Keyring models: an approach to steerability

Carl A. Miller,[1,2] Roger Colbeck,[3] and Yaoyun Shi[4]

[1] *National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899, USA*
[2] *Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD 20742, USA**
[3] *Department of Mathematics, University of York, York, YO10 5DD, UK*†
[4] *Aliyun Quantum Laboratory, Alibaba USA, Bellevue, WA 98004, USA*‡

(Dated: 18th December 2017)

If a measurement is made on one half of a bipartite system then, conditioned on the outcome, the other half has 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*. Determining which states are steerable is a challenging problem even for low dimensions. In the case of two-qubit systems a criterion is known for T-states (that is, those with maximally mixed marginals) under projective measurements. In the current work we introduce the concept of *keyring models* — a special class of local hidden state model. When the measurements made correspond to real projectors, these allow us to study steerability beyond T-states.

Using keyring models, we completely solve the steering problem for real projective measurements when the state arises from mixing a pure two-qubit state with uniform noise. We also give a partial solution in the case when the uniform noise is replaced by independent depolarizing channels.

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 input $q \in \mathcal{Q}$ and Bob is given a private input $s \in \mathcal{S}$, 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 $\mathbf{P}(ab \mid qs)$ 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 cryptographic tasks and at the same time verify their security [2, 3].

In 2007, the related notion of quantum steering was distilled [4], in which, rather than having Bob make a measurement, we directly consider the subnormalized marginal states $\tilde{\rho}_B^{q,a}$ that he holds when Alice receives input q and produces output a. A local hidden state (LHS) model attempts to generate these using shared randomness. Denoting the shared randomness by a random variable λ, distributed according to probability distribution $\mu(\lambda)$, Bob can output quantum state σ_λ, while Alice outputs a according to a probability distribution $\mathbf{P}_{q,\lambda}(a)$.

Suppose when Alice gets input q she performs a POVM $\{E_a^q\}_{a\in\mathcal{A}}$, so that $\tilde{\rho}_B^{q,a} = \mathrm{Tr}_A((E_a^q \otimes \mathbb{I}_B)\rho_{AB})$. A LHS model produces a faithful simulation if $\tilde{\rho}_B^{q,a} = \int_\lambda \mathbf{P}_{q,\lambda}(a)\sigma_\lambda \, \mathrm{d}\mu(\lambda)$ for all q and a. If such a model exists, then we say that the state ρ_{AB} is unsteerable for the family of measurements $\{\{E_a^q\}_{a\in\mathcal{A}}\}_{q\in\mathcal{Q}}$. If a LHS model exists for all possible measurements Alice could do (i.e., all POVMs), we say ρ_{AB} is unsteerable. Conversely, if there exists a set of measurements for which no LHS model exists, then ρ_{AB} is said to be steerable.

One can think of steering as an analog of non-locality for the case where one party (Bob) trusts his 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 [5] and (sub)channel discrimination [6]. 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: y.shi@alibaba-inc.com

The steering decision problem is to determine whether or not a given state is steerable. This problem has proved to be difficult even for 2-qubit systems. To understand why this is so, consider a two-qubit state ρ_{AB}. If Alice were to measure $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ on input $q = 0$ and $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ on input $q = 1$ (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, $\tilde{\rho}_B^0 = \mathrm{Tr}_A[(|0\rangle\langle 0| \otimes \mathbb{I}_B)\rho]$). Determining whether a LHS model exists for these four states is a search over a finite-dimensional space and is not difficult (see [7, 8] for techniques for searching for LHS models). Next suppose Alice additionally performs the measurement $\{|\pi/4\rangle\langle\pi/4|, |5\pi/4\rangle\langle 5\pi/4|\}$ for input $q = 2$, 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 has achieved success by exploiting the symmetries of certain classes of states. For the class of Werner states [9] $\{\rho_{AB}(\eta) \mid \eta \in [0,1]\}$ given by

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

where $|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, an exact classification of P-steerability (i.e., steerability for all projective measurements) has been performed (see Appendix A 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 and ρ_B are maximally mixed) has been given [10–12]. [Note that the requirement on ρ_B can be dropped due to Lemma 16.] In both cases the methods depend critically on the symmetry of the states. For 2-qubit states outside the family of T-states, partial results on steerability exist (e.g., [13, 14]) but a full classification is not known.

In the current work, we develop new techniques to decide steerability in the case where ρ_A is not maximally mixed. We study Real Projective (RP)-steerability (i.e., steerability by the family of all measurements of the form $\{|\theta\rangle\langle\theta|, |\theta+\pi\rangle\langle\theta+\pi|\}$) for real two-qubit states. [A state is *real* if its matrix elements are real in the $\{|0\rangle, |1\rangle\}$ basis.] To illustrate our techniques, we give a complete classification of RP-steerability for the class of states, $\{\rho_{AB}(\alpha,\eta)\}$, formed by mixing partially entangled pure states with uniform noise, i.e.,

$$\rho_{AB}(\alpha,\eta) = \eta|\phi_\alpha\rangle\langle\phi_\alpha| + (1-\eta)\mathbb{I}/4\,, \tag{3}$$

where $|\phi_\alpha\rangle = \cos\alpha|00\rangle + \sin\alpha|11\rangle$. The classification is shown in Figure 1, where the shaded/unshaded region represents the states that are unsteerable/steerable for real projective measurements. As a special case we recover the existing result [15, 16] that Werner states are RP-steerable if and only if $\eta > 2/\pi$ (see Theorem 17).

Our criterion 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 14 and Corollary 15 for the formal statements. To achieve this classification we introduce the concept of *keyring models*, which are a geometrically motivated class of local hidden state models for one-dimensional families of measurements. We explain these in more detail in the next subsection.

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 go further identify the set of all *RP*-steerable real 2-qubit states. Additionally, the keyring 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 for experimental setups in which measurements in one plane of the Bloch sphere are easier than the most general measurements. 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 arbitrary 2-qubit states.

Keyring models can also be used to construct a class of LHV models if we also consider a (classical) function on Bob's side that maps his input and the hidden state to his output. They can hence be applied to the related problem of classically simulating bipartite correlations and may, for example, be useful for shedding new light on the problem of identifying the smallest detector efficiency for observing Bell inequality violations. We hope to find further applications of keyring models in this direction.

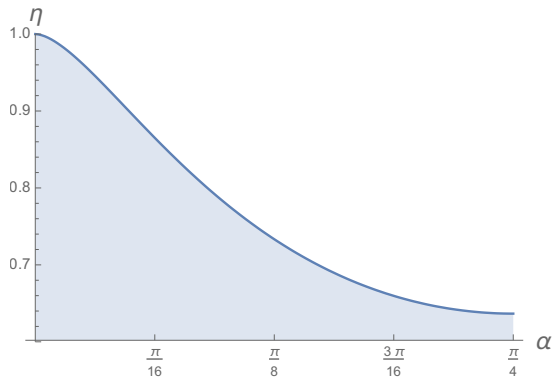


FIG. 1: *RP*-unsteerability for the states $\rho_{AB}(\alpha, \eta)$. In the shaded region the states are unsteerable under real projective measurements, while above it they are steerable. (Note that the shaded region extends to $\eta = 0$.)

A. Sketch of the proof techniques

The difficulty in establishing steerability over all measurements is the need to rule out *all* LHS models. Our proof begins with the observation that, in the case where ρ_{AB} is a real 2-qubit state and where the set of measurements comprises real projective measurements (i.e., those of the form $\{|\theta\rangle\langle\theta|, |\theta + \pi\rangle\langle\theta + \pi|\}$), a more tractable (though still infinite dimensional) class of LHS models suffices. Specifically, we consider a class of LHS models that we call "keyring models", which we now define.

Let $\mathbb{RP}^1$ denote the set of all real one-dimensional projectors on $\mathbb{C}^2$ (i.e., the set $\{|\theta\rangle\langle\theta|\}_{\theta\in[0,2\pi)}$). A keyring model is a pair $(\mu, \{f_\theta\}_\theta)$, where μ is a probability distribution on $\mathbb{RP}^1$, and $f_\theta \colon \mathbb{RP}^1 \to [0, 1]$ is a two-step function – that is, roughly speaking, a function that is constant at all but two elements of $\mathbb{RP}^1$ (see Definition 4). The word "keyring" refers to the configuration of the two nonconstant points on $\mathbb{RP}^1$ as θ varies. An example configuration is shown in Figure 2. (This definition is related to the local hidden state models of [10–12, 15], which are based on functions on $\mathbb{RP}^2$ that are supported on half-spheres. One key difference in the definition of a keyring model is that there is no uniformity in the positioning of the nonconstant points of the functions f_θ — they need not be diametrically opposite.)

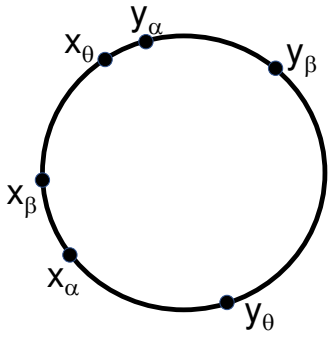


FIG. 2: An example configuration of endpoints in a keyring distribution. For every point in $\mathbb{RP}^1$ there are two associated endpoints in $\mathbb{RP}^1$. Here three pairs of endpoints are illustrated with (x_α, y_α) being the end points for α, for example.

We show that ρ_{AB} is RP-steerable if and only if it can be simulated by a keyring model. Denoting the subnormalized reduced states on Bob's side by $\tilde{\rho}_B(\theta) = \mathrm{Tr}_A\left((|\theta\rangle\langle\theta| \otimes \mathbb{I}_B)\rho_{AB}\right)$, this is equivalent to the requirement

$$\tilde{\rho}_B(\theta) \;=\; \int_{x\in\mathbb{RP}^1} x f_\theta(x)\, \mathrm{d}\mu \tag{4}$$

for all θ. From this we can conclude that that if the circumference of the steering ellipse $\{\tilde{\rho}_B(\theta)\}$ is greater than 2, i.e.,

$$\int_{\mathbb{RP}^1} \left\| \frac{\mathrm{d}}{\mathrm{d}\theta} \tilde{\rho}_B(\theta) \right\|_1 \mathrm{d}\theta \;>\; 2, \tag{5}$$

where $\|\cdot\|_1$ is the trace norm, then the state ρ_{AB} has no local hidden state model (see Proposition 6).

At this point our proof diverges from that of [10–12, 15], since the converse of the above statement is not true in our case: if (5) fails to hold, there could still be no local hidden state model. However, the following stronger condition guarantees the existence of a local hidden state model:

$$\int_{\mathbb{RP}^1} \left| \frac{\mathrm{d}}{\mathrm{d}\theta} \tilde{\rho}_B(\theta) \right| \mathrm{d}\theta \;\leq\; 2\rho_B, \tag{6}$$

where $|X| = \sqrt{X^\dagger X}$ is the absolute value of the operator. Moreover, the state ρ_{AB} is steerable if and only if

$$\rho'_{AB} := (\mathbb{I}_A \otimes Y)\rho_{AB}(\mathbb{I}_A \otimes Y) \tag{7}$$

is steerable for all positive definite Y (see Lemma 16), and by substituting in ρ'_{AB} for ρ_{AB} in (5) and (6) we obtain an infinite family of criterion for RP-steerability and RP-unsteerability. We thus need to find a Y such that one of (5) and (6) 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

$$Y^{-1} \left[\int_{\mathbb{RP}^1} \left| Y \left(\frac{\mathrm{d}}{\mathrm{d}\theta} \tilde{\rho}_B(\theta) \right) Y \right| \mathrm{d}\theta \right] Y^{-1} \tag{8}$$

is a scalar multiple of ρ_B. This compels (8) 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 $\mathbb{RP}^1$, then (8) must tend to an operator proportional to the orthogonal projector $\widehat{P}$. Any continuous 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 – it turns out that the rate at which the normalization of (8) approaches $\widehat{P}$ is only logarithmic.)

Theorem 14 gives a formal statement of our main result. To apply the criteria (e.g., to obtain Figure 1), we use numerical computations to find the appropriate operators Y from a given state ρ_{AB}.

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 $\langle i|X|j\rangle \in \mathbb{R}$ for all i, j, where $\{|i\rangle\}$ is the standard basis). If $A, B \in \mathcal{P}_{\geq}(\mathcal{H})$ we write $A \geq B$ to mean that $A - B \in \mathcal{P}_{\geq}(\mathcal{H})$ and $A \ngeq B$ for the complement of this. 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. If $\mathrm{Tr}(X) \neq 0$, we use $\langle X\rangle$ to denote the normalized version of X, i.e., $\langle X\rangle := X/\mathrm{Tr}(X)$. In addition, if Y is also an operator on $\mathcal{H}$, then we use $\langle X, Y\rangle := \mathrm{Tr}(X^\dagger Y)$.

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

1. *The steering ellipse*

Any operator $\lambda \in \mathcal{RA}(\mathbb{C}^2)$ can be expressed uniquely in terms of real numbers n, r_1, r_3 as

$$\lambda = \frac{1}{2}(n\mathbb{I} + r_1\sigma_1 + r_3\sigma_3)\,, \tag{9}$$

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. Note that $\lambda \in \mathbb{RP}^1$ if and only if $n = 1$ and $r_1^2 + r_3^2 = 1$.

The *tilt* of λ, denoted $\mathrm{Tilt}(\lambda)$, is the quantity $\sqrt{r_1^2 + r_3^2}/|n|$ (if $n = 0$, the tilt is ∞). 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 use these coordinates when we sketch steering ellipses later in this work. Note that an operator is positive semidefinite if and only if $n \geq 0$ and its tilt is less than or equal to 1. It is useful to note that

$$\|\lambda\|_1 = \begin{cases} |n| & \text{if } \mathrm{Tilt}(\lambda) \leq 1 \\ \sqrt{r_1^2 + r_3^2} & \text{if } \mathrm{Tilt}(\lambda) > 1 \end{cases} \tag{10}$$

Let $\rho_{AB} \in \mathcal{RD}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. 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

$$\tilde{\rho}_B(\theta) \;:=\; \mathrm{Tr}_A \left[(|\theta\rangle\langle\theta| \otimes \mathbb{I}_B)\, \rho_{AB} \right] , \tag{11}$$

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. Note also that the term "steering ellipsoid" is used to refer to the set of normalized states in the literature [10, 17], while our steering ellipse comprises subnormalized states).

Definition 1. Let $\rho_{AB} \in \mathcal{RD}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. 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}. [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 ∞.]

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. This is a consequence of Lemma 20 in the appendix.

2. Local hidden state models

In this section we give a definition of a local hidden state model. It is not the most general definition possible, but it suffices for our purposes because of the form of the steering problem we are considering, as we first explain.

In the most general sense, a local hidden state model for a set of real 2-qubit subnormalized states $\{\tilde{\rho}_B^{q,a}\}_{q \in \mathcal{Q}, a \in \mathcal{A}}$ is a probability distribution μ on $\mathcal{D}(\mathbb{C}^2)$ and set of functions $\left\{ f_{q,a} \colon \mathcal{D}(\mathbb{C}^2) \to [0,1] \right\}_{q,a}$ with $\sum_{a \in \mathcal{A}} f_{q,a}(x) = 1$ such that

$$\tilde{\rho}_B^{q,a} \;=\; \int_{x \in \mathcal{D}(\mathbb{C}^2)} x f_{q,a}(x)\, \mathrm{d}\mu \,. \tag{12}$$

(To connect with the earlier description, $f_{q,a}(x)$ is the probability that Alice gives the outcome a for measurement q when the hidden variable takes the value x.) 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 $\mu, f_{a,q}$ have support $\mathcal{RD}(\mathbb{C}^2)$, and by decomposing each operator in $\mathcal{RD}(\mathbb{C}^2)$ into a convex combination of one-dimensional projectors, we may further assume that $\mu, f_{q,a}$ have support $\mathbb{RP}^1$. We are thus led to the following definition.

Definition 2. A *local hidden state model* for a set $\{\tilde{\rho}_B^{q,a}\}_{q \in \mathcal{Q}, a \in \mathcal{A}} \subseteq \mathcal{RP}_{\geq}(\mathbb{C}^2)$ is a pair $(\mu, \{f_{q,a}\}_{q,a})$ such that μ is a probability distribution on $\mathbb{RP}^1$, $f_{q,a} \colon \mathbb{RP}^1 \to [0,1]$ with $\sum_{a \in \mathcal{A}} f_{q,a}(x) = 1$ for all q, and

$$\tilde{\rho}_B^{q,a} \;=\; \int_{x \in \mathbb{RP}^1} x f_{q,a}(x)\, \mathrm{d}\mu \,. \tag{13}$$

In the case of steering for real 2-qubit states under real projective measurements, it suffices to consider whether we can find $(\mu, \{f_\theta\}_\theta)$ with $f_\theta \colon \mathbb{RP}^1 \to [0,1]$ such that

$$\tilde{\rho}_B(\theta) = \int_{x \in \mathbb{RP}^1} x f_\theta(x)\, \mathrm{d}\mu \,. \tag{14}$$

(Here $f_\theta(x)$ is the probability that Alice gives the outcome corresponding to the first projector for the measurement $\{|\theta\rangle\langle\theta|, |\theta + \pi\rangle\langle\theta + \pi|\}$ when the hidden variable has value x.) If such a $(\mu, \{f_\theta\}_\theta)$ can be found, this constitutes a LHS model for the set $\{\tilde{\rho}_B(\theta)\}_{\theta \in [0, 2\pi)}$ and we say that ρ_{AB} is *RP-unsteerable*. Conversely, if no such model exists, we say that ρ_{AB} is *RP-steerable*.

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).

III. KEYRING MODELS

In this section we formalize the class of keyring models. We begin with some preliminary definitions. Drawing from [12], if μ is a probability distribution on $\mathbb{RP}^1$, let $\mathrm{Box}(\mu)$ denote the convex set of all operators of the form

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

where $f : \mathbb{RP}^1 \to [0,1]$. 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 $\frac{1}{2}(\mathbb{I} + r_1\sigma_1 + r_3\sigma_3) \leftrightarrow (r_1, r_3)$ 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 a *counterclockwise* sequence 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 $(x, y) = \mathbb{RP}^1 \setminus [y, x]$. Note that, as implied by the notation, $[x, y]$ is a closed set and (x, y) is open.

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

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

with $q \leq f(x) \leq 1-q$ and $q \leq f(y) \leq 1-q$. We refer to q as the *bias* of the function and to x, y as 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*.

A *keyring* model for a set $\{\sigma^a\}_a \subseteq \mathcal{RP}_{\geq}(\mathbb{C}^2)$ of subnormalized states is a local hidden state model $(\mu, \{f_a\})$ in which the functions are all two-step functions (see Figure 2). The next proposition, which is proven in Appendix B 1, shows that any set that has a local hidden state model also has a keyring model. Hence when considering our steering problem it suffices to restrict the set of local hidden state models to keyring models.

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

$$z = \int_{x\in\mathbb{RP}^1} x g(x)\ \mathrm{d}\mu, \tag{17}$$

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

Next we will use these 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:

$$\int_0^1 \left\| \frac{\mathrm{d}}{\mathrm{d}t} S(t) \right\|_1 \mathrm{d}t. \tag{18}$$

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

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

To prove Proposition 6, we first consider LHS models in which the distribution μ is supported on a finite set of points of $\mathbb{RP}^1$. Any probability distribution μ on $\mathbb{RP}^1$ can be approximated to an arbitrary degree of accuracy by a probability distribution which is supported on a finite set of points in the sense that for any $\epsilon > 0$ there exists a finitely supported distribution μ' such that for all two-step functions f we have

$$\left\| \int_{x\in\mathbb{RP}^1} x f(x)\ \mathrm{d}\mu - \int_{x\in\mathbb{RP}^1} x f(x)\ \mathrm{d}\mu' \right\|_1 \leq \epsilon\,.$$

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

Lemma 7. *Let μ be a probability distribution on $\mathbb{RP}^1$ with finite support such that $\int_{x\in\mathbb{RP}^1} x \, \mathrm{d}\mu = \rho$, and let $H \in \mathcal{RP}_>(\mathbb{C}^2)$. Then, the set*

$$\{M \in \mathrm{Box}(\mu) \mid \langle M, H\rangle = (1/2)\langle \rho, H\rangle\} \tag{19}$$

is enclosed by a curve of length ≤ 2.

This is proven in Appendix B 2.

Proof of Proposition 6. Let $(\mu, \{f_\theta\})$ be a keyring 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 less than 1 by assumption). Because it is normal to the ellipse, $\langle \tilde{\rho}_B(\theta), H\rangle = u$ (independent of θ). Choose a sequence $\mu_1, \mu_2, \ldots$ of probability distributions on $\mathbb{RP}^1$ with finite support which converges to μ. Then, due to Lemma 7 the sets

$$\{M \in \mathrm{Box}(\mu_i) \mid \langle M, H\rangle = (1/2)\langle \rho_B, H\rangle\}, \tag{20}$$

are each enclosed by some curve of circumference ≤ 2. They furthermore converge to the set

$$\{M \in \mathrm{Box}(\mu) \mid \langle M, H\rangle = (1/2)\langle \rho_B, H\rangle\}. \tag{21}$$

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

IV. THE STEERING OPERATOR

Proposition 6 gives a criterion for steerability that is sufficient but not necessary. In order to develop a criterion that is both necessary and sufficient, we will need to work not with the circumference of the steering ellipse, but with the following operator whose trace is equal to the circumference of the steering ellipse:

$$\int_0^{2\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\theta} \tilde{\rho}_B(\theta) \right| \mathrm{d}\theta. \tag{22}$$

It is easiest to work with cases in which (22) is a scalar multiple of ρ_B. Our goal in the current section is to show that for any 2-qubit state ρ_{AB} whose steering ellipse has tilt < 1, there is a $Y \in \mathcal{RD}_>(\mathbb{C}^2)$ such that the operator (22) for $\rho'_{AB} = (\mathbb{I}_A \otimes Y)\rho_{AB}(\mathbb{I}_A \otimes Y)$ is a scalar multiple of ρ'_B. This will enable the proof of our main result in Section V.

The first two subsections will contain technical preparations. First we prove a concentration result for a particular type of integral.

A. Integrals of the form $\int [F(x)/\sqrt{G(x)}] \, \mathrm{d}x$

Proposition 8. *Let $U \subset \mathbb{R}^n$ contain the origin in its interior, $F\colon U \to \mathcal{RP}_\geq(\mathbb{C}^2)$ be a continuous function such that $F(\mathbf{0}) \neq \mathbf{0}$ and let $G : U \to \mathbb{R}_{\geq 0}$ be twice differentiable with $G(\mathbf{x}) = 0$ if and only if $\mathbf{x} = \mathbf{0}$. Then,*

$$\lim_{(x_2,\ldots,x_n)\to\mathbf{0}} \left\langle \int_{-a}^{a} \frac{F(\mathbf{x})}{\sqrt{G(\mathbf{x})}} \, \mathrm{d}x_1 \right\rangle = \langle F(\mathbf{0})\rangle. \tag{23}$$

Proof. Since G is twice differentiable and $\mathbf{x} = \mathbf{0}$ is a minimum of G, we have $|G(\mathbf{x})| \leq C|\mathbf{x}|^2$ for some constant $C > 0$. Thus,

$$\int_{-a}^{a} \frac{\mathrm{d}x_1}{G(\mathbf{x})} \geq \frac{1}{C}\int_{-a}^{a} \frac{\mathrm{d}x_1}{\sqrt{x_1^2 + y^2}} \tag{24}$$

$$= \frac{1}{C}\log\left(\frac{\sqrt{a^2+y^2}+a}{\sqrt{a^2+y^2}-a}\right) \tag{25}$$

$$= \frac{1}{C}\left(\log(1/y^2) + 2\log(\sqrt{a^2+y^2}+a)\right), \tag{26}$$

where $y^2 = \sum_{i=2}^n x_i^2$. Since $y \to 0$ as $(x_2, \ldots, x_n) \to (0, \ldots, 0)$, this tends to ∞. On the other hand, for any $\delta \in (0, a)$,

$$\lim_{(x_2,\ldots,x_n)\to\mathbf{0}} \int_{[-a,a]\smallsetminus(-\delta,\delta)} \frac{\mathrm{d}x_1}{\sqrt{G(\mathbf{x})}} = \int_{[-a,a]\smallsetminus(-\delta,\delta)} \frac{\mathrm{d}x_1}{\sqrt{G(x_1,0,\ldots,0)}} < \infty, \tag{27}$$

since we assumed that $G(\mathbf{x})$ has only one zero. Thus as $(x_2, \ldots, x_n) \to \mathbf{0}$, the integral of $F(\mathbf{x})/\sqrt{G(\mathbf{x})}$ on $(-\delta, \delta)$ dominates the integral of the same quantity on $[-a, a] \smallsetminus (-\delta, \delta)$. The quantity on the left side of Equation (23) is therefore in the convex hull of $F((-\delta, \delta))$. Since this holds true for any $\delta > 0$, Equation (23) follows. □

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

Throughout this section, X and Y denote 2×2 real symmetric matrices. For any such matrix $Y = \begin{bmatrix} d & e \\ e & f \end{bmatrix}$, let $\widehat{Y} = \begin{bmatrix} f & -e \\ -e & d \end{bmatrix}$ denote the adjugate matrix. (The adjugate matrix has the same eigenspaces as Y, with the two eigenvalues interchanged.) Note that $Y\widehat{Y} = \det(Y)\mathbb{I}$.

Definition 9. If $X, Y \in \mathcal{RA}(\mathbb{C}^2)$ and Y is invertible, let

$$|X|_Y = Y^{-1}\,|YXY|\,Y^{-1}. \tag{28}$$

Note that if X is positive semidefinite, then its trace-norm and absolute value are easily computed: $\|X\|_1 = \mathrm{Tr}(X)$, and $|X| = X$. The next propositions compute these values in the case where X is neither positive semidefinite nor negative semidefinite.

Proposition 10. *If X is such that $X \not\geq 0$ and $X \not\leq 0$, then*

$$\|X\|_1 = \sqrt{\mathrm{Tr}(X^2 - X\widehat{X})} \tag{29}$$

$$|X| = \frac{X^2 - X\widehat{X}}{\|X\|_1}. \tag{30}$$

Proof. Direct computation. □

Proposition 11. *If X is such that $X \not\geq 0$ and $X \not\leq 0$, and Y is invertible, then*

$$|X|_Y = \frac{XY^2X - (\det X)\widehat{Y}^2}{\|YXY\|_1}. \tag{31}$$

Proof. See Appendix B 5. □

Note that $\|YXY\|_1^2$ is a polynomial in the entries of X and Y (via (29)) and is therefore infinitely differentiable as a function of X and Y.

C. The steering operator of a two-qubit state

We now apply the results from the previous subsections. Suppose, that 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 function $X\colon \mathbb{R} \to \mathcal{RA}(\mathbb{C}^2)$ so that

$$X(\theta) = \frac{\mathrm{d}}{\mathrm{d}\theta}\tilde{\rho}_B(\theta) = \mathrm{Tr}_A((D(\theta) \otimes \mathbb{I})\rho_{AB})\,, \tag{32}$$

where $D(\theta) = \frac{1}{2}(-\sin\theta|0\rangle\langle 0| + \cos\theta(|0\rangle\langle 1| + |1\rangle\langle 0|) + \sin\theta|1\rangle\langle 1|)$.

Note that because the steering ellipse $\{\tilde{\rho}_B(\theta)\}$ has tilt < 1, for every θ the operator $X(\theta)$ is neither positive semidefinite nor negative semidefinite (cf. Corollary 21).

Let $P \in \mathbb{RP}^1$. Let $Y\colon \mathbb{R}^2 \to \mathcal{RP}_{\geq}(\mathbb{C}^2)$ be given by

$$Y(r_1, r_3) = P + r_1\sigma_1 + r_3\sigma_3. \tag{33}$$

The function $\theta \mapsto \mathrm{Tr}(PX(\theta))$ varies sinusoidally and has exactly two zeros in $[0, 2\pi)$. Without loss of generality, we will assume that the zeros are $\theta = 0$ and $\theta = \pi$. We wish to compute

$$\lim_{(r_1,r_3)\to(0,0)} \left\langle \int_{-\pi/2}^{\pi/2} |X|_Y \, \mathrm{d}\theta \right\rangle \tag{34}$$

$$= \lim_{(r_1,r_3)\to(0,0)} \left\langle \int_{-\pi/2}^{\pi/2} \frac{XY^2X - (\det X)\widehat{Y}^2}{\sqrt{\|YXY\|_1^2}} \, \mathrm{d}\theta \right\rangle. \tag{35}$$

The function $\|PX(\theta)P\|_1^2 = (\mathrm{Tr}(PX(\theta)))^2$ on the interval $[-\pi/2, \pi/2]$ has a zero only at $\theta = 0$. By Proposition 8 (with $G(\theta, r_1, r_3) = \|YXY\|_1^2$ and $F(\theta, r_1, r_3)$ equal to the numerator of the integrand in (35)), we obtain the following:

$$\lim_{(r_1,r_3)\to(0,0)} \left\langle \int_{-\pi/2}^{\pi/2} |X|_Y \, \mathrm{d}\theta \right\rangle = \left\langle X(0)P^2X(0) - \det(X(0))\widehat{P}^2 \right\rangle \tag{36}$$

$$= \left\langle -2\det(X(0))\widehat{P}^2 \right\rangle \tag{37}$$

$$= \widehat{P}. \tag{38}$$

Exploiting symmetry, the same equality holds when we replace the upper and lower integral limits with $-\pi/2$ and $3\pi/2$ (or equivalently, with 0 and 2π). We therefore have the following.

Theorem 12. *Let ρ_{AB} be a two-qubit state whose steering ellipse $\{\tilde{\rho}_B(\theta) \mid \theta \in \mathbb{R}\}$ has tilt less than 1. Then, for any $P \in \mathbb{RP}^1$,*

$$\lim_{Y\to P} \left\langle \int_0^{2\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\theta} \tilde{\rho}_B(\theta) \right|_Y \mathrm{d}\theta \right\rangle = \widehat{P} = \mathbb{I} - P, \tag{39}$$

where the limit is taken over all density operators Y.

As a consequence of Theorem 12, the function $\mathcal{RD}_>(\mathbb{C}^2) \to \mathcal{RD}(\mathbb{C}^2)$ given by

$$Y \mapsto \left\langle \int_0^{2\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\theta} \tilde{\rho}_B(\theta) \right|_Y \mathrm{d}\theta \right\rangle \tag{40}$$

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 [see, for example, Theorem D on Page 78 of [18].]. By Lemma 22 in the appendix, the function given by (40) is onto. In particular, its image contains ρ_B. We therefore have the following.

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. Then, there exists $Y \in \mathcal{RD}_>(\mathbb{C}^2)$ such that*

$$\int_0^{2\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\theta} \tilde{\rho}_B(\theta) \right|_Y \mathrm{d}\theta \tag{41}$$

is a scalar multiple of ρ_B.

Note that if we use $\rho'_{AB} = (\mathbb{I}_A \otimes Y)\rho_{AB}(\mathbb{I}_A \otimes Y)$ in Lemma 13 then we have that

$$\int_0^{2\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\theta} \tilde{\rho}'_B(\theta) \right| \mathrm{d}\theta \tag{42}$$

is a scalar multiple of ρ'_B, which was our original goal.

V. A CRITERION FOR RP-STEERABILITY

Now we are ready to prove a criterion for RP-steerability that is both necessary and sufficient. The next theorem and corollary contain our main result.

Theorem 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, ρ_{AB} is RP-unsteerable if and only if there exists $Y \in \mathcal{RP}_>(\mathbb{C}^2)$ such that*

$$Y\rho_B Y - \int_0^\pi \left| Y \frac{\mathrm{d}}{\mathrm{d}\theta} \left(\tilde{\rho}_B\left(\theta\right)\right) Y \right| \, \mathrm{d}\theta \geq 0\,. \tag{43}$$

Corollary 15. *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*

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

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

Note that (43) can be rewritten as

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

The following result found in [19] will be important for the proofs that follow.

Lemma 16. *If ρ_{AB} has a LHS model (for any set of measurements), then so does $\langle(\mathcal{I}\otimes\mathcal{M})(\rho_{AB})\rangle$ for any positive linear map $\mathcal{M}$.*

In particular, for any invertible Hermitian operator Y, ρ_{AB} is RP-steerable if and only if $\langle(\mathbb{I}_A \otimes Y)\rho_{AB}(\mathbb{I}_A \otimes Y)\rangle$ is RP-steerable.

Proof of Theorem 14. For any Hermitian operator X, define $|X|_\pm := (|X| \pm X)/2$, and $\|X\|_\pm = \mathrm{Tr}\,|X|_\pm$.

Case 1: Suppose

$$\rho_B \;\geq\; \rho' := \int_0^\pi \left| \frac{\mathrm{d}}{\mathrm{d}\theta} \left(\tilde{\rho}_B\left(\theta\right)\right) \right| \mathrm{d}\theta\,, \tag{46}$$

and define

$$\sigma_\lambda \;:=\; \left| \frac{\mathrm{d}}{\mathrm{d}\lambda} \left(\tilde{\rho}_B\left(\lambda\right)\right) \right|_+ + \frac{\rho_B - \rho'}{2\pi}. \tag{47}$$

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

$$\sigma_\lambda \;=\; \left| \frac{\mathrm{d}}{\mathrm{d}\lambda} \left(\tilde{\rho}_B\left(\lambda+\pi\right)\right) \right|_- + \frac{\rho_B - \rho'}{2\pi}. \tag{48}$$

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

$$\begin{aligned}
\int_0^{2\pi} \sigma_\lambda \, \mathrm{d}\lambda \;&=\; \int_0^{2\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\lambda} \tilde{\rho}_B\left(\lambda\right) \right|_+ \mathrm{d}\lambda + \rho_B - \rho' && (49)\\
&=\; \int_0^{\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\lambda} \tilde{\rho}_B\left(\lambda\right) \right|_+ \mathrm{d}\lambda + \int_\pi^{2\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\lambda} \tilde{\rho}_B\left(\lambda\right) \right|_+ \mathrm{d}\lambda + (\rho_B - \rho') && (50)\\
&=\; \int_0^{\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\lambda} \tilde{\rho}_B\left(\lambda\right) \right|_+ \mathrm{d}\lambda + \int_0^{\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\lambda} \tilde{\rho}_B\left(\lambda\right) \right|_- \mathrm{d}\lambda + (\rho_B - \rho') && (51)\\
&=\; \int_0^{\pi} \left| \frac{\mathrm{d}}{\mathrm{d}\lambda} \tilde{\rho}_B\left(\lambda\right) \right| \mathrm{d}\lambda + (\rho_B - \rho') && (52)\\
&=\; \rho' + \rho_B - \rho' && (53)\\
&=\; \rho_B. && (54)
\end{aligned}$$

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,

$$\begin{aligned}
\int_0^{2\pi} g_\theta(\lambda)\sigma_\lambda \, \mathrm{d}\lambda &= \frac{1}{2}\left[\int_0^{2\pi} (2g_\theta(\lambda)-1)\sigma_\lambda \, \mathrm{d}\lambda + \int_0^{2\pi} \sigma_\lambda \, \mathrm{d}\lambda\right] \\
&= \frac{1}{2}\left[-\int_\theta^{\theta+\pi \bmod 2\pi} \sigma_\lambda \, \mathrm{d}\lambda + \int_{\theta+\pi \bmod 2\pi}^{\theta+2\pi \bmod 2\pi} \sigma_\lambda \, \mathrm{d}\lambda + \rho_B\right] \\
&= \frac{1}{2}\left[-\int_\theta^{\theta+\pi \bmod 2\pi} \left(\left|\frac{\mathrm{d}}{\mathrm{d}\lambda}\tilde{\rho}_B(\lambda)\right|_+ - \left|\frac{\mathrm{d}}{\mathrm{d}\lambda}\tilde{\rho}_B(\lambda)\right|_-\right) \mathrm{d}\lambda + \rho_B\right] \\
&= \frac{1}{2}\left[-\int_\theta^{\theta+\pi \bmod 2\pi} \frac{\mathrm{d}}{\mathrm{d}\lambda}\tilde{\rho}_B(\lambda) \, \mathrm{d}\lambda + \rho_B\right] \\
&= \frac{1}{2}\left[-\tilde{\rho}_B(\theta+\pi) + \tilde{\rho}_B(\theta) + \rho_B\right] = \tilde{\rho}_B(\theta)\,.
\end{aligned}$$

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

$$Y\rho_B Y \;\geq\; \int_0^\pi \left| Y \frac{\mathrm{d}}{\mathrm{d}\theta}\left(\tilde{\rho}_B(\theta)\right) Y \right| \mathrm{d}\theta\,. \tag{55}$$

In this case, the state

$$\overline{\rho_{AB}} = \langle (\mathbb{I}\otimes Y)\rho_{AB}(\mathbb{I}\otimes Y)\rangle \tag{56}$$

satisfies the conditions of Case 1. Since $\mathcal{M} : X \mapsto Y^{-1}XY^{-1}$ is a positive map, by Lemma 16, a local hidden state model exists for ρ_{AB}.

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

$$Y\rho_B Y \;\not\geq\; I_Y := \int_0^\pi \left| Y \frac{\mathrm{d}}{\mathrm{d}\theta}\left(\tilde{\rho}_B(\theta)\right) Y \right| \mathrm{d}\theta \tag{57}$$

By Lemma 13, we can find Y such that I_Y is a scalar multiple of $Y\rho_B Y$ (this is why Corollary 15 follows from Theorem 14). Thus we have

$$Y\rho_B Y \;=\; c\int_0^\pi \left| Y \frac{\mathrm{d}}{\mathrm{d}\theta}\left(\rho_B(\theta)\right) Y \right| \mathrm{d}\theta \tag{58}$$

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

$$\gamma_B \;=\; c\int_0^\pi \left| \frac{\mathrm{d}}{\mathrm{d}\theta}\left(\gamma_B(\theta)\right) \right| \mathrm{d}\theta \tag{59}$$

which in particular means

$$\int_0^\pi \left\| \frac{\mathrm{d}}{\mathrm{d}\theta}\left(\gamma_B(\theta)\right) \right\|_1 \mathrm{d}\theta \;\geq\; (1/c)\mathrm{Tr}(\gamma_B) > 1. \tag{60}$$

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

$$\int_0^{2\pi} \left\| \frac{\mathrm{d}}{\mathrm{d}\theta}\left(\gamma_B(\theta)\right) \right\|_1 \mathrm{d}\theta \;>\; 2, \tag{61}$$

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

VI. 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, i.e., the family $\rho_{AB}(\eta) = \eta|\Phi_+\rangle\langle\Phi_+| + (1-\eta)\mathbb{I}/4$ where $\eta \in [0,1]$ and $|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Theorem 17. *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 $\mathbb{I}/2$). 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 $|\frac{\mathrm{d}}{\mathrm{d}\theta}(\tilde{\rho}_B(\theta))| = \frac{\eta}{4}\mathbb{I}$. Hence,

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

Applying Theorem 14 and Corollary 15 with $Y = \mathbb{I}$ 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 $\eta > \frac{2}{\pi}$. □

Note that this boundary was already known [15, 16], and that it is possible to get close to this bound with small numbers of measurements [15, 20].

B. Application II: RP-steerability of partially entangled states mixed with uniform noise

Consider the family $\rho_{AB}(\alpha,\eta) := \eta|\phi_\alpha\rangle\langle\phi_\alpha| + (1-\eta)\mathbb{I}/4$, 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 18. 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

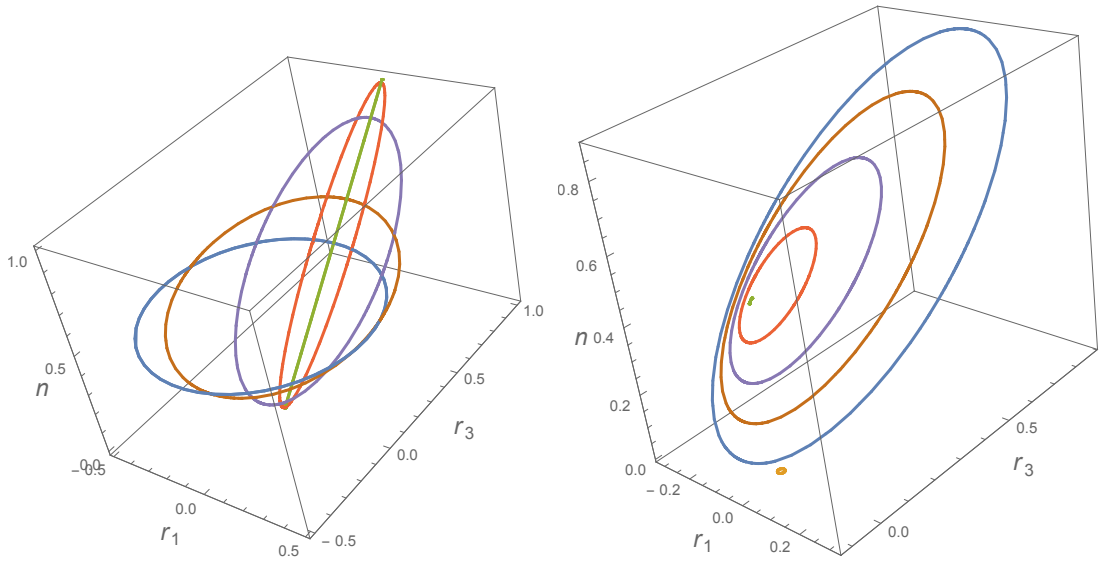
$$\frac{\mathrm{d}}{\mathrm{d}\theta}\tilde{\rho}_B^{\alpha,\eta}(\theta) = \frac{\eta}{2}\begin{pmatrix} -\cos^2(\alpha)\sin\left(\theta\right) & \cos(\alpha)\sin(\alpha)\cos(\theta) \\ \cos(\alpha)\sin(\alpha)\cos(\theta) & \sin^2(\alpha)\sin\left(\theta\right) \end{pmatrix}. \tag{62}$$

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 $\eta \leq \bar{\eta}(\alpha)$. We search for this critical value numerically.

Since Y has real entries, is positive and multiplying by a constant doesn't affect whether (43) 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 $Y = \frac{1}{2}(\mathbb{I} + r_1\sigma_1 + r_3\sigma_3)$. 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 (43). 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., (43) 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 (43), terminating either when a negative value is obtained or when no improvement can be found for some minimal step-size.



(a) (b)

FIG. 3: (a) 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); (b) $\alpha = 0.35$ 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.

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 (43) 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 $\mathcal{S}(\mathbb{C}^2 \otimes \mathbb{C}^2) \to \mathcal{S}(\mathbb{C}^2 \otimes \mathbb{C}^2) : \rho_{AB} \mapsto \hat{\rho}_{AB} := (\mathcal{E}_{\eta_A} \otimes \mathcal{E}_{\eta_B})(\rho_{AB})$, where $\mathcal{E}_\eta : \mathcal{S}(\mathbb{C}^2) \to \mathcal{S}(\mathbb{C}^2)$ is given by $\mathcal{E}_\eta(\rho) = \eta\rho + (1-\eta)\mathbb{I}/2$.

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

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

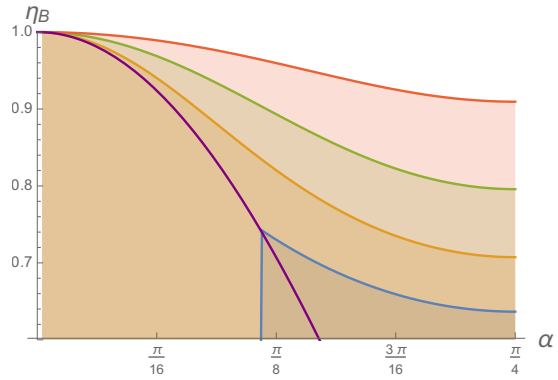


FIG. 4: Plot of the regions where a LHS model exists for all real projective measurements for $\eta_A = 1$ (blue), $\eta_A = 0.9$ (orange) and $\eta_A = 0.8$ (green), $\eta_A = 0.7$ (red) (although not shown, all regions extend downwards to $\eta_B = 0$), together with the purple curve $\eta_B = \cos(2\alpha)$ which we need to be above to use Theorem 14 and Corollary 15. In the case $\eta_A = \frac{2}{\pi}$ (not shown), the state is RP-unsteerable for all η_B and α. For $\eta_A = 0.9$, 0.8 and 0.7 we have a complete classification: above each of the corresponding regions, the state is RP-steerable. In the case $\eta_A = 1$, the classification is incomplete for $\alpha \lessapprox 0.37$. Here, if $\eta_B \leq \cos(2\alpha)$ we are unable to decide whether or not the states are RP-steerable (while for $\eta_B > \cos(2\alpha)$ we know the states are RP-steerable).

For $A_{\alpha,\eta_A,\eta_B} = \begin{pmatrix} \frac{\eta_B - \cos(2\alpha)}{2\eta_B} & 0 \\ 0 & \frac{\eta_B + \cos(2\alpha)}{2\eta_B} \end{pmatrix}$, 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 less than 1 for $\eta_B > \cos(2\alpha)$, so we can use Theorem 14 and Corollary 15 provided this holds.

The derivative of the steering ellipse is

$$\frac{\mathrm{d}}{\mathrm{d}\theta}\tilde{\rho}_B^{\alpha,\eta_A,\eta_B}(\theta) = \frac{\eta_A}{4}\begin{pmatrix} -(\eta_B + \cos(2\alpha))\sin(\theta) & \eta_B \sin(2\alpha)\cos(\theta) \\ \eta_B \sin(2\alpha)\cos(\theta) & (\eta_B - \cos(2\alpha))\sin(\theta) \end{pmatrix}. \tag{63}$$

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.

We first make two observations for special cases, before proceeding with the general case:

1. If there is no noise on Bob's side (i.e., the trusted side), i.e., if $\eta_B = 1$, then $\frac{\mathrm{d}}{\mathrm{d}\theta}\tilde{\rho}_B^{\alpha,\eta_A,1}(\theta)$ is identical to that in (62), 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. If the state is maximally entangled, i.e., $\alpha = \frac{\pi}{4}$, then 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 $\rho_{AB}(\pi/4,\eta_A,\eta_B)$.

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

The left hand side of (43) 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 19. *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 $\hat{\rho}_{AB}(\alpha,\eta_A,\eta'_B)$ is equal to $\frac{\eta'_B}{\eta_B}\hat{\rho}_{AB}(\alpha,\eta_A,\eta_B) + \frac{\eta_B - \eta'_B}{\eta_B}\hat{\rho}_A(\alpha,\eta_A,\eta_B)\otimes\mathbb{I}/2$, i.e., is a convex combination of $\hat{\rho}_{AB}(\alpha,\eta_A,\eta_B)$ and $\hat{\rho}_A(\alpha,\eta_A,\eta_B)\otimes\mathbb{I}/2$, both of which have LHS models. □

Hence, although we cannot use Theorem 14 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 $\alpha \gtrapprox 0.37$ (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 $\eta_A \lessapprox 0.92$).

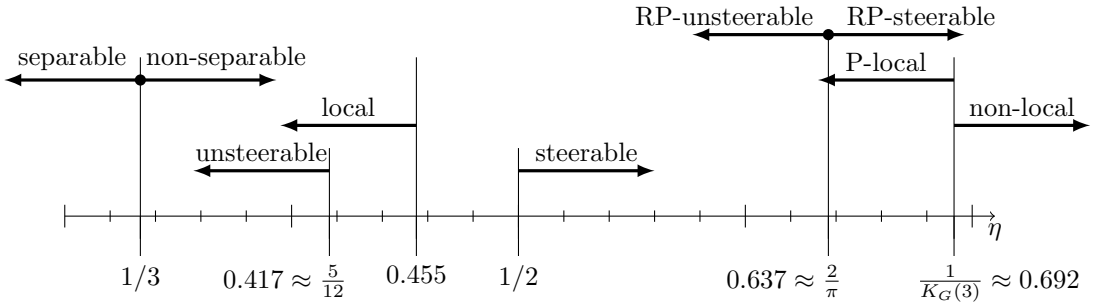


FIG. 5: Summary of known results for Werner states. The approximation taken for $1/K_G(3)$ is the mean of the known upper and lower bounds.

Acknowledgments

We are grateful to Kim Winick for numerous helpful discussions, to Emanuel Knill, Sania Jevtic, Stephen Jordan, and Chau Nguyen for useful feedback on an earlier version of the manuscript, and to Nicholas Brunner, Daniel Cavalcanti and Ivan Supic for pointers to the literature. 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 in part by US NSF grants 1500095, 1526928, and 1717523. YS was also supported in part by University of Michigan.

Appendix A: Summary of known results for Werner states

Werner states (cf. (2)) are separable if and only if $\eta \leq \frac{1}{3}$ [9], are steerable if $\eta > \frac{1}{2}$ [4] and are non-local if $\eta > 1/K_G(3)$ [21], where $K_G(3)$ is Grothendieck's constant of order 3 [22], which is known to satisfy $1.426 < K_G(3) < 1.464$, so that $0.683 < 1/K_G(3) < 0.701$ [23, 24]. They are local for projective measurements if $\eta \leq 1/K_G(3)$ [21] and are local for all measurements for $\eta \leq 0.455$ [24] and also have a LHS model for all measurements for $\eta \leq 5/12$ [19, 25]. 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 [19].

The above is summarized in Figure 5.

Appendix B: Additional Proofs

1. Proof of Proposition 5

This proof uses similar methods to those in [12].

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 $\mathrm{Box}(\mu)$, because $\mathrm{Box}(\mu)$ is convex, 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

$$\rho \;=\; \int_{x\in\mathbb{RP}^1} x \,\mathrm{d}\mu \tag{B1}$$

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

$$z = \int_{x \in \mathbb{RP}^1} x f(x)\ \mathrm{d}\mu \tag{B2}$$

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

$$g(x) \ = \ \begin{cases} 1 & \text{if} \quad x \in (y, w) \\ 0 & \text{if} \quad x \in (w, y) \\ f(y) & \text{if} \quad x = y \\ f(w) & \text{if} \quad x = w. \end{cases} \tag{B3}$$

and let

$$r \ = \ \int_{x \in \mathbb{RP}^1} x g(x)\ \mathrm{d}\mu\,. \tag{B4}$$

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

$$0 \geq \langle r - z, H\rangle \ = \ \left\langle \int_{x \in (y,w)} (1 - f(x)) x\ \mathrm{d}\mu, H \right\rangle - \left\langle \int_{x \in (w,y)} f(x) x\ \mathrm{d}\mu, H \right\rangle \geq 0\,, \tag{B5}$$

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

$$g(x) \ = \ \begin{cases} 1 & \text{if} \quad x \neq y \\ f(y) & \text{if} \quad x = y\,, \end{cases} \tag{B6}$$

where $f\colon \mathbb{RP}^1 \to [0, 1]$ is a function such that (B2) 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

$$c \ = \ \int_{x \in \mathbb{RP}^1} (1/2) x\ \mathrm{d}\mu. \tag{B7}$$

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. □

2. Proof of Lemma 7

We will construct an explicit curve which is the boundary of (19). 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

$$t \in \left[\langle \rho_m, H\rangle\,, \langle \rho_{m+1}, H\rangle\right), \tag{B8}$$

then

$$h_t(x) \ = \ 1 \quad \text{for } x \in [|0\rangle\langle 0|, s_{m+1}) \tag{B9}$$

$$h_t(s_{m+1}) \ = \ \left(\frac{t - \langle \rho_m, H\rangle}{\mu(s_{m+1})\,\langle s_{m+1}, H\rangle}\right), \tag{B10}$$

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

$$\int_{x \in \mathbb{RP}^1} h_t(x)\,\langle x, H\rangle\ \mathrm{d}\mu \ = \ t. \tag{B11}$$

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

$$\overline{h}_t \;=\; \begin{cases} h_{(t+\langle \rho, H\rangle/2)} - h_t & \text{if } t < \langle \rho, H\rangle /2 \\ 1 - h_t + h_{(t-\langle \rho, H\rangle/2)} & \text{otherwise,} \end{cases} \tag{B12}$$

so that for any t,

$$\int_{x\in\mathbb{RP}^1} \overline{h}_t(x)\, \langle x, H\rangle \;\mathrm{d}\mu \;=\; \langle \rho, H\rangle /2. \tag{B13}$$

Let

$$G(t) \;=\; \int_{x\in\mathbb{RP}^1} \overline{h}_t(x) x \;\mathrm{d}\mu. \tag{B14}$$

The points in the image of $G(t)$ are in the region (19) by construction, and since they are obtained from zero-bias two-level functions, they lie on the boundary of $\mathrm{Box}(\mu)$ (see Proposition 5). The image of G is the boundary of (19).

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 $\langle \rho, H\rangle$) and thus

$$\int_0^{\langle \rho, H\rangle} \left| \frac{\mathrm{d}}{\mathrm{d}t} \left(\overline{h}_t(s_i)\right)\right| \mathrm{d}t \le 2. \tag{B15}$$

Therefore, the length of the curve G is given by

$$\begin{aligned} \int_0^{\langle \rho, H\rangle} \left\| \frac{\mathrm{d}}{\mathrm{d}t} G(t)\right\|_1 \mathrm{d}t \;&=\; \int_0^{\langle \rho, H\rangle} \left\| \frac{\mathrm{d}}{\mathrm{d}t} \int_{x\in\mathbb{RP}^1} \overline{h}_t(x) x \mathrm{d}\mu \right\|_1 \mathrm{d}t && \text{(B16)} \\ &=\; \int_0^{\langle \rho, H\rangle} \left\| \frac{\mathrm{d}}{\mathrm{d}t} \sum_{i=1}^n \overline{h}_t(s_i) s_i \mu(s_i) \right\|_1 \mathrm{d}t && \text{(B17)} \\ &\le\; \int_0^{\langle \rho, H\rangle} \sum_{i=1}^n \left| \frac{\mathrm{d}}{\mathrm{d}t} \left(\overline{h}_t(s_i)\right)\right| \mu(s_i) \;\mathrm{d}t && \text{(B18)} \\ &\le\; \sum_{i=1}^n 2\mu(s_i) = 2\,, && \text{(B19)} \end{aligned}$$

as desired. □

3. Tilt of the derivative of the steering ellipse

Lemma 20. *Suppose* $\lambda, \mu \in \mathcal{RA}(\mathbb{C}^2)$ *with* $\mathrm{Tr}(\lambda\mu) = 0$ *and* $\mathrm{Tilt}(\mu) < 1$. *Then* $\mathrm{Tilt}(\lambda) > 1$.

Proof. Suppose $\lambda = \frac{1}{2}(n\mathbb{I} + r_1\sigma_1 + r_3\sigma_3)$ and $\mu = \frac{1}{2}(m\mathbb{I} + s_1\sigma_1 + s_3\sigma_3)$ and write $(r_1, r_3) = r\mathbf{e}_r$ and $(s_1, s_3) = s\mathbf{e}_s$, where $\mathbf{e}_r, \mathbf{e}_s$ are unit vectors and $r, s \ge 0$.

The condition $\mathrm{Tr}(\lambda\mu) = 0$ can be written $-\mathbf{r}.\mathbf{s} = nm$. $\mathrm{Tilt}(\mu) < 1$ is equivalent to $s^2 < m^2$. It follows that $(\mathbf{r}.\mathbf{s})^2 = n^2m^2 > n^2s^2$. This rearranges to $(\mathbf{r}.\mathbf{e_s})^2 > n^2$, from which it follows that $r^2 > n^2$, i.e., $\mathrm{Tilt}(\lambda) > 1$. □

Corollary 21. *Let* $\rho_{AB} \in \mathcal{RD}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ *be a two-qubit state whose steering ellipse* $\{\tilde{\rho}_B(\theta)\}$ *has tilt smaller than* 1. *Then* $\mathrm{Tilt}(\frac{\mathrm{d}}{\mathrm{d}\theta}\tilde{\rho}_B(\theta)) > 1$ *for all* θ.

4. A topological lemma

Lemma 22. *Let* $D = \{z \in \mathbb{C} \mid |z| \le 1\}$ *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 satisfies $G(z) = -z$ for $z \in S^1$. 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. □

5. Proof of Proposition 11

By Proposition 10, we have

$$
\begin{aligned}
|X|_Y &= Y^{-1}\,|YXY|\,Y^{-1} && \text{(B20)}\\
&= \frac{Y^{-1}(YXY)(YXY)Y^{-1} - Y^{-1}(YXY)(\hat{Y}\hat{X}\hat{Y})Y^{-1}}{\|YXY\|_1} && \text{(B21)}\\
&= \frac{XY^2X - X\det(Y)\hat{X}\hat{Y}Y^{-1}}{\|YXY\|_1} && \text{(B22)}\\
&= \frac{XY^2X - X\hat{X}\hat{Y}(\det(Y)Y^{-1})}{\|YXY\|_1} && \text{(B23)}\\
&= \frac{XY^2X - \det(X)\hat{Y}\hat{Y}}{\|YXY\|_1}, && \text{(B24)}
\end{aligned}
$$

which is equal to the desired formula.

---

[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] Barrett, J., Hardy, L. & Kent, A. No signalling and quantum key distribution. *Physical Review Letters* **95**, 010503 (2005). URL `https://doi.org/10.1103/PhysRevLett.95.010503`.

[4] 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`.

[5] 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`.

[6] 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`.

[7] Cavalcanti, D., Guerini, L., Rabelo, R. & Skrzypczyk, P. General method for constructing local hidden variable models for entangled quantum states. *Phys. Rev. Lett.* **117**, 190401 (2016). URL `https://doi.org/10.1103/PhysRevLett.117.190401`.

[8] Hirsch, F., Quintino, M. T., Vértesi, T., Pusey, M. F. & Brunner, N. Algorithmic construction of local hidden variable models for entangled quantum states. *Phys. Rev. Lett.* **117**, 190402 (2016). URL `https://doi.org/10.1103/PhysRevLett.117.190402`.

[9] Werner, R. F. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A* **40**, 4277–4281 (1989). URL `https://doi.org/10.1103/PhysRevA.40.4277`.

[10] 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`.

[11] Nguyen, H. C. & Vu, T. Nonseparability and steerability of two-qubit states from the geometry of steering outcomes. *Phys. Rev. A* **94**, 012114 (2016). URL `http://doi.org/10.1103/PhysRevA.94.012114`.

[12] Nguyen, H. C. & Vu, T. Necessary and sufficient condition for steerability of two-qubit states by the geometry of steering outcomes. *Europhysics Letters* **115**, 10003 (2016). URL `http://stacks.iop.org/0295-5075/115/i=1/a=10003`.

[13] Jones, S. J., Wiseman, H. M. & Doherty, A. C. Entanglement, Einstein-Podolsky-Rosen correlations, Bell nonlocality, and steering. *Phys. Rev. A* **76**, 052116 (2007). URL `https://doi.org/10.1103/PhysRevA.76.052116`.

[14] Bowles, J., Hirsch, F., Quintino, M. T. & Brunner, N. Sufficient criterion for guaranteeing that a two-qubit state is unsteerable. *Phys. Rev. A* **93**, 022121 (2016). URL `https://link.aps.org/doi/10.1103/PhysRevA.93.022121`.

[15] Jones, S. J. & Wiseman, H. M. Nonlocality of a single photon: Paths to an einstein-podolsky-rosen-steering experiment. *Phys. Rev. A* **84**, 012110 (2011). URL `http://doi.org/10.1103/PhysRevA.84.012110`.

[16] Uola, R., Luoma, K., Moroder, T. & Heinosaari, T. Adaptive strategy for joint measurements. *Phys. Rev. A* **94**, 022109 (2016). URL `http://doi.org/10.1103/PhysRevA.94.022109`.

[17] Jevtic, S., Pusey, M., Jennings, D. & Rudolph, T. Quantum steering ellipsoids. *Phys. Rev. Lett.* **13**, 020402 (2014). URL `https://doi.org/10.1103/PhysRevLett.113.020402`.

[18] Simmons, G. F. *Introduction to Topology and Modern Analysis* (Krieger Publishing Company, 1983), reprint edn.

[19] Quintino, M. T. *et al.* Inequivalence of entanglement, steering, and Bell nonlocality for general measurements. *Phys. Rev. A* **92**, 032107 (2015). URL `http://doi.org/10.1103/PhysRevA.92.032107`.

[20] Bavaresco, J. *et al.* Most incompatible measurements for robust steering tests. e-print `arXiv:1704.02994` (2017).

[21] Acín, A., Gisin, N. & Toner, B. Grothendieck's constant and local models for noisy entangled quantum states. *Phys. Rev. A* **73**, 062105 (2006). URL `http://doi.org/10.1103/PhysRevA.73.062105`.

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

[23] Brierley, S., Navascués, M. & Vértesi, T. Convex separation from convex optimization for large-scale problems. e-print `arXiv:1609.05011` (2016).

[24] Hirsch, F., Quintino, M. T., Vértesi, T., Navascués, M. & Brunner, N. Better local hidden variable models for two-qubit Werner states and an upper bound on the Grothendieck constant $K_G(3)$. *Quantum* **1**, 3 (2017). URL `https://doi.org/10.22331/q-2017-04-25-3`.

[25] Barrett, J. Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality. *Phys. Rev. A* **65**, 042302 (2002). URL `http://doi.org/10.1103/PhysRevA.65.042302`.