The Resource Theory of Steering

Rodrigo Gallego and Leandro Aolita

Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany

Abstract

We present an operational framework for Einstein-Podolsky-Rosen steering as a physical resource. To begin with, we characterize the set of *steering non-increasing operations* (SNIOs) – i.e., those that do not create steering– on arbitrary-dimensional bipartite systems composed of a quantum subsystem and a black-box device. Next, we introduce the notion of *convex steering monotones* as the fundamental axiomatic quantifiers of steering. As a convenient example thereof, we present the *relative entropy of steering*. In addition, we prove that two previously proposed quantifiers, the steerable weight and the robustness of steering, are also convex steering monotones. To end up with, for minimal-dimensional systems, we establish, on the one hand, necessary and sufficient conditions for pure-state steering conversions under stochastic SNIOs and prove, on the other hand, the non-existence of *steering bits*, i.e., measure-independent maximally steerable states from which all states can be obtained by means of the free operations. Our findings reveal unexpected aspects of steering and lay foundations for further resource-theory approaches, with potential implications in Bell non-locality.

1998 ACM Subject Classification J.2 Physics

Keywords and phrases Entanglement, EPR-steering, nonlocality, resource theories

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.27

1 Introduction

Steering, as Schrödinger named it [38], is an exotic quantum effect by which ensembles of quantum states can be remotely prepared by performing local measurements at a distant lab. It allows [43, 23, 34] to certify the presence of entanglement between a user with an untrusted measurement apparatus, Alice, and another with a trusted quantum-measurement device, Bob. Thus, it constitutes a fundamental notion between quantum entanglement [22], whose certification requires quantum measurements on both sides, and Bell non-locality [13], where both users possess untrusted black-box devices. Steering can be detected through simple tests analogous to Bell inequalities [14], and has been verified in a variety of remarkable experiments [29, 8, 37, 7, 20, 39], including steering without Bell non-locality [35] and a fully loop-hole free steering demonstration [44]. Apart from its fundamental relevance, steering has been identified as a resource for one-sided device-independent quantum key-distribution (QKD), where only one of the parts has an untrusted apparatus while the other ones possess trusted devices [9, 21]. There, the experimental requirements for unconditionally secure keys are less stringent than in fully (both-sided) device-independent QKD [4, 1, 2].

The formal treatment of a physical property as a resource is given by a *resource theory.*The basic component of this is a restricted class of operations, called the *free operations*, subject to a physically relevant constraint. The free operations are such that every *free state*, i.e., every one without the property in question, is mapped into a free state, so that the resourceful states can be defined as those not attainable by free operations acting on any free state. Furthermore, the quantification of the resource is also built upon the free operations: The fundamental

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 27–38
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

necessary condition for a function to be a measure of the resource is that it is monotonous – non-increasing – under the free operations. That is, the operations that do not increase the resource on the free states do not increase it on all other states either. Entanglement theory [22] is the most popular and best understood [40, 32, 10, 11] resource theory. There, the constrain on the operations is the unavailability of quantum communication, which yields the local operations assisted by classical communication (LOCCs) [6] as the corresponding free operations. Nevertheless, resource theories have been formulated also for states out of thermal equilibrium [12], asymmetry [3], reference frames [19], and quantum coherence [26, 5], for instance.

In steering theory, systems are described by an ensemble of quantum states, on Bob's side, each one associated to the conditional probability of a measurement outcome (output) given a measurement setting (input), on Alice's. Such conditional ensembles are sometimes called *assemblages* [33, 36, 31]. The free operations for steering, which we call *steering non-increasing operations* (SNIOs), must thus arise from constrains native of a natural scenario where steerable assemblages are useful for some physical task. Curiously, up to now, no attempt for an operational framework of steering as a resource has been reported.

In this submission we develop the resource theory of steering. First, we derive the explicit expression of the most general SNIO, for arbitrarily many inputs and outputs for Alice's black box and arbitrary dimension for Bob's quantum system. We show that this class of free operations emerges naturally from the basic restrictions of QKD with assemblages, i.e., of one-side device-independent QKD [9, 21]. With the derived SNIOs, we provide a formal definition of steering monotones. As an example thereof, we present the relative entropy of steering, for which we also introduce, on the way, the notion of relative entropy between assemblages. In addition, we prove SNIO monotonicity for two other recently proposed steering measures, the steerable weight [36] and the robustness of steering [31], and convexity for all three measures. To end up with, we prove two theorems on steering conversion under stochastic SNIOs for the lowest-dimensional case, i.e., qubits on Bob's side and 2 inputs $\times$ 2 outputs on Alice's. In the first one, we show that it is impossible to transform via SNIOs, not even probabilistically, an assemblage composed of pairs of pure orthogonal states into another assemblage composed also of pairs of pure orthogonal states but with a different pair overlap, unless the latter is unsteerable. This yields infinitely many inequivalent classes of steering already for systems of the lowest dimension. In the second one, we show that there exists no assemblage composed of pairs of pure states that can be transformed into any assemblage by stochastic SNIOs. It follows that, in striking contrast to entanglement theory, there exists no operationally well defined, measure-independent maximally steerable assemblage of minimal dimension.

The submission is organized as follows. In Sec. 2 we formally define assemblages and present their basic properties. In Sec. 3 we characterise the SNIOs. In Sec. 4 we introduce the notion of convex steering monotones. In Sec. 5 we present the relative entropy of steering. In Sec. 6 we show convexity and SNIO-monotonicity of the steerable weight and the robustness of steering. In Sec. 7 we study, for minimal-dimensional systems, assemblage conversions under SNIOs and prove the in existence of pure-assemblage steering bits. Finally, in Sec. 8 we present our conclusions and mention some future research directions that our results offer.

Note also, that some proofs and supplemental material can be found in the Appendix of the online version on which this submission is based [17], in which case it will be indicated explicitly.

2 Assemblages and steering

We consider two distant parties, Alice and Bob, who have each a half of a bipartite system. Alice holds a so-called black-box device, which, given a classical input $x \in [s]$, generates a classical output $a \in [r]$, where s and r are natural numbers and the notation $[n] \equiv \{0, \ldots, n-1\}$, for $n \in \mathbb{N}$, is introduced. Bob holds a quantum system of dimension d (*qudit*), whose state he can perfectly characterize tomographically via trusted quantum measurements. The joint state of their system is thus fully specified by an *assemblage*

$$\rho_{A|X} \equiv \{P_{A|X}(a,x), \varrho(a,x)\}_{a\in[r],x\in[s]}, \tag{1}$$

of normalized quantum states $\varrho(a,x) \in \mathcal{L}(\mathcal{H}_B)$, with $\mathcal{L}(\mathcal{H}_B)$ the set of linear operators on Bob's subsystem's Hilbert space $\mathcal{H}_B$, each one associated to a conditional probability $P_{A|X}(a,x)$ of Alice getting an output a given an input x. We denote by $P_{A|X}$ the corresponding conditional probability distribution.

Equivalently, each pair $\{P_{A|X}(a,x), \varrho(a,x)\}$ can be univocally represented by the unnormalized quantum state

$$\varrho_{A|X}(a,x) \equiv P_{A|X}(a,x) \times \varrho(a,x). \tag{2}$$

In turn, an alternative representation of the assemblage $\rho_{A|X}$ is given by the set $\hat{\rho}_{A|X} \equiv \{\hat{\rho}_{A|X}(x)\}_x$ of quantum states

$$\hat{\rho}_{A|X}(x) \equiv \sum_a |a\rangle\langle a| \otimes \varrho_{A|X}(a,x) \in \mathcal{L}(\mathcal{H}_E \otimes \mathcal{H}_B), \tag{3}$$

where $\{|a\rangle\}$ is an orthonormal basis of an auxiliary extension Hilbert space $\mathcal{H}_E$ of dimension r. The states $\{|a\rangle\}$ do not describe the system inside Alice's box, they are just abstract flag states to represent its outcomes with a convenient bra-ket notation. Expression (3) gives the counterpart for assemblages of the so-called extended Hilbert space representation used for ensembles of quantum states [28]. We refer to $\hat{\rho}_{A|X}$ for short as the *quantum representation* of $\rho_{A|X}$ and use either notation upon convenience.

We restrict throughout to *no-signaling assemblages*, i.e., those for which Bob's reduced state $\varrho_B \in \mathcal{L}(\mathcal{H}_B)$ does not depend on Alice's input choice x:

$$\varrho_B \equiv \sum_a \varrho_{A|X}(a,x) = \sum_a \varrho_{A|X}(a,x') \ \ \forall\, x, x'. \tag{4}$$

The assemblages fulfilling the no-signaling condition (4) are the ones that possess a *quantum realization*. That is, they can be obtained from local quantum measurements by Alice on a joint quantum state $\varrho_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ shared with Bob, where $\mathcal{H}_A$ is the Hilbert space of the system inside Alice's box. For any no-signaling assemblage $\rho_{A|X}$, we refer as the *trace of the assemblage* to the x-independent quantity

$$Tr[\rho_{A|X}] \equiv Tr_{EB}[\hat{\rho}_{A|X}] = Tr[\varrho_B] = \sum_a P_{A|X}(a,x), \tag{5}$$

and say that the assemblage is normalized if $Tr[\rho_{A|X}] = 1$ and unnormalized if $Tr[\rho_{A|X}] \leq 1$.

An assemblage $\sigma_{A|X} \equiv \{\varsigma_{A|X}(a,x)\}_{a\in[r],x\in[s]}$, being $\varsigma_{A|X}(a,x) \in \mathcal{L}(\mathcal{H}_B)$ unnormalized states, is called *unsteerable* if there exist a probability distribution P_Λ, a conditional probability distribution $P_{A|X\Lambda}$, and normalized states $\xi(\lambda) \in \mathcal{L}(\mathcal{H}_B)$ such that

$$\varsigma_{A|X}(a,x) = \sum_\lambda P_\Lambda(\lambda) P_{A|X\Lambda}(a,x,\lambda)\, \xi(\lambda) \ \ \forall\, x, a. \tag{6}$$

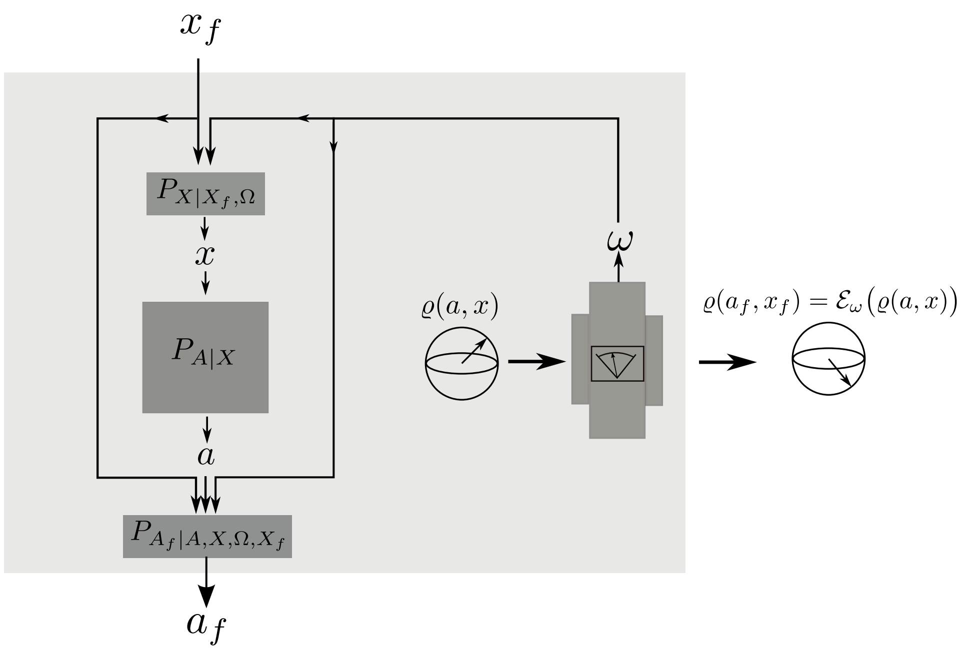

Figure 1 Schematic representation of a SNIO map $\mathcal{M}$: The initial assemblage $\rho_{A|X}$ consists of a black-box, with inputs x and outputs a, governed by the probability distribution $P_{A|X}$, in Alice's hand, and a quantum subsystem in one of the states $\{\varrho(a,x)\}_{a,x}$, in Bob's hands. The final assemblage $\rho_{A_f|X_f} = \mathcal{M}(\rho_{A|X})$ is given by a final black-box, represented by the light-grey rectangle, of inputs x_f and outputs a_f, and a final subsystem, represented outside the light-grey rectangle, in the state $\varrho(a_f,x_f) = \mathcal{E}_\omega(\varrho(a,x))$. To implement $\mathcal{M}$, first, Bob applies, with a probability $P_\Omega(\omega)$, a stochastic quantum operation $\mathcal{E}_\omega$ that leaves his subsystem in the state $\mathcal{E}_\omega(\varrho(a,x))$. He communicates ω to Alice. Then, Alice generates x by processing the classical bits ω and x_f according to the conditional distribution $P_{X|X_f,\Omega}$. She inputs x to her initial device, upon which the bit a is output. Finally, Alice generates the output a_f of the final device by processing x_f, ω, x, and a, according to the conditional distribution $P_{A_f|A,X,\Omega,X_f}$.

Such assemblages can be obtained by sending a shared classical random variable λ to Alice, correlated with the state $\xi(\lambda)$ sent to Bob, and letting Alice classically post-process her random variable according to $P_{A|X\Lambda}$, with $P_{X,\Lambda} = P_X \times P_\Lambda$ so that condition (4) holds. The variable λ is called a *local-hidden variable* and the decomposition (6) is accordingly referred to as a *local-hidden state* (LHS) model. We refer to the set of all unsteerable assemblages as LHS. Any assemblage that does not admit a LHS model as in Eq. (6) is called *steerable*. An assemblage is compatible with classical correlations if, and only if, it is unsteerable.

3 The operational framework

3.1 Physical constraints defining the free operations

QKD consists of the extraction of a secret key from the correlations of local-measurement outcomes on a bipartite quantum state. The most fundamental constraint to which any generic QKD protocol is subject is, of course, the lack of a private safe classical-communication channel between distant labs. Otherwise, if such channel was available, the whole enterprise of QKD would be pointless. This imposes restrictions on the operations allowed so as not to break the security of the protocol. For instance, clearly, the local-measurement outcomes cannot be communicated, as they can be intercepted by potential eavesdroppers who could, with them, immediately crack the key. Of particular relevance for this submission are the assumptions on the measurement devices. In non-device-independent QKD protocols entanglement is the resource and security is proven under the assumption that the users have a specific quantum state and perfectly characterized measurement devices [16]. Knowledge of the state by an eavesdropper does not compromise the security. Therefore, prior to the measurements producing the key, the users are allowed to preprocess the state in any way and exchange information about it, for instance with LOCCs and even eventually disregarding the state and aborting the protocol run. Pre-processing abortions or classical communication can at most provide an eavesdropper with knowledge about the state, not about the key, and therefore do not affect the security.

The situation is different in device-independent QKD (DIQKD) [4, 1, 2]. There, the resource is given by Bell non-local correlations and no assumption is made either on the quantum state or the measurement devices. The users effectively hold black-box measurement devices, whose inputs and outputs are all to which they have access. Since such inputs and outputs are precisely the bits with which the key is established, both classical communication and abortions are forbidden. Communication of outputs can directly reveal the key, as mentioned, whereas abortions and communication of inputs can, due to the locality and detection loopholes, respectively, be maliciously exploited by an eavesdropper to obtain information about the key too. Hence, the natural constrains of DIQKD impose that operations are restricted to well-known [18, 41] paradigm of shared-randomness and local classical information processing.

Steerable assemblages are resources for one-sided DIQKD (1S-DIQKD) [9, 21]. There, while no assumption is made on the bipartite quantum state or Alice's measurement device, Bob's measurement device is perfectly characterized. This is effectively described by assemblages as given in Eq. (1). Thus, it is reasonable to take the natural constrains of 1S-DIQKD as the basic restrictions to define the free operations for steering. The asymmetry in the assumptions on Alice and Bob's devices, results in an asymmetry between the operations allowed to each of them. Alice is subject to the same restrictions as in device-independent QKD, while Bob, to those of non-device-independent QKD. Hence, Alice cannot abort or transmit any information, but, prior to his key-producing measurement, Bob is allowed to implement arbitrary local quantum operations to his subsystem, including stochastic ones with possible abortions, and send any feedback about them to Alice. Altogether, this gives a clear physical motivation for our operational framework: We take SNIOs as the assemblage transformations involving only deterministic classical maps on Alice's side and arbitrary – possibly stochastic – quantum operations on Bob's side assisted by one-way classical communication only from Bob to Alice.[1]. Note that shared randomness, which also does not introduce any security compromise in 1S-DIQKD, can always be recast as one-way classical communication from Bob to Alice and needs, therefore, not be considered explicitly.

[1] Throughout the article, the term "deterministic" is used to refer probability (trace) preserving classical (quantum) maps. These are maps such that, given an input bit (state), generate an output bit (state), respectively, with certainty, i.e., they never cause an abortion. This does not mean that the output cannot be chosen at random. That is, this should not be confused with classical (quantum) maps where the output bit (state) is a Kronecker delta function of the input bit (a unitary transformation of the input state). In turn, the term "stochastic" is used throughout to refer to non probability-preserving classical or non trace-preserving quantum transformations that do not occur with certainty.

3.2 The free operations

More technically, we consider the general scenario of *stochastic SNIOs*, i.e., SNIOs that do not necessarily occur with certainty, which map the initial assemblage $\rho_{A_f|X_f}$ into a final assemblage $\rho_{A_f|X_f}$ (see Fig. 1). Bob's generic quantum operation can be represented by an incomplete generalised measurement. This is described by a completely-positive non trace-preserving map $\mathcal{E} : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_{Bf})$ defined by

$$\mathcal{E}(\cdot) := \sum_{\omega} \mathcal{E}_{\omega}(\cdot), \text{ with } \mathcal{E}_{\omega}(\cdot) := K_{\omega} \; \cdot \; K_{\omega}^{\dagger}, \tag{7a}$$

$$\text{such that } \sum_{\omega} K_{\omega}^{\dagger} K_{\omega} \leq \mathbb{1}, \tag{7b}$$

where $\mathcal{H}_{Bf}$ is the final Hilbert space, of dimension d_f, and $K_\omega : \mathcal{H}_B \to \mathcal{H}_{Bf}$ is the measurement operator corresponding to the ω-th measurement outcome. For any normalized $\varrho_B \in \mathcal{L}(\mathcal{H}_B)$, the trace $Tr[\mathcal{E}(\varrho_B)] \leq 1$ of the map's output $\mathcal{E}(\varrho_B)$ represents the probability that the physical transformation $\varrho_B \to \mathcal{E}(\varrho_B)/Tr[\mathcal{E}(\varrho_B)]$ takes place. In turn, the map $\mathcal{E}_\omega(\cdot)$ describes the post-selection of the ω-th outcome, which occurs with a probability

$$P_{\Omega}(\omega) := Tr[\mathcal{E}_{\omega}(\rho_B)] = Tr[K_{\omega} \varrho_B K_{\omega}^{\dagger}] \leq 1. \tag{8}$$

Since Alice can only process classical information, the allowed one-way communication from Bob to her must be classical too. Thus, it can only consists of the outcome ω of his quantum operation. Classical bit processings are usually referred to as *wirings* [13]. Alice's wirings map $a \in [r]$ and $x \in [s]$ into input and out bits $a_f \in [r_f]$ and $x_f \in [s_f]$, respectively, of the final assemblage, where s_f and r_f are natural numbers. The most general wirings respecting the above constraints are described by conditional probability distributions $P_{X|X_f,\Omega}$ and $P_{A_f|A,X,\Omega,X_f}$ of generating x from ω and x_f and a_f from x_f, ω, x, and a, respectively, as sketched in Fig. 1. Finally, since, as mentioned, her wirings must be deterministic, $P_{X|X_f,\Omega}$ and $P_{A_f|A,X,\Omega,X_f}$ must be normalized probability-preserving distributions.

All in all, the general form of the resulting maps is parametrized in the following definition (see App. A in [17]).

▶ **Definition 1** (Stochastic SNIOs). We define the class SNIO of *(stochastic) SNIOs* as the set of (stochastic) maps $\mathcal{M}$ that take an arbitrary assemblage $\hat{\rho}_{A|X}$ into a final assemblage $\hat{\rho}_{A_f|X_f} := \mathcal{M}(\hat{\rho}_{A|X})$, where

$$\mathcal{M}(\hat{\rho}_{A|X}) := \sum_{\omega} (\mathbb{1} \otimes K_{\omega})\, \mathcal{W}_{\omega}(\hat{\rho}_{A|X})\, (\mathbb{1} \otimes K_{\omega}^{\dagger}), \tag{9}$$

being $\mathcal{W}_\omega$ a *deterministic w*iring map given by

$$\begin{aligned}[\mathcal{W}_{\omega}(\hat{\rho}_{A|X})](x_f) := & \sum_{a_f,a,x} P(x|x_f,\omega) P(a_f|a,x,\omega,x_f) \\ & \times \; (|a_f\rangle\langle a| \otimes \mathbb{1})\, \hat{\rho}_{A|X}(x)\, (|a\rangle\langle a_f| \otimes \mathbb{1}),\end{aligned} \tag{10}$$

with $P(x|x_f,\omega)$ and $P(a_f|a,x,\omega,x_f)$ short-hand notations for the conditional probabilities $P_{X|X_f,\Omega}(x,x_f,\omega)$ and $P_{A_f|A,X,\Omega,X_f}(a_f,a,x,\omega,x_f)$, respectively.

Note that the final assemblage (9) is in general not normalized: Introducing

$$\mathcal{M}_{\omega}(\,\cdot\,) := (\mathbb{1} \otimes K_{\omega})\, \mathcal{W}_{\omega}(\,\cdot\,)\, (\mathbb{1} \otimes K_{\omega}^{\dagger}), \tag{11}$$

such that $\mathcal{M}(\,\cdot\,) = \sum_\omega \mathcal{M}_\omega(\,\cdot\,)$, we obtain, using Eqs. (3), (4), (5), (8), (9), and (10), that

$$Tr[\mathcal{M}(\hat{\rho}_{A|X})] = \sum_\omega Tr[\mathcal{M}_\omega(\hat{\rho}_{A|X})] = \sum_\omega P_\Omega(\omega) \leq 1. \tag{12}$$

As with quantum operations, the trace (12) of $\mathcal{M}(\hat{\rho}_{A|X})$ represents the probability that the physical transformation $\hat{\rho}_{A|X} \to \mathcal{M}(\hat{\rho}_{A|X})/Tr[\mathcal{M}(\hat{\rho}_{A|X})]$ takes place. Analogously, the map $\mathcal{M}_\omega$ describes the assemblage transformation that takes place when Bob post-selects the ω-th outcome, which occurs with probability $Tr[\mathcal{M}_\omega(\hat{\rho}_{A|X})] = P_\Omega(\omega)$. In the particular case where $\mathcal{M}$ is trace-preserving, we refer to it as a *deterministic SNIO*.

Finally, we prove in App. B of Ref. [17] the following theorem.

▶ **Theorem 2** (SNIO invariance of LHS). *Any map of the class* SNIO *takes every unsteerable assemblage into an unsteerable assemblage.*

4 Steering monotonicity

As the natural next step, we introduce an axiomatic approach to define steering measures, i.e., a set of reasonable postulates that a bona fide quantifier of the steering of a given assemblage should fulfill.

▶ **Definition 3** (SNIO-monotonicity and convexity). A function $\mathscr{S}$, from the space of assemblages into $\mathbb{R}_{\geq 0}$, is a *steering monotone* if it fulfils the following two axioms:

(i) $\mathscr{S}(\hat{\rho}_{A|X}) = 0$ for all $\hat{\rho}_{A|X} \in$ LHS.

(ii) $\mathscr{S}$ does not increase, on average, under deterministic SNIOs, i.e.,

$$\sum_\omega P_\Omega(\omega)\mathscr{S}\left(\frac{\mathcal{M}_\omega(\hat{\rho}_{A|X})}{Tr\left[\mathcal{M}_\omega(\hat{\rho}_{A|X})\right]}\right) \leq \mathscr{S}(\hat{\rho}_{A|X}) \tag{13}$$

for all $\hat{\rho}_{A|X}$, with $P_\Omega(\omega) = Tr\left[\mathcal{M}_\omega(\hat{\rho}_{A|X})\right]$ and $\sum_\omega P_\Omega = 1$.

Besides, $\mathscr{S}$ is a *convex steering monotone* if it additionally satisfies the property:

(iii) Given any real number $0 \leq \mu \leq 1$, and assemblages $\hat{\rho}_{A|X}$ and $\hat{\rho}'_{A|X}$, then

$$\mathscr{S}\left(\mu\,\hat{\rho}_{A|X} + (1-\mu)\hat{\rho}'_{A|X}\right) \leq \mu\,\mathscr{S}\left(\hat{\rho}_{A|X}\right) + (1-\mu)\mathscr{S}\left(\hat{\rho}'_{A|X}\right). \tag{14}$$

Condition *i*) reflects the basic fact that unsteerable assemblages should have zero steering. Condition *ii*) formalizes the intuition that, analogously to entanglement, steering should not increase – on average – under SNIOs, even if the flag information ω produced in the transformation is available. Finally, condition *iii*) states the desired property that steering should not increase by probabilistically mixing assemblages. The first two conditions are taken as mandatory necessary conditions, the third one only as a convenient property. Importantly, there exists a less demanding definition of monotonicity. There, the left-hand side of Eq. (13) is replaced by $\mathscr{S}\left(\mathcal{M}(\hat{\rho}_{A|X})/Tr[\mathcal{M}(\hat{\rho}_{A|X})]\right)$. That is, *ii'*) it is demanded only that steering itself, instead of its average over ω, is non-increasing under SNIOs. The latter is actually the most fundamental necessary condition for a measure. However, monotonicity *ii*) is in many cases (including the present submission) easier to prove and, together with condition *iii*), implies monotonicity *ii'*). Hence, we focus throughout on monotonicity as defined by Eq. (13) and refer to it simply as *SNIO monotonicity.* All three known quantifiers of steering, the two ones introduced in Refs. [36, 31] as well as the one we introduce next, turn out to be convex steering monotones in the sense of Definition 3.

5 The relative entropy of steering

The first step is to introduce the notion of *relative entropy* between assemblages. To this end, for any two density operators ϱ and ϱ', we first recall the *quantum von-Neumann relative entropy*

$$S_{\mathrm{Q}}(\varrho\|\varrho') := Tr\left[\varrho\left(\log\varrho - \log\varrho'\right)\right] \tag{15}$$

of ϱ with respect to ϱ' and, for any two probability distributions P_X and P'_X, the *classical relative entropy*, or *Kullback-Leibler divergence*,

$$S_{\mathrm{C}}(P_X\|P'_X) := \sum_x P_X(x)[\log P_X(x) - \log P'_X(x)] \tag{16}$$

of P_X with respect to P'_X. The quantum and classical relative entropies (15) and (16) measure the distinguishability of states and distributions, respectively. To find an equivalent measure for assemblages, we note, for $\hat{\rho}_{A|X}(x)$ given by Eq. (3) and $\hat{\rho}'_{A|X}(x) := \sum_a P'_{A|X}(a,x)|a\rangle\langle a| \otimes \varrho'(a,x)$, that

$$\begin{aligned} S_{\mathrm{Q}}\left(\hat{\rho}_{A|X}(x)\|\hat{\rho}'_{A|X}(x)\right) &= S_{\mathrm{C}}\left(P_{A|X}(\cdot,x)\|P'_{A|X}(\cdot,x)\right) \\ &\quad + \sum_a P_{A|X}(a,x) S_{\mathrm{Q}}\left(\varrho(a,x)\|\varrho'(a,x)\right), \end{aligned} \tag{17}$$

where $P_{A|X}(\cdot,x)$ and $P'_{A|X}(\cdot,x)$ are respectively the distributions over a obtained from the conditional distributions $P_{A|X}$ and $P'_{A|X}$ for a fixed x. That is, the distinguishability between the states $\hat{\rho}_{A|X}(x)$ and $\hat{\rho}'_{A|X}(x) \in \mathcal{L}(\mathcal{H}_E \otimes \mathcal{H}_B)$ equals the sum of the distinguishabilities between $P_{A|X}(x)$ and $P'_{A|X}(x)$ and between $\varrho(a,x)$ and $\varrho'(a,x) \in \mathcal{L}(\mathcal{H}_B)$, weighted by $P_{A|X}(a,x)$ and averaged over a.

The entropy (17), which depends on x, does not measure the distinguishability between the assemblages $\rho_{A|X}$ and $\rho'_{A|X}$. Since the latter are conditional objects, i.e., with inputs, a general strategy to distinguish them must allow for Alice choosing the input for which the assemblages' outputs are optimally distinguishable. Furthermore, Bob can first apply a generalised measurement on his subsystem and communicate the outcome γ to her, which she can then use for her input choice. This is the most general procedure within the allowed SNIOs. Hence, a generic distinguishing strategy under SNIOs involves probabilistically chosen inputs that depend on γ. Note, in addition, that the statistics of γ generated, described by distributions P_Γ or P'_Γ, encode differences between $\rho_{A|X}$ and $\rho'_{A|X}$ too and must therefore also be accounted for by a distinguishability measure. The following definition incorporates all these considerations.

▶ **Definition 4** (Relative entropy between assemblages). Given any two assemblages $\rho_{A|X}$ and $\rho'_{A|X}$, we define the *assemblage relative entropy* of $\rho_{A|X}$ with respect to $\rho'_{A|X}$ as

$$\begin{aligned} S_{\mathrm{A}}(\rho_{A|X}\|\rho'_{A|X}) := \max_{P_{X|\Gamma},\{E_\gamma\}} \Bigg[& S_{\mathrm{C}}(P_\Gamma\|P'_\Gamma) \\ + \sum_{\gamma,x} P(x|\gamma) P_\Gamma(\gamma) S_{\mathrm{Q}} & \left(\frac{\mathbb{1}\otimes E_\gamma \hat{\rho}_{A|X}(x) \mathbb{1}\otimes E_\gamma^\dagger}{P_\Gamma(\gamma)} \,\Bigg\|\, \frac{\mathbb{1}\otimes E_\gamma \hat{\rho}'_{A|X}(x) \mathbb{1}\otimes E_\gamma^\dagger}{P'_\Gamma(\gamma)} \right) \Bigg], \end{aligned} \tag{18}$$

where $E_\gamma : \mathcal{H}_B \to \mathcal{H}_B$ are generalised-measurement operators such that $\sum_\gamma E_\gamma^\dagger E_\gamma = \mathbb{1}$, $P_{X|\Gamma}$ is a conditional probability distribution of x given γ, the short-hand notation $P(x|\gamma) :=$

$P_{X|\Gamma}(x,\gamma)$ has been used, and

$$P_\Gamma(\gamma) := Tr[\mathbb{1}\otimes E_\gamma \hat{\rho}_{A|X}(x)\mathbb{1}\otimes E_\gamma^\dagger] = Tr_B[E_\gamma \varrho_B E_\gamma^\dagger], \tag{19a}$$
$$P'_\Gamma(\gamma) := Tr[\mathbb{1}\otimes E_\gamma \hat{\rho}'_{A|X}(x)\mathbb{1}\otimes E_\gamma^\dagger] = Tr_B[E_\gamma \varrho'_B E_\gamma^\dagger], \tag{19b}$$

where ϱ'_B is Bob's reduced state for the assemblage $\rho'_{A|X}$.

In App. C of Ref. [17], we show that S_{A} does not increase – on average – under deterministic SNIOs and, as its quantum counterpart S_{Q}, is jointly convex. Hence, S_{A} is a proper measure of distinguishability between assemblages under SNIOs.[2]. The first term inside the maximization in Eq. (18) accounts for the distinguishability between the distributions of measurement outcomes γ and the second one for that between the distributions of Alice's outputs and Bob's states resulting from each γ, averaged over all inputs and measurement outcomes. In turn, the maximization over $\{E_\gamma\}$ and $P_{X|\Gamma}$ ensures that these output distributions and states are distinguished using the optimal SNIO-compatible strategy.

We are now in a good position to introduce a convex steering monotone. We do it with a theorem.

▶ **Theorem 5** (SNIO-monotonicity and convexity of $\mathscr{S}_{\mathrm{R}}$)**.** *The relative entropy of steering $\mathscr{S}_R$, defined for an assemblage $\rho_{A|X}$ as*

$$\mathscr{S}_R(\rho_{A|X}) := \min_{\sigma_{A|X}\in \mathsf{LHS}} S_A(\rho_{A|X} \parallel \sigma_{A|X}), \tag{20}$$

is a convex steering monotone.

The theorem is proven in App. C in Ref. [17].

6 Other convex steering monotones

Apart from $\mathscr{S}_{\mathrm{R}}$ two other quantifiers of steering have been recently proposed: the steerable weight [36] and the robustness of steering [31]. In this section, we show that these are also convex steering monotones.

▶ **Definition 6** (Steerable weight [36])**.** The steerable weight $\mathscr{S}_{\mathrm{W}}(\rho_{A|X})$ of an assemblage $\rho_{A|X}$ is the minimum $\nu\in\mathbb{R}_{\geq 0}$ such that

$$\rho_{A|X} = \nu\,\tilde{\rho}_{A|X} + (1-\nu)\sigma_{A|X}, \tag{21}$$

with $\tilde{\rho}_{A|X}$ an arbitrary assemblage and $\sigma_{A|X}\in\mathsf{LHS}$.

▶ **Definition 7** (Robustness of steering [31])**.** The robustness of steering $\mathscr{S}_{\mathrm{Rob}}(\rho_{A|X})$ of an assemblage $\rho_{A|X}$ is the minimum $\nu\in\mathbb{R}_{\geq 0}$ such that

$$\sigma_{A|X} := \frac{1}{1+\nu}\rho_{A|X} + \frac{\nu}{1+\nu}\,\tilde{\rho}_{A|X} \tag{22}$$

belongs to LHS, with $\tilde{\rho}_{A|X}$ an arbitrary assemblage.

[2] A natural question (which we leave open) is how to define a relative entropy between assemblages that is non-increasing under generic assemblage transformations instead of just SNIOs, so that it can be understood as measure of distinguishability under fully general strategies. That is the case of S_{Q}, for instance, which is non-increasing under not only LOCCs but also any completely positive map. However, to introduce a steering monotone, SNIO-monotonicity of S_{A} suffices.

In App. D in Ref. [17], we prove the following theorem.

▶ **Theorem 8** (SNIO-monotonicity and convexity of $\mathscr{S}_{\mathsf{W}}$ and $\mathscr{S}_{\mathsf{Rob}}$). *Both $\mathscr{S}_W$ and $\mathscr{S}_{Rob}$ are convex steering monotones.*

To end up with, we note that a steering measure for assemblages containing continuous-variable (CV) bosonic systems in Gaussian states has very recently appeared [24]. Even though our formalism can be straightforwardly extended to CV systems, such extension is outside the scope of the present submission.

7 Assemblage conversions and no steering bits

We say that $\Psi_{A|X}$ and $\Psi'_{A|X}$ are *pure assemblages* if they are of the form

$$\Psi_{A|X} \coloneqq \{P_{A|X}(a,x), |\psi(a,x)\rangle\langle\psi(a,x)|\}_{a,x}, \tag{23a}$$
$$\Psi'_{A|X} \coloneqq \{P'_{A|X}(a,x), |\psi'(a,x)\rangle\langle\psi'(a,x)|\}_{a,x}, \tag{23b}$$

where $|\psi(a,x)\rangle$ and $|\psi'(a,x)\rangle \in \mathcal{H}_B$, and *pure orthogonal assemblages* if, in addition, $\langle\psi(a,x)|\psi(\tilde{a},x)\rangle = \delta_{a\,\tilde{a}} = \langle\psi'(a,x)|\psi'(\tilde{a},x)\rangle$ for all x. Note that pure orthogonal assemblages are the ones obtained when Alice and Bob share a pure maximally entangled state and Alice performs a von-Neumann measurement on her share. We present two theorems about assemblage conversions under SNIOs.

The first one, proven in App. E in Ref. [17], establishes necessary and sufficient conditions for stochastic-SNIO conversions between pure orthogonal assemblages, therefore playing a similar role here to the one played in entanglement theory by Vidal's theorem [42] for stochastic-LOCC pure-state conversions.

▶ **Theorem 9** (Criterion for stochastic-SNIO conversion). *Let $\Psi_{A|X}$ and $\Psi'_{A|X}$ be any two pure orthogonal assemblages with $d = s = r = 2$. Then, $\Psi_{A|X}$ can be transformed into $\Psi'_{A|X}$ by a stochastic SNIO iff: either $\Psi'_{A|X} \in \mathsf{LHS}$ or $P'_{A|X} = P_{A|X}$ and*

$$|\langle\psi'(a,0)|\psi'(a,1)\rangle| = |\langle\psi(a,0)|\psi(a,1)\rangle| \ \forall\ a. \tag{24}$$

In other words, no pure orthogonal assemblage of minimal dimension can be obtained via a SNIO, not even probabilistically, from a pure orthogonal assemblage of minimal dimension with a different state-basis overlap unless the former is unsteerable. Hence, each state-basis overlap defines an inequivalent class of steering, there being infinitely many of them. This is in a way reminiscent to the inequivalent classes of entanglement in multipartite [15] or infinite-dimensional bipartite [30] systems, but here the phenomenon is found already for bipartite systems of minimal dimension.

The second theorem, proven in App. F in [17], rules out the possibility of there being a (non-orthogonal) minimal-dimension pure assemblage from which all assemblages can be obtained.

▶ **Theorem 10** (Non-existence of steering bits). *There exists no pure assemblage with $d = s = r = 2$ that can be transformed into any assemblage by stochastic SNIOs.*

Hence, among the minimal-dimension assemblages there is no operationally well defined *unit of steering*, or *steering bit*, i.e., an assemblage from which all assemblages can be obtained for free and can therefore be taken as a measure-independent maximally steerable assemblage. This is again in striking contrast to entanglement theory, where pure maximally entangled states can be defined without the need of entanglement quantifiers and each one can be transformed into any state by deterministic LOCCs [42, 27].

8 Discussion and outlook

We have introduced the resource theory of Einstein-Podolsky-Rosen steering. The restricted class of free operations for the theory, which we abbreviate by SNIOs, arises naturally from the basic physical constraints in one-sided device-independent QKD. It is composed of all the transformations involving deterministic bit wirings on Alice's side and stochastic quantum operations on Bob's assisted by one-way classical communication from Bob to Alice. With it, we introduced the notion of *convex steering monotones*, presented the *relative entropy of steering* as a convenient example thereof, and proved monotonicity and convexity of two other previously proposed steering measures. In addition, for minimal-dimensional systems, we established necessary and sufficient conditions for stochastic-SNIO conversions between pure-state assemblages and proved the non-existence of *steering bits*.

It is instructive to emphasize that the derived SNIOs correspond to a combination of the operations that do not increase the entanglement of quantum states, stochastic LOCCs, and the ones that do not increase the Bell non-locality of correlations, local wirings assisted by shared randomness. Regarding the latter, a resource-theory approach to Bell non-locality is only partially developed [18, 25, 41]. Hence, our findings are potentially useful also in Bell non-locality. In addition, our submission offers a number of challenges for future research. Namely, for example, the non-existence of steering bits of minimal dimension can be seen as an impossibility of steering dilution of minimal-dimension assemblages in the single-copy regime. We leave as open questions what the rules for steering dilution and distillation are for higher-dimensional systems, mixed-state assemblages, or in asymptotic multi-copy regimes, and what the steering classes are for mixed-state assemblages. Moreover, other fascinating questions are whether one can formulate a notion of *bound steering* or an analogue to the positive-partial-transpose criterion for assemblages.

References

1 A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).
2 A. Acín *et al.*, Phys. Rev. Lett. **98**, 230501 (2007).
3 M. Ahmadi, D. Jennings and T. Rudolph, New J. Phys. **15**, 013057 (2013).
4 J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
5 T. Baumgratz, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. **113**, 140401 (2014).
6 C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
7 A. J. Bennet *et al.*, Phys. Rev. X **2**, 031003 (2012).
8 W. P. Bowen, R. Schnabel, and P. K. Lam, Phys. Rev. Lett. **90**, 043601 (2003).
9 C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani and H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).
10 F. G. S. L. Brandão and M. B. Plenio, Nature Phys. **4**, 873 (2008).
11 F. G. S. L. Brandão and M. B. Plenio, Comm. Math. Phys. 295, 829 (2010).
12 F. G. S. L. Brandão, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Phys. Rev. Lett. **111**, 250404 (2013).
13 N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
14 E. G. Cavalcanti, S. J. Jones, H. M. Wiseman and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).
15 W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
16 A. K. Ekert, Phys. Rev. Lett. **67**, 661(1991).
17 R. Gallego and L. Aolita. The resource theory of steering. arXiv:1409.5804 (2014).

18 R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués. Phys. Rev. Lett. **109**, 070401 (2012).

19 G. Gour and R. W. Spekkens, New J. Phys. **10**, 033023 (2008).

20 V. Händchen *et al.*, Nat. Phot. **6**, 598 (2012).

21 Q. Y. He and M. D. Reid, Phys. Rev. Lett. **111**, 250403 (2013).

22 R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

23 S. J. Jones *et al.*, Phys. Rev. A **76**, 052116 (2007).

24 I. Kogias, A. R. Lee, S. Ragy and G. Adesso, arXiv:1410.1637 (2014).

25 B. Lang, T. Vertesi and M. Navascués, arXiv:1402.2850 (2014).

26 F. Levi and F. Mintert, New J. Phys. **16**, 033007 (2014).

27 M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).

28 O. Oreshkov and J. Calsamiglia. Phys. Rev. A **79**, 032336 (2009).

29 Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992).

30 M. Owari, K. Matsumoto, and M. Murao, Phys. Rev. A **70**, 050301(R) (2004).

31 M. Piani and J. Watrous, arXiv:1406.0530 (2014).

32 M. B. Plenio and S. Virmani, Quant. Inf. Comput. **7**, 1 (2007).

33 M. F. Pusey, Phys. Rev. A **88**, 032313 (2013).

34 M. D. Reid, P. D. Drummond, W. P. Bowen, E. G. Cavalcanti, P. K. Lam, H. A. Bachor, U. L. Andersen, and G. Leuchs, Rev. Mod. Phys. **81**, 1727 (2009).

35 D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Nat. Phys. **6**, 845 (2010).

36 P. Skrzypczyk, M. Navascués, and D. Cavalcanti, Phys. Rev. Lett. **112**, 180404 (2014).

37 D.-H. Smith *et al.*, Nat. Commun. **3**, 625 (2012).

38 E. Schrödinger, Proc. Camb. Phil. Soc. **31**, 555 (1935).

39 S. Steinlechner, J. Bauchrowitz, T. Eberle, and R. Schnabel, Phys. Rev. A **87**, 022104 (2013).

40 V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

41 J. I. de Vicente, J. Phys. A: Math. Theor. **47**, 424017 (2014).

42 G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).

43 H. M. Wiseman, S. J. Jones and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

44 B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. Wiseman, R. Ursin, A. Zeilinger, New J. Phys. **14**, 053030 (2012).