d}{d\theta} \left(\tilde{\rho}_B \left(\theta \right) \right) \right| d\theta \, , \tag{53}$$

and define

$$\sigma_\lambda \ := \ \left| \frac{d}{d\lambda} \left(\tilde{\rho}_B \left(\lambda \right) \right) \right|_{+} + \frac{\rho_B - \rho'}{2\pi} . \tag{54}$$

Because $\tilde{\rho}_B(\lambda + \pi) = \rho_B - \tilde{\rho}_B(\lambda)$, the operator $(d/d\lambda)\tilde{\rho}_B(\lambda + \pi)$ is the negation of the operator $(d/d\lambda)\tilde{\rho}_B(\lambda)$, and so the following equality also holds:

$$\sigma_\lambda \ = \ \left| \frac{d}{d\lambda} \left(\tilde{\rho}_B \left(\lambda + \pi \right) \right) \right|_{-} + \frac{\rho_B - \rho'}{2\pi} . \tag{55}$$

We proceed to construct a local hidden state model from $\{\sigma_\lambda\}_\lambda$. We have the following:

$$\begin{aligned}
\int_0^{2\pi} \sigma_\lambda d\lambda \ &= \ \int_0^{2\pi} \left| \frac{d}{d\lambda} \tilde{\rho}_B \left(\lambda \right) \right|_{+} d\lambda + \rho_B - \rho' && (56) \\
&= \ \int_0^{\pi} \left| \frac{d}{d\lambda} \tilde{\rho}_B \left(\lambda \right) \right|_{+} d\lambda + \int_{\pi}^{2\pi} \left| \frac{d}{d\lambda} \tilde{\rho}_B \left(\lambda \right) \right|_{+} d\lambda + (\rho_B - \rho') && (57) \\
&= \ \int_0^{\pi} \left| \frac{d}{d\lambda} \tilde{\rho}_B \left(\lambda \right) \right|_{+} d\lambda + \int_0^{\pi} \left| \frac{d}{d\lambda} \tilde{\rho}_B \left(\lambda \right) \right|_{-} d\lambda + (\rho_B - \rho') && (58) \\
&= \ \int_0^{\pi} \left| \frac{d}{d\lambda} \tilde{\rho}_B \left(\lambda \right) \right| d\lambda + (\rho_B - \rho') && (59) \\
&= \ \rho' + \rho_B - \rho' && (60) \\
&= \ \rho_B . && (61)
\end{aligned}$$

For any $\theta \in [0, \pi]$ let $g_\theta \colon \mathbb{RP}^1 \to [0, 1]$ be equal to zero on the interval $[\theta, \theta + \pi]$ and equal to 1 elsewhere, and define

g_θ for $\theta \in (\pi, 2\pi]$ by $g_\theta = 1 - g_{\theta-\pi}$. Then,

$$\begin{aligned}
\int_0^{2\pi} g_\theta(\lambda)\sigma_\lambda d\lambda &= \frac{1}{2}\left[\int_0^{2\pi}(2g_\theta(\lambda)-1)\sigma_\lambda d\lambda + \int_0^{2\pi}\sigma_\lambda d\lambda\right] &(62)\\
&= \frac{1}{2}\left[-\int_\theta^{\theta+\pi \textbf{ mod } 2\pi}\sigma_\lambda d\lambda + \int_{\theta+\pi \textbf{ mod } 2\pi}^{\theta+2\pi \textbf{ mod } 2\pi}\sigma_\lambda d\lambda + \rho_B\right] &(63)\\
&= \frac{1}{2}\left[-\int_\theta^{\theta+\pi \textbf{ mod } 2\pi}\left|\frac{d}{d\lambda}\tilde{\rho}_B(\lambda)\right|_+ d\lambda + \int_\theta^{\theta+\pi \textbf{ mod } 2\pi}\left|\frac{d}{d\lambda}\tilde{\rho}_B(\lambda)\right|_- d\lambda + \rho_B\right] &(64)\\
&= \frac{1}{2}\left[-\int_\theta^{\theta+\pi \textbf{ mod } 2\pi}\frac{d}{d\lambda}\tilde{\rho}_B(\lambda)d\lambda + \rho_B\right] &(65)\\
&= \frac{1}{2}\left[-\tilde{\rho}_B(\theta+\pi) + \tilde{\rho}_B(\theta) + \rho_B\right] &(66)\\
&= \tilde{\rho}_B(\theta). &(67)
\end{aligned}$$

Thus $\{\tilde{\rho}_B(\theta)\}_\theta$ has a local hidden state model.

Case 2: Suppose that there exists $Y \in \mathcal{RP}_>(\mathbb{C}^2)$ such that

$$Y\rho_B Y \geq \int_0^\pi \left|Y\frac{d}{d\theta}\left(\tilde{\rho}_B(\theta)\right)Y\right| d\theta\,. \tag{68}$$

In this case, the state

$$\overline{\rho_{AB}} = \frac{(\mathbb{1}\otimes Y)\rho_{AB}(\mathbb{1}\otimes Y)}{\mathrm{Tr}[(\mathbb{1}\otimes Y)\rho_{AB}(\mathbb{1}\otimes Y)]} \tag{69}$$

satisfies the conditions of Case 1. Since $\mathcal{M} : X \mapsto Y^{-1}XY^{-1}$ is a positive map, by Lemma 12, a local hidden state model exists for ρ_{AB}.

Case 3: Suppose that for all $Y \in \mathcal{RP}_>(\mathbb{C})$,

$$Y\rho_B Y \ngeq I_Y := \int_0^\pi \left|Y\frac{d}{d\theta}\left(\tilde{\rho}_B(\theta)\right)Y\right| d\theta \tag{70}$$

By Lemma 14, we can find Y such that I_Y is a scalar multiple of $Y\rho_B Y$ (this is why Corollary 10 follows from Theorem 9). Thus we have

$$Y\rho_B Y = c\int_0^\pi \left|Y\frac{d}{d\theta}\left(\rho_B(\theta)\right)Y\right| d\theta \tag{71}$$

for some $c < 1$. Letting $\gamma_{AB} = \langle(\mathbb{1}\otimes Y)\rho_{AB}(\mathbb{1}\otimes Y)\rangle$, we have

$$\gamma_B = c\int_0^\pi \left|\frac{d}{d\theta}\left(\gamma_B(\theta)\right)\right| d\theta \tag{72}$$

which in particular means

$$\int_0^\pi \left\|\frac{d}{d\theta}\left(\gamma_B(\theta)\right)\right\|_1 d\theta \geq (1/c)\mathrm{Tr}(\gamma_B) > 1. \tag{73}$$

By symmetry, replacing the upper limit (π) in the integral above has the effect of doubling its value; thus,

$$\int_0^{2\pi} \left\|\frac{d}{d\theta}\left(\gamma_B(\theta)\right)\right\|_1 d\theta > 2, \tag{74}$$

which implies by Proposition 6 that γ (and therefore ρ) has no local hidden variable model. □

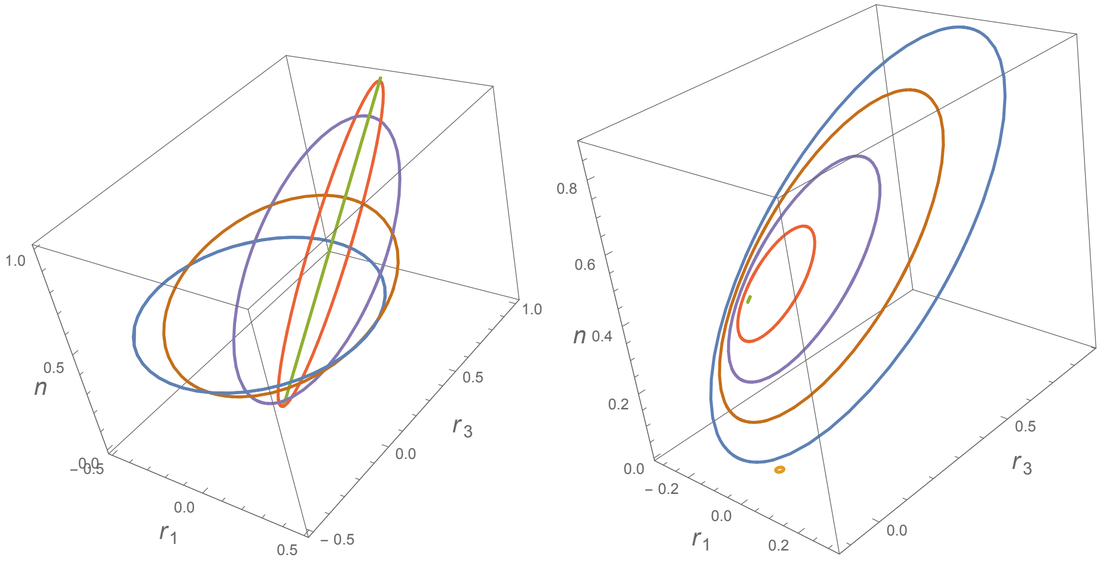

FIG. 3: [left] Steering ellipses in the Bloch representation for $\eta = 1$, $\alpha = \pi/4$ (blue), 0.65 (brown), 0.35 (purple), 0.1 (red) and 0 (green); [right] $\alpha = 0.35$ and $\eta = 1$ (blue), $\frac{3}{4}$ (brown), $\frac{1}{2}$ (purple), $\frac{1}{4}$ (red) and $\eta = 0.01$ (green). The small yellow circle on the right marks the origin.

V. EXPLICIT CALCULATIONS FOR STEERING ELLIPSES

A. Application I: RP-steerability of Werner states

It is interesting to see what this criteria gives for Werner states. Let us consider the family $\rho_{AB}(\eta) = \eta|\Phi_+\rangle\langle\Phi_+| + (1-\eta)\mathbb{1}/4$ where $\eta \in [0,1]$ and $|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Theorem 15. *States of the form $\rho_{AB}(\eta)$ are RP-unsteerable for $\eta \leq \frac{2}{\pi}$ and are RP-steerable for $\eta > \frac{2}{\pi}$.*

Proof. The steering ellipses for these states are $\tilde{\rho}_B(\theta) = \frac{1}{4}\begin{pmatrix} 1+\eta\cos\theta & \eta\sin\theta \\ \eta\sin\theta & 1-\eta\cos\theta \end{pmatrix}$ and have zero tilt for all η (since all these states have the same trace, the difference between any two states on the ellipse is orthogonal to $\mathbb{1}/2$). The derivative with respect to θ is $\frac{\mathrm{d}}{\mathrm{d}\theta}(\tilde{\rho}_B(\theta)) = \frac{\eta}{4}\begin{pmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{pmatrix}$ which has $|\frac{\mathrm{d}}{\mathrm{d}\theta}(\tilde{\rho}_B(\theta))| = \frac{\eta}{4}\mathbb{1}$. Hence,

$$\rho_B - \int_0^\pi \left|\frac{\mathrm{d}}{\mathrm{d}\theta}\left(\tilde{\rho}_B\left(\theta\right)\right)\right| \mathrm{d}\theta = \mathbb{1}/2 - \frac{\pi\eta}{4}\mathbb{1}\,.$$

Applying Theorem 9 and Corollary 10 with $Y = \mathbb{1}$ we have that Werner states are RP-unsteerable if $\frac{\pi\eta}{4} \leq \frac{1}{2}$, i.e., $\eta \leq \frac{2}{\pi} \approx 0.637$ and are RP-steerable if $\eta > \frac{2}{\pi}$. □

B. Application II: RP-steerability of partially entangled Werner states

Consider the family $\rho_{AB}(\alpha,\eta) := \eta|\phi_\alpha\rangle\langle\phi_\alpha| + (1-\eta)\mathbb{1}/4$, where $|\phi_\alpha\rangle := \cos\alpha|00\rangle + \sin\alpha|11\rangle$ for $0 \leq \alpha \leq \frac{\pi}{4}$. The steering ellipses for these states are $\tilde{\rho}_B^{\alpha,\eta}(\theta) = \begin{pmatrix} \eta\cos^2(\alpha)\cos^2\left(\frac{\theta}{2}\right) - \frac{\eta}{4} + \frac{1}{4} & \frac{1}{2}\eta\cos(\alpha)\sin(\alpha)\sin(\theta) \\ \frac{1}{2}\eta\cos(\alpha)\sin(\alpha)\sin(\theta) & \eta\sin^2(\alpha)\sin^2\left(\frac{\theta}{2}\right) - \frac{\eta}{4} + \frac{1}{4} \end{pmatrix}$ and are plotted in the Bloch representation in Fig. 3.

One can verify that for $A_\alpha = \begin{pmatrix} \sin^2\alpha & 0 \\ 0 & \cos^2\alpha \end{pmatrix}$, $\mathrm{tr}(A_\alpha\tilde{\rho}_B^{\alpha,\eta}(\theta)) = \frac{1}{8}(2-\eta(1-\cos(4\alpha)))$, i.e., is independent of θ. A_α is hence normal to the steering ellipse and so the tilt of the ellipse is $\cos(2\alpha) \leq 1$, and approaches 1 as α approaches 0.

Remark 16. The tilt is independent of η and hence the steering ellipse for any two-qubit pure state has tilt at most 1.

We have $\rho_B(\alpha,\eta) = \frac{1}{2}(1+\eta\cos(2\alpha))|0\rangle\langle 0| + \frac{1}{2}(1-\eta\cos(2\alpha))|1\rangle\langle 1|$.

The derivative of the steering ellipse with respect to θ is

$$\frac{\mathrm{d}}{\mathrm{d}\theta}\tilde{\rho}_B^{\alpha,\eta}(\theta) = \frac{\eta}{2}\begin{pmatrix} -\cos^2(\alpha)\sin(\theta) & \cos(\alpha)\sin(\alpha)\cos(\theta) \\ \cos(\alpha)\sin(\alpha)\cos(\theta) & \sin^2(\alpha)\sin(\theta)\end{pmatrix}\Bigg(. \tag{75}$$

For $\alpha = \frac{\pi}{4}$ the case is as before. To investigate other values of α, we note that, by Remark 3, if $\rho_{AB}(\alpha,\eta)$ has a LHS model, then so does $\rho_{AB}(\alpha,\eta')$ for $\eta' < \eta$. Thus, for each α there is a critical value $\bar{\eta}(\alpha)$ such that $\rho_{AB}(\alpha,\eta)$ is RP-steerable for $\eta > \bar{\eta}(\alpha)$ and is RP-unsteerable for $\eta < \bar{\eta}(\alpha)$. We search for this critical value numerically.

Since Y has real entries, is positive and multiplying by a constant doesn't affect whether (52) holds, we can take Y to have $\mathrm{tr}(Y) = 1$ and parameterize it in terms of two parameters r_1 and r_3 using a plane of the Bloch sphere via $Y = \frac{1}{2}(\mathbb{1} + r_1\sigma_1 + r_3\sigma_3)$. To do the search we use the following subroutines:

1. For fixed α and η this searches over r_1, r_3 to find the largest value of the minimum eigenvalue of the expression on the left of (52). This uses gradient ascent with decreasing step-size, terminating when no improvement can be found for some minimal step-size, or when r_1, r_3 are found such that the minimum eigenvalue is positive (i.e., (52) is satisfied). The output is either the largest value found or the first positive value found.

2. This is analogous to Subroutine 1, except it searches for the smallest value of the maximum eigenvalue of the expression on the left of (52), terminating either when a negative value is obtained or when no improvement can be found for some minimal step-size.

3. For fixed α, this uses Binary Search to find the largest η for which Subroutine 1 returns a positive value, for some number of search steps.

4. For fixed α, this uses Binary Search to find the smallest η for which Subroutine 2 returns a negative value, for some number of search steps.

Subroutine 3 hence gives a certified lower bound on $\bar{\eta}(\alpha)$ and Subroutine 4 a certified upper bound. By varying the step-sizes and number of steps, in principle, we can make the gap between these as small as we like (in practice, the limits of machine precision provide a cut-off).

Note that if Subroutine 1 has a negative output, we cannot strictly rule out that there exists a Y such that condition (52) holds: in principle a smaller step-size might reveal a suitable Y. This is why we use Subroutine 2 in parallel.

The result is given in Figure 1 (although the plot only shows $\eta > 0.6$, the region extends to $\eta = 0$).

C. RP-steerability of depolarizing channel states

Consider a source that generates an entangled state that is sent to two parties via two depolarizing channels with parameters η_A and η_B, i.e., these channels take $\mathcal{S}(\mathbb{C}^2\otimes\mathbb{C}^2) \mapsto \mathcal{S}(\mathbb{C}^2\otimes\mathbb{C}^2) : \rho_{AB} \mapsto \hat{\rho}_{AB} := (\mathcal{E}_{\eta_A}\otimes\mathcal{E}_{\eta_B})(\rho_{AB})$, where $\mathcal{E}_\eta : \mathcal{S}(\mathbb{C}^2) \mapsto \mathcal{S}(\mathbb{C}^2)$ is given by $\mathcal{E}_\eta(\rho) = \eta\rho + (1-\eta)\mathbb{1}/2$.

For $\rho_{AB} = |\Phi_+\rangle\langle\Phi_+|$, this channel leads to Werner states (except with parameter $\eta_A\eta_B$ instead of η). The states are hence RP-unsteerable iff $\eta_A\eta_B \leq \frac{2}{\pi} \approx 0.637$.

More generally, for $\rho_{AB} = |\phi_\alpha\rangle\langle\phi_\alpha|$, we call the state after the channel $\hat{\rho}_{AB}(\alpha,\eta_A,\eta_B)$ and note that $\hat{\rho}_B = \frac{1}{2}\left((1+\eta_B\cos(2\alpha))|0\rangle\langle 0| + (1-\eta_B\cos(2\alpha))|1\rangle\langle 1|\right)$ is independent of η_A. The steering ellipse for such a state is

$$\tilde{\rho}_B^{\alpha,\eta_A,\eta_B}(\theta) = \frac{1}{4}\begin{pmatrix} 1+\eta_A\cos(2\alpha)\cos(\theta)+\eta_B(\eta_A\cos(\theta)+\cos(2\alpha)) & \eta_A\eta_B\sin(2\alpha)\sin(\theta) \\ \eta_A\eta_B\sin(2\alpha)\sin(\theta) & 1+\eta_A\cos(2\alpha)\cos(\theta)-\eta_B(\eta_A\cos(\theta)+\cos(2\alpha))\end{pmatrix}\Bigg($$

For $A_{\alpha,\eta_A,\eta_B} = \begin{pmatrix} \frac{\eta_B-\cos(2\alpha)}{2\eta_B} & 0 \\ 0 & \frac{\eta_B+\cos(2\alpha)}{2\eta_B}\end{pmatrix}\Bigg($, we have $\mathrm{tr}(A_{\alpha,\eta_A,\eta_B}\tilde{\rho}_B^{\alpha,\eta_A,\eta_B}(\theta)) = \frac{1}{2}\sin^2(2\alpha)$, which is independent of θ. Hence A_{α,η_A,η_B} is the normal to the steering ellipse, and the ellipse has tilt $\frac{\cos(2\alpha)}{\eta_B}$. This is at most 1 for $\eta_B \geq \cos(2\alpha)$, so we can use Theorem 9 and Corollary 10 provided this holds.

The derivative of the steering ellipse is

$$\frac{\mathrm{d}}{\mathrm{d}\theta}\tilde{\rho}_B^{\alpha,\eta_A,\eta_B}(\theta) = \frac{\eta_A}{4}\begin{pmatrix} -(\eta_B+\cos(2\alpha))\sin(\theta) & \eta_B\sin(2\alpha)\cos(\theta) \\ \eta_B\sin(2\alpha)\cos(\theta) & (\eta_B-\cos(2\alpha))\sin(\theta)\end{pmatrix}\Bigg(.$$

Since this is proportional to η_A, the amount of noise on Alice's side (the untrusted side), the case of noise only on Bob's side is representative of the general case.

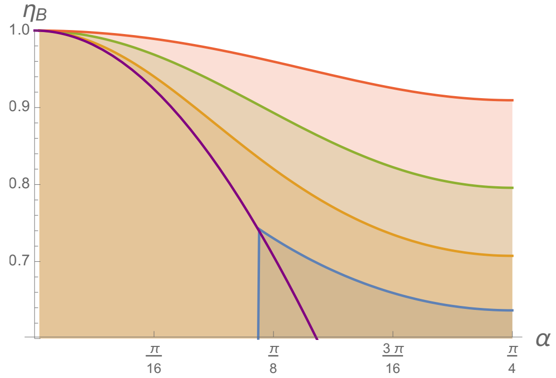

FIG. 4: Plot of the region where a LHS model exists for all real projective measurements for $\eta_A = 1$ (blue), $\eta_A = 0.9$ (orange) and $\eta_A = 0.8$ (green), $\eta_A = 0.7$ (red), together with the purple curve $\eta_B = \cos(2\alpha)$ which we need to be above to use Theorem 9 and Corollary 10. In the case $\eta_A = \frac{2}{\pi}$ (not shown), the state is steerable for all η_B and α. Above each of the regions, the state is RP-steerable. To the left of the blue region our criteria is unable to decide whether or not the states have a LHS model because the boundary between criteria (52) and (45) is below the purple curve. The line intersects the curve upper bounding the blue region at $(\alpha, \eta_B) \approx (0.37, 0.74)$.

1. *No noise on Bob's side (i.e., the trusted side)*

Firstly, if $\eta_B = 1$, $\frac{\mathrm{d}}{\mathrm{d}\theta}\tilde{\rho}_B^{\alpha,\eta_A,1}(\theta)$ is identical to that in (75), and the tilt of the steering ellipse of $\rho_{AB}(\alpha, \eta_A, 1)$ is $\cos(2\alpha) \leq 1$, so we obtain the same result.

2. *The maximally entangled case*

Secondly, if $\alpha = \frac{\pi}{4}$, the situation is exactly the same as for a Werner state with $\eta = \eta_A\eta_B$. In other words, $\eta_A\eta_B \leq \frac{2}{\pi}$ is a necessary and sufficient condition for RP-unsteerability of a state of the form $\rho_{AB}(\pi/4, \eta_A, \eta_B)$.

3. *The general case*

We study this numerically, using similar techniques to before. The results are shown in Figure 4.

The left hand side of (52) becomes easier to satisfy for lower η_A and so the region of RP-unsteerability increases as η_A is lowered. In other words, if $\hat{\rho}_{AB}(\alpha, \eta_A, \eta_B)$ is RP-unsteerable, then so is $\hat{\rho}_{AB}(\alpha, \eta'_A, \eta_B)$ for $\eta'_A \leq \eta_A$. At $\eta_A = \frac{2}{\pi}$ the state is RP-unsteerable for all η_B and α.

Note that the regions shown in the above plot extend below the purple curve, although the condition on the tilt of the steering ellipse ceases to be satisfied there. To extend to this region we use the fact that more noise (lower η_B) makes a LHS model easier to construct. This is stated in the following lemma.

Lemma 17. *If $\hat{\rho}_{AB}(\alpha, \eta_A, \eta_B)$ has a LHS model (for any set of measurements), then so does $\hat{\rho}_{AB}(\alpha, \eta_A, \eta'_B)$ for all $\eta'_B < \eta_B$.*

Proof. This follows from Remark 3 and the fact that $\hat{\rho}_{AB}(\alpha, \eta_A, \eta'_B) = \frac{\eta'_B}{\eta_B}\hat{\rho}_{AB}(\alpha, \eta_A, \eta_B) + \frac{\eta_B - \eta'_B}{\eta_B}\hat{\rho}_A(\alpha, \eta_A, \eta_B) \otimes \mathbb{1}/2$, i.e., is a convex combination of $\hat{\rho}_{AB}(\alpha, \eta_A, \eta_B)$ and $\hat{\rho}_A(\alpha, \eta_A, \eta_B) \otimes \mathbb{1}/2$, both of which have LHS models. □

Hence, although we cannot use Theorem 9 throughout the α-η_B plane, we can nevertheless establish steerability of all states of the form $\hat{\rho}_{AB}(\alpha, 1, \eta_B)$ for $\alpha \gtrsim 0.37$ (for example). Furthermore, the numerics point to the existence of a critical value around 0.92 such that for values of η_A below this we can always use our criteria (graphically, the boundary of the region in which a LHS model exists always lies above $\eta_B = \cos(2\alpha)$ for $\eta_A \lesssim 0.92$).

Acknowledgments

We are grateful to Kim Winick for numerous helpful discussions. RC is supported by the EPSRC's Quantum Communications Hub (grant number EP/M013472/1) and by an EPSRC First Grant (grant number EP/P016588/1).

CAM and YS were supported by NSF grants 1500095 and 1526928.

Appendix A: Supplementary Proofs

1. A topological lemma

Lemma 18. *Let $D = \{z \in \mathbb{C} \mid |z| \leq 1\}$ and let $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$. Let $F\colon D \to D$ be a continuous function such that for any $z \in S^1$, $F(z) = -z$. Then, F is onto.*

Proof. Suppose, for the sake of contradiction, that $y \in D \setminus F(D)$. Let $G\colon D \to S^1$ be the (unique) function defined by the condition that for any $z \in D$, $F(z)$ lies on the line segment from y to $G(z)$. Note that the function G also fixes S^1. The family of functions $\left\{H_\alpha\colon S^1 \to S^1 \mid \alpha \in [0,1]\right\}$ given by $H_\alpha(z) = G(\alpha z)$ is a continuous deformation between the negation map on S^1 and the constant map which takes S^1 to $G(0)$. This is impossible, since these maps represent different elements of the fundamental group of S^1. Thus, by contradiction, the original map F must be onto. □

2. Integrals with denominator $\sqrt{x^2+y^2}$

Proposition 19. *Let a be a positive real number. Let $F\colon [-a,a]^2 \to \mathbb{R}$ be a continuous function such that $|F(x,y) - F(0,0)| \leq O(\sqrt{x^2+y^2})$. Then,*

$$\lim_{y \to 0} \frac{\int_{-a}^{a} [F(x,y)/\sqrt{x^2+y^2}]dx}{\ln(1/y^2)} \;=\; F(0,0). \tag{A1}$$

Proof. We have $F(0,0) - C\sqrt{x^2+y^2} \leq F(x,y) \leq F(0,0) + C\sqrt{x^2+y^2}$ for some $C > 0$. Thus,

$$\begin{aligned}
\int_{-a}^{a} [F(x,y)/\sqrt{x^2+y^2}]dx \;&\leq\; \int_{-a}^{a} [F(0,0)/\sqrt{x^2+y^2}]dx + 2aC && \text{(A2)}\\
&=\; F(0,0)\left[\ln\left|\sqrt{x^2+y^2}+x\right|\right]_{x=-a}^{x=a} + 2aC && \text{(A3)}\\
&=\; F(0,0)\ln\left(\frac{\sqrt{a^2+y^2}+a}{\sqrt{a^2+y^2}-a}\right) + 2aC && \text{(A4)}\\
&=\; F(0,0)\ln\left(\frac{(\sqrt{a^2+y^2}+a)^2}{y^2}\right) + 2aC && \text{(A5)}\\
&=\; F(0,0)\ln(1/y^2) + 2F(0,0)\ln\left(\sqrt{a^2+y^2}+a\right) + 2aC && \text{(A6)}
\end{aligned}$$

The second and third summands in (A6) are both $o(\ln(1/y^2))$ — in fact, they both tend to constants, since $\lim_{y\to 0}\ln\left(\sqrt{a^2+y^2}+a\right) = \ln(2a) < \infty$. Thus

$$\lim_{y \to 0} \frac{\int_{-a}^{a} [F(x,y)/\sqrt{x^2+y^2}]dx}{\ln(1/y^2)} \;\leq\; F(0,0). \tag{A7}$$

Similar reasoning shows the reverse inequality. □

Next we state some generalizations of the above proposition.

Proposition 20. *Let $U \subseteq \mathbb{R}^2$ be a compact region that contains $(0,0)$ in its interior. Let $F\colon U \to \mathbb{R}$ be a continuous function such that $|F(x,y) - F(0,0)| \leq O(\sqrt{x^2+y^2})$. Then,*

$$\lim_{y \to 0} \frac{\int_{\{x \mid (x,y) \in U\}} [F(x,y)/\sqrt{x^2+y^2}]dx}{\ln(1/y^2)} \;=\; F(0,0). \tag{A8}$$

Proof. Choose a sufficiently small that $[-a,a] \subseteq U$. Since $\int_{U \setminus [-a,a]} |F(x,y)|/\sqrt{x^2+y^2} < \infty$, replacing U with $[-a,a]$ in (A8) has no effect on the resulting limit. □

For any differentiable function $H\colon \mathbb{R}^n \to \mathbb{R}^n$, let $\mathrm{Jac}(H) = [\partial H_i/\partial x_j]_{ij}$ denote the Jacobian of H.

Corollary 21. *Let $U \subseteq \mathbb{R}^2$ be a compact region that contains $(0,0)$ in its interior, and let $F\colon U \to \mathbb{R}$ be a continuous function such that $|F(x,y) - F(0,0)| \leq O(\sqrt{x^2+y^2})$. Let $G\colon U \to \mathbb{R}^2$ be a twice-differentiable function such that $Jac(G)(0,0) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and $G^{-1}(0,0) = \{(0,0)\}$. Then,*

$$\lim_{y \to 0} \frac{\int_{\{x \mid (x,y) \in U\}} [F(x,y)/\left|G(x,y)\right|]dx}{\ln(1/y^2)} = F(0,0). \tag{A9}$$

Proof. Let

$$g(x,y) = \begin{cases} \left|G(x,y)\right| / \left|\sqrt{x^2+y^2}\right| & \text{if } (x,y) \neq (0,0) \\ 1 & \text{if } (x,y) = (0,0) \end{cases} \tag{A10}$$

Let $I\colon \mathbb{R}^2 \to \mathbb{R}^2$ be the identity map. By assumption, $|G - I| \leq O(|I|^2)$, and thus

$$\begin{aligned} \left| \frac{|G(x,y)|}{\left|\sqrt{x^2+y^2}\right|} - 1 \right| &= \left| \frac{|G|}{|I|} - 1 \right| && \text{(A11)} \\ &\leq O(|I|) && \text{(A12)} \\ &= O(\sqrt{x^2+y^2}). && \text{(A13)} \end{aligned}$$

Therefore, $|g(x,y) - g(0,0)| \leq O(\sqrt{x^2+y^2})$, and likewise if we let $\overline{F}(x,y) = F(x,y)/g(x,y)$, we have $\left|\overline{F}(x,y) - F(0,0)\right| \leq O(\sqrt{x^2+y^2})$. Applying Proposition 20 with the function $F(x,y)$ replaced by $\overline{F}(x,y)$ yields the result. □

The next corollary follows easily by change of coordinates.

Corollary 22. *Let $U \subseteq \mathbb{R}^2$ be a compact region that contains $(0,0)$ in its interior, and let $F\colon U \to \mathbb{R}$ be a continuous function such that $|F(x,y) - F(0,0)| \leq O(\sqrt{x^2+y^2})$. Let $G\colon U \to \mathbb{R}^2$ be a twice-differentiable function such that $Jac(G)(0,0)$ is invertible, and $G^{-1}(0,0) = \{(0,0)\}$. Then,*

$$\lim_{y \to 0} \frac{\int_{\{x \mid (x,y) \in U\}} [F(x,y)/\left|G(x,y)\right|]dx}{\ln(1/y^2)} = \frac{F(0,0)}{\left|\frac{\partial G}{\partial x}(0,0)\right|}. \quad \square \tag{A14}$$

3. Formulas for the absolute value of a 2×2 matrix

The following propositions address the asymptotic behavior of the modified absolute value function. In all of the following, ϵ denotes a real parameter from the interval $(0,1]$.

If $\epsilon \in (0,1]$, let

$$D_\epsilon = \begin{bmatrix} 1 & \\ & \epsilon \end{bmatrix}. \tag{A15}$$

If $X = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$, then let $\Delta(X) = (x_1 - x_2)^2$, where x_1, x_2 denote the eigenvalues of X. (This is the discriminant of X.)

Proposition 23. *Let $X = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$. Then, the discriminant $\Delta = \Delta(X)$ is given by*

$$\Delta = (a-c)^2 + 4b^2. \tag{A16}$$

The tilt of X is equal to

$$\mathrm{Tilt}(X) = \frac{\sqrt{\Delta}}{a+c}. \tag{A17}$$

If X is positive semidefinite, then $|X| = |X|_+ = X$ and $|X|_- = 0$. If X is negative semidefinite, then $|X| = |X|_- = -X$ and $|X|_+ = 0$. If X is neither positive semidefinite nor negative semidefinite, then an orthogonal rank-one decomposition for X is given by

$$\begin{aligned} X &= \left[\begin{pmatrix} (a-c)+\sqrt{\Delta} & 2b \\ 2b & (c-a)+\sqrt{\Delta} \end{pmatrix}\right]\left(\frac{a+c+\sqrt{\Delta}}{4\sqrt{\Delta}}\right) \\ &\quad + \left[\begin{pmatrix} (c-a)+\sqrt{\Delta} & -2b \\ -2b & (a-c)+\sqrt{\Delta} \end{pmatrix}\right]\left(\frac{a+c-\sqrt{\Delta}}{4\sqrt{\Delta}}\right), \end{aligned} \tag{A18}$$

(The above expression can be used easily to express $|X|_+, |X|_-$, and $|X|$.) If X is neither positive semidefinite nor negative semidefinite, the following formula holds:

$$|X| = \left[\begin{pmatrix} a^2-ac+2b^2 & ab+ac \\ ab+ac & c^2-ac+2b^2 \end{pmatrix}\right]\left(\frac{1}{\sqrt{\Delta}}\right) \tag{A19}$$

Proof. If we let x_1, x_2 denote the eigenvalues of X, then

$$\begin{aligned} \Delta &= (x_1-x_2)^2 && \text{(A20)} \\ &= (x_1+x_2)^2 - 4x_1x_2 && \text{(A21)} \\ &= \mathrm{Tr}(X)^2 - 4\det(X) && \text{(A22)} \\ &= (a+c)^2 - 4(ac-b^2), && \text{(A23)} \end{aligned}$$

which is easily transformed into (A16). For (A18), it is easy to check by direct computation that the difference between the two summands is equal to X, that the summands are of rank one and orthogonal.

We obtain (A19) from (A18). Exactly one of the terms in (A18) is positive semidefinite; suppose that it is the first term. Then,

$$\begin{aligned} |X| &= \left[\begin{pmatrix} (a-c)+\sqrt{\Delta} & 2b \\ 2b & (c-a)+\sqrt{\Delta} \end{pmatrix}\right]\left(\frac{a+c+\sqrt{\Delta}}{4\sqrt{\Delta}}\right) \\ &\quad - \left[\begin{pmatrix} (c-a)+\sqrt{\Delta} & -2b \\ -2b & (a-c)+\sqrt{\Delta} \end{pmatrix}\right]\left(\frac{a+c-\sqrt{\Delta}}{4\sqrt{\Delta}}\right), \end{aligned} \tag{A24}$$

Multiplying the numerators of the fractions in (A24) into the respective matrices, and performing cancellations,

$$\begin{aligned} \left|\left[\begin{pmatrix} a & b \\ b & c \end{pmatrix}\right]\right| &= \left[\begin{pmatrix} 2a^2-2c^2+2\Delta & 4b(a+c) \\ 4b(a+c) & -2a^2+2c^2+2\Delta \end{pmatrix}\right]\left(\frac{1}{4\sqrt{\Delta}}\right) && \text{(A25)} \\ &= \left[\begin{pmatrix} 2a^2-2c^2+2[(a-c)^2+4b^2] & 4b(a+c) \\ 4b(a+c) & -2a^2+2c^2+2[(a-c)^2+4b^2] \end{pmatrix}\right]\left(\frac{1}{4\sqrt{\Delta}}\right) && \text{(A26)} \\ &= \left[\begin{pmatrix} a^2-c^2+[(a-c)^2+4b^2] & 2b(a+c) \\ 2b(a+c) & -a^2+c^2+[(a-c)^2+4b^2] \end{pmatrix}\right]\left(\frac{1}{2\sqrt{\Delta}}\right) && \text{(A27)} \\ &= \left[\begin{pmatrix} 2a^2-2ac+4b^2 & 2ab+2ac \\ 2ab+2ac & 2c^2-2ac+4b^2 \end{pmatrix}\right]\left(\frac{1}{2\sqrt{\Delta}}\right) && \text{(A28)} \\ &= \left[\begin{pmatrix} a^2-ac+2b^2 & ab+ac \\ ab+ac & c^2-ac+2b^2 \end{pmatrix}\right]\left(\frac{1}{\sqrt{\Delta}}\right) && \text{(A29)} \end{aligned}$$

as desired. □

We wish to understand how the function

$$\epsilon \mapsto |X|_{D_\epsilon} \tag{A30}$$

varies as $\epsilon \to 0$. If $X \geq 0$ or $X \leq 0$, this is easy: the function is constant and is equal to $|X|$. Thus we focus on the case where X is neither positive semidefinite nor negative semidefinite.

By substitution,

$$\left|\left|\begin{bmatrix}1 & 0\\ 0 & \epsilon\end{bmatrix}\begin{bmatrix}a & b\\ b & c\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & \epsilon\end{bmatrix}\right|\right| = \left|\left|\begin{bmatrix}a & \epsilon b\\ \epsilon b & \epsilon^2 c\end{bmatrix}\right|\right| \tag{A31}$$

$$= \left(\begin{bmatrix}a^2 - \epsilon^2 ac + 2\epsilon^2 b^2 & \epsilon ab + \epsilon^2 ac\\ \epsilon ab + \epsilon^2 ac & \epsilon^4 c^2 - \epsilon^2 ac + 2\epsilon^2 b^2\end{bmatrix} \frac{1}{\sqrt{(a-\epsilon^2 c)^2 + 4\epsilon^2 b^2}}\right) \tag{A32}$$

Multiplying the above equation on both the left and the right by $(D_\epsilon)^{-1}$, we obtain the following proposition.

Proposition 24. *Let* $X = \begin{bmatrix}a & b\\ b & c\end{bmatrix}$ *and* $\epsilon \in (0,1]$. *Then,*

$$\left|\left|\begin{bmatrix}a & b\\ b & c\end{bmatrix}\right|\right|_{D_\epsilon} = \left(\begin{bmatrix}a^2 - \epsilon^2 ac + 2\epsilon^2 b^2 & ab + \epsilon ac\\ ab + \epsilon ac & \epsilon^2 c^2 - ac + 2b^2\end{bmatrix} \frac{1}{\sqrt{(a-\epsilon^2 c)^2 + 4\epsilon^2 b^2}}\right). \tag{A33}$$

4. The steering ellipse of a two-qubit state

We now integrate the results from the previous subsections. Assume, as in the main text, that ρ_{AB} is a two-qubit state and that its steering ellipse $\{\tilde{\rho}_B(\theta) \mid \theta \in \mathbb{R}\}$ has tilt less than 1. Define functions $a, b, c \colon \mathbb{R} \to \mathbb{R}$ so that

$$\frac{d}{d\theta}\tilde{\rho}_B(\theta) = \begin{bmatrix}a(\theta) & b(\theta)\\ b(\theta) & c(\theta)\end{bmatrix} \tag{A34}$$

Let

$$F(\theta,\epsilon) = \begin{bmatrix}a^2 - \epsilon^2 ac + 2\epsilon^2 b^2 & ab + \epsilon ac\\ ab + \epsilon ac & \epsilon^2 c^2 - ac + 2b^2\end{bmatrix} \tag{A35}$$

and

$$G(\theta,\epsilon) = (a - \epsilon^2 c, 2\epsilon b) \tag{A36}$$

The function $a \colon \mathbb{R} \to \mathbb{R}$ is a sinusoidal function with period 2π. There are two values of $\theta \in [0, 2\pi)$ at which $a = 0$. By changing of coordinates if necessary, we can assume that these two values are θ_0 and $\theta_0 + \pi$, where $\theta_0 \in (0,\pi)$. Then, using Proposition 24,

$$\lim_{\epsilon\to 0}\frac{\int_0^\pi \left|\frac{d}{d\theta}\rho_B(\theta)\right|_{D_\epsilon} d\theta}{\ln(1/\epsilon)} = \lim_{\epsilon\to 0}\frac{\int_0^\pi [F(\theta_0,\epsilon)/\left|G(\theta,\epsilon)\right|]d\theta}{\ln(1/\epsilon)} \tag{A37}$$

$$= \frac{F(\theta_0, 0)}{\frac{\partial}{\partial\theta}\left|G(\theta,\epsilon)\right|(\theta_0,0)} \tag{A38}$$

$$= \frac{\begin{bmatrix}0 & 0\\ 0 & 2(b(\theta_0))^2\end{bmatrix}}{a'(\theta_0)} \tag{A39}$$

$$= \begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}\frac{2(b(\theta_0))^2}{a'(\theta_0)}, \tag{A40}$$

and similarly,

$$\lim_{\epsilon\to 0}\frac{\int_\pi^{2\pi} \left|\frac{d}{d\theta}\rho_B(\theta)\right|_{D_\epsilon} d\theta}{\ln(1/\epsilon)} = \begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}\frac{2(b(\theta_0))^2}{a'(\theta_0)}. \tag{A41}$$

We thus have the following:

Proposition 25. *Let ρ_{AB} denote a real two-qubit state whose steering ellipse has tilt < 1, and define a, b, c by (A34). Then,*

$$\lim_{\epsilon\to 0}\frac{\int_0^{2\pi} \left|\frac{d}{d\theta}\rho_B(\theta)\right|_{D_\epsilon} d\theta}{\ln(1/\epsilon)} = \begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}\frac{4(b(\theta_0))^2}{a'(\theta_0)} \tag{A42}$$

The following corollary is immediate by change of basis.

Corollary 26. *Let ρ_{AB} denote a real two-qubit state whose steering ellipse has tilt < 1. Let $\{v, w\}$ be an orthonormal basis for $\mathbb{R}^2$, and let $D_{\epsilon,v} = |v\rangle\langle v| + \epsilon|w\rangle\langle w|$. Then, the limit*

$$\lim_{\epsilon\to 0} \frac{\int_0^{2\pi} \left| \frac{d}{d\theta}\rho_B(\theta)\right|_{D_{\epsilon,v}} d\theta}{\ln(1/\epsilon)} \tag{A43}$$

converges and is equal to a positive scalar multiple of $|w\rangle\langle w|$.

[1] Bell, J. S. On the Einstein-Podolsky-Rosen paradox. In *Speakable and unspeakable in quantum mechanics*, chap. 2 (Cambridge University Press, 1987).

[2] Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, 503–509 (1998).

[3] Wiseman, H. M., Jones, S. J. & Doherty, A. C. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.* **98**, 140402 (2007). URL `http://link.aps.org/doi/10.1103/PhysRevLett.98.140402`.

[4] Branciard, C., Cavalcanti, E. G., Walborn, S. P., Scarani, V. & Wiseman, H. M. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A* **85**, 010301 (2012). URL `https://link.aps.org/doi/10.1103/PhysRevA.85.010301`.

[5] Piani, M. & Watrous, J. Necessary and sufficient quantum information characterization of einstein-podolsky-rosen steering. *Phys. Rev. Lett.* **114**, 060404 (2015). URL `https://link.aps.org/doi/10.1103/PhysRevLett.114.060404`.

[6] Jevtic, S., Hall, M. J. W., Anderson, M. R., Zwierz, M. & Wiseman, H. M. Einstein–Podolsky–Rosen steering and the steering ellipsoid. *J. Opt. Soc. Am. B* **32**, A40–A49 (2015). URL `http://josab.osa.org/abstract.cfm?URI=josab-32-4-A40`.

[7] Nguyen, H. C. & Vu, T. Necessary and sufficient condition for steerability of two-qubit states by the geometry of steering outcomes. arXiv:1604.03815 (2016).

[8] Werner, R. F. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A* **40**, 4277–4281 (2006).

[9] Acín, A., Gisin, N. & Toner, B. Grothendieck's constant and local models for noisy entangled quantum states. *Phys. Rev. A* **73**, 062105 (2006).

[10] Grothendieck, A. Résumé de la théorie métrique des produits tensoriels topologiques. *Bol. Soc. Mat. São Paulo* **8**, 1–79 (1953).

[11] Barrett, J. Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality. *Phys. Rev. A* **65**, 042302 (2002).

[12] Quintino, M. T. *et al.* Inequivalence of entanglement, steering, and Bell nonlocality for general measurements. *Phys. Rev. A* **92**, 032107 (2015).