

Coherent control of quantum systems as a resource theory

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2016 Quantum Sci. Technol. 1 01LT01

(<http://iopscience.iop.org/2058-9565/1/1/01LT01>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 84.233.183.161

This content was downloaded on 15/08/2016 at 15:37

Please note that [terms and conditions apply](#).

Quantum Science and Technology



LETTER

Coherent control of quantum systems as a resource theory

RECEIVED
15 March 2016

REVISED
14 June 2016

ACCEPTED FOR PUBLICATION
28 June 2016

PUBLISHED
12 August 2016

J M Matera^{1,2,3}, D Egloff^{1,3}, N Killoran¹ and M B Plenio¹

¹ Institut für Theoretische Physik and IQST, Albert-Einstein-Allee 11, Universität Ulm, D-89069 Ulm, Germany

² Departamento de Física-IFLP, Universidad Nacional de La Plata, C.C. 67, La Plata 1900, Argentina

³ These authors contributed equally to this work.

E-mail: matera@fisica.unlp.edu.ar and dario.egloff@uni-ulm.de

Keywords: resource theories, coherence, entanglement, discord, quantumness, quantum computation

Abstract

Control at the interface between the classical and the quantum world is fundamental in quantum physics. In particular, how classical control is enhanced by coherence effects is an important question both from a theoretical as well as from a technological point of view. In this work, we establish a resource theory describing this setting and explore relations to the theory of coherence, entanglement and information processing. Specifically, for the coherent control of quantum systems, the relevant resources of entanglement and coherence are found to be equivalent and closely related to a measure of discord. The results are then applied to the DQC1 protocol and the precision of the final measurement is expressed in terms of the available resources.

Introduction

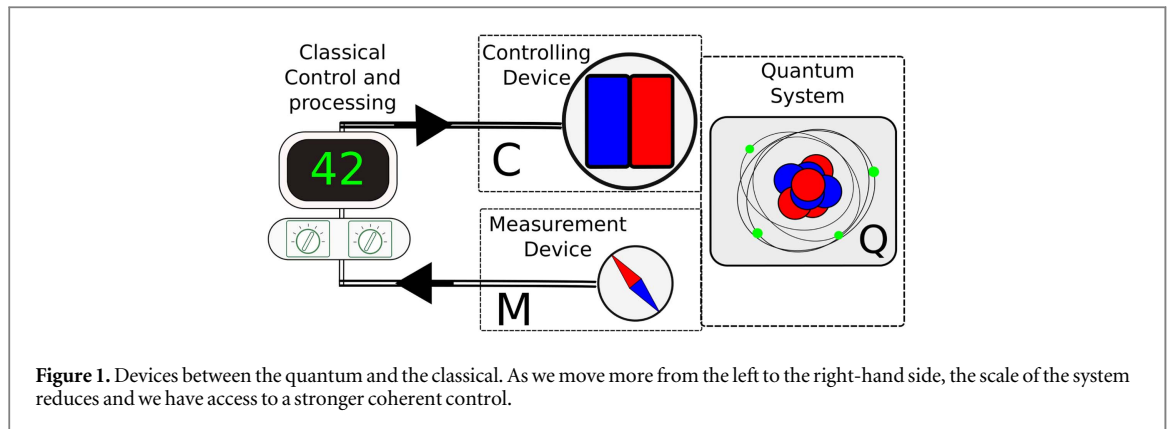
Coherent superposition is a defining characteristic of the quantum world. Coherence indicates the fundamental misalignment, or noncommutativity, between quantum states and the interactions or observables which we may use to probe them. Due to its intimate connection with quantum superposition, coherence is also important in a large number of quantum information protocols. In fact, coherence can be seen as a type of *resource*, allowing one to perform tasks that would be more difficult or not possible otherwise. Indeed, coherence has recently been developed into a formal quantum resource theory [1–14]⁴, similar to that for entanglement [20, 21].

In the macroscopic classical world, where states and observables commute, superposition effects are suppressed and physical systems can be described without coherence using classical probability distributions. Yet some special systems, often found at mesoscopic scales, can exist in the murky borderlands between the classical and quantum worlds. In fact, systems that bridge between these worlds are very important in modern experiments. Operationally, it is common to employ intermediary physical systems, such as lasers, magnetic fields, or photodiodes, to interface with a separate ‘target’ quantum system. By coupling to the target system, these mediator systems can function as state preparation, control, and measurement devices.

To interact meaningfully with the controlled system, the mediator systems must themselves be able to exert a nonclassical effect on their targets. At the same time, they must also interface with the classical world to communicate human- or machine-readable instructions and measurement outcomes. Through this, they are inevitably exposed to classical noise and decoherence effects which makes the creation and the conservation of coherence a costly task. Recognising that coherence is a potential resource, we might ask what value might be gained if we were to pay these costs and what potential quantum advantages do coherent resources provide in this standard operational paradigm?

In this work, we address these questions by formalizing a resource theory for the tasks of preparing, controlling, and measuring quantum systems, and explore the differences between having incoherent versus coherent resources at our disposal. Within this framework, coherence and entanglement can be freely

⁴ Another possible approach to coherence theory [15, 16] is based on the theory of reference frames [17, 18], which proved useful in quantum thermodynamics [19].



interconverted and thus represent the same underlying resource, which we call the *recoverable coherence*. We introduce a quantifier for this resource and connect it to measures of quantum discord [22–25]. Finally, we illustrate these ideas through an application to the family of quantum algorithms known as ‘Deterministic Quantum Computation with one qubit’ (DQC1) proposed in [26]. In the last decade, this family of algorithms has instigated a lively debate as to what is the quantum resource behind the speed-up obtained with quantum algorithms, as DQC1 can be implemented even with a very small amount of entanglement [14, 27–31]. We show how the accuracy of the outcome in DQC1 can be quantified in terms of the recoverable coherence, and how this connects with entanglement and discord. We discuss connections with related works in the section defining the resource theory and in the [appendix](#).

The framework

To motivate the following framework, we start by considering a generic experimental set-up for controlling a quantum system (see figure 1). Humans can only interact mechanically with macroscopic objects, therefore one part of any experiment needs to be macroscopic, be it only the keyboard of a computer. This part is fully described by classical physics. To model this in quantum mechanics, following [1] we say that the state of a system is incoherent if it is diagonal in a fixed basis.

Definition 1. Given a system A and a fixed orthonormal basis $\mathcal{Z} = \{|c\rangle\}_{c=0}^{D-1}$, we call a state ρ incoherent (with respect to \mathcal{Z}) if $\rho = \sum_c p_c |c\rangle\langle c|$ for some $p_c \geq 0$, where $\sum_c p_c = 1$.

Secondly, there are some experimental devices that allow us to operate on the full quantum system. These intermediary devices are usually in the mesoscopic domain, because we want to manipulate their operating parameters in a deterministic way and, at the same time, use them to manipulate microscopic quantum system. Because of their size, it is an operationally hard task to bring these devices controllably into a coherent superposition that remains stable against decoherence. To cast this situation into a resource theory perspective, it is advantageous to assume that only incoherent operations are available and all required coherence is supplied by a third party. For this reason, we might think of coherence as a resource for the manipulation of the controlling devices. Following [1], we thus define⁵:

Definition 2. We call a quantum operation incoherent if each of its Kraus operators K_α is incoherent. That is, for any σ incoherent, $K_\alpha \sigma K_\alpha^\dagger$ is incoherent.

We want to use these intermediary devices to *control* a quantum system, and in the best case we can have perfect quantum control. We must keep in mind that the controlling devices decohere quickly due to their size. Therefore, it might be hard to encode information in a control basis that is not the incoherent one and still have a stable quantum control. The best stable control we can hope for is therefore given by the unitary

$$U_{control} = \sum_c |c\rangle\langle c| \otimes U_c. \quad (1)$$

We also assume that we can add ancillae to the quantum system and that we can trace out parts of the system, i.e. we can *prepare* and *discard* parts of it.

⁵ See the [appendix](#) for a brief discussion on this choice.

Ultimately, we might wish to *measure* the quantum system. We therefore include a measurement device, which couples to the quantum system, performs any measurement of the quantum system, and sends the classical measurement result to a computer. This is described by

$$|0\rangle \langle 0| \otimes \rho \mapsto \sum_c |c\rangle \langle c| \otimes K_c \rho K_c^\dagger, \quad (2)$$

where the left-hand side of the tensor product denotes a register in the computer's memory and the right-hand side is the state of the quantum system.

We note that incoherent operations include anything one can do with a computer. Because we focus on the control of a quantum system in this paper, we only need to consider two systems: the controlling system A, on which we can do any incoherent operations for free, and the quantum system B, for which we have full quantum control, including measurements. In this way, the complete family of allowed operations in our framework is defined as follows.

Definition 3. Consider a bipartite system AB . The class of Global Operations Incoherent on A , with respect to the local orthonormal basis $\mathcal{Z} = \{|c\rangle\}$ on A (abbreviated as $GOIA_{\mathcal{Z}}$), is the family of quantum channels consisting of (finite) combinations of

1. Incoherent operations on A (def. 2),
2. Controlled operations in the incoherent basis from A to B (equation (1)),
3. Adding or removing (tracing out) ancillae on B , and
4. Measurement and postselection on B (equation (2)).

Notice that if we extend this set of operations by allowing general unitary operations on A , we recover the full set of quantum operations on AB .

The resource theory

Having defined the free operations, we need to address what are the free and the resource states in the framework and investigate how these resources can be distilled if someone provides a source of non-free states.

Free states

With $\mathcal{Z} = \{|c\rangle\}$ as the incoherent basis of A , we can prepare any state of the form $\rho_0 = \sum_c p_c |c\rangle \langle c|_A \otimes |0\rangle \langle 0|_B$ using only incoherent operations on A . Performing controlled operations (equation (1)) on ρ_0 (with the aid of ancillary states), we can prepare any state in the set of \mathcal{Z} -classical-quantum states [9],

$$CQ_{\mathcal{Z}} := \{\rho | \rho = \sum_c p_c |c\rangle \langle c| \otimes \rho_c, \quad |c\rangle \in \mathcal{Z}\}, \quad (3)$$

where the ρ_c are arbitrary quantum states. Conversely, any operations in the $GOIA_{\mathcal{Z}}$ framework conserve this set. The largest set of operations that preserves the set of classical-quantum states $CQ_{\mathcal{Z}}$ was defined in [14]. While all of our operations are inside that set, the converse remains an open question. Using the physical picture we have introduced, we can link together other seemingly disparate recent works in the field [7–14] (see the [appendix](#) for a brief overview and also see the related independent work [32], which discusses a different subset of the $CQ_{\mathcal{Z}}$ -preserving operations [14]).

Most notably, in [9] the subset of the bipartite operations on AB , that can be performed *locally*, only with the aid of classical communication (the Local Quantum-Incoherent operations and Classical Communication, $LQICC_{\mathcal{Z}}$) was introduced. These operations are a strict subset of $GOIA_{\mathcal{Z}}$: we get them by restricting the control to be performed by local operations on B , conditional to measurements outcomes on A . The connections will prove useful to unravel the resource theory defined by $GOIA_{\mathcal{Z}}$, which is done in the following sections.

Coherence as a resource

Now, we determine the set of resource states in our framework, i.e. the set of states that makes $GOIA_{\mathcal{Z}}$ operations universal. To this end, we first note that from a supply of maximally coherent states $|+\rangle$ on A we are able to implement any local operation on A [1]. Secondly, the supply of $|+\rangle$ on A also allows for the generation of entanglement between A and B by application of equation (1). Thirdly, the provision of arbitrary local operations on A and B and arbitrary amounts of entanglement between A and B allows for the generation of arbitrary joint operations between A and B [33] (see also [11]). In particular, by applying a CNOT (included in

the $GOIA_{\mathcal{Z}}$, but not in the $LQICC_{\mathcal{Z}}$ -operations), one can create a pure maximally entangled state (a singlet) from a maximally coherent state [7] and one can steer an incoherent state to a maximally coherent one under $LQICC_{\mathcal{Z}}$ operations by using up a singlet state [12]. Therefore, the pure resource states can be produced from one another with $GOIA_{\mathcal{Z}}$ operations.

We can now ask how many resource states one can distill from n copies of a given state.

Definition 4. Let $r^\epsilon(\rho, n) \cdot n$ be the maximal number of fully coherent qubit states (on subsystem A) that can be prepared from n copies of the state ρ_{AB} with fidelity at least $1 - \epsilon$, by applying maps $\Lambda \in GOIA_{\mathcal{Z}}$:

$$r^\epsilon(\rho, n) := \sup_{\Lambda \in GOIA_{\mathcal{Z}}} \{R \mid F(\Lambda(\rho^{\otimes n}), |+\rangle\langle +|^{\otimes nR}) \geq 1 - \epsilon\}.$$

The recoverable coherence (with respect to the basis \mathcal{Z}) is the infinite-copy and infinitesimal error limit of the above maximal ratio:

$$C_{\mathcal{Z}}^{REC}(\rho) = \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} r^\epsilon(\rho, n). \quad (4)$$

As entangled and coherent resource states can be interconverted, the analogous notion of recoverable entanglement coincides with $C_{\mathcal{Z}}^{REC}$:

$$E_{\mathcal{Z}}^{REC}(\rho) \equiv C_{\mathcal{Z}}^{REC}(\rho). \quad (5)$$

Notice that these quantities are not equivalent to the distillable entanglement [20]. Moreover, they are not entanglement monotones [34], as $GOIA_{\mathcal{Z}}$ allows to convert product states (not incoherent on A) into entangled states. However, for pure states, distillable entanglement is a lower bound to the distillable entanglement under $GOIA_{\mathcal{Z}}$ ⁶. We give general lower bounds to the distillable coherence in the [appendix](#). As was noticed in [9], for any state outside of $CQ_{\mathcal{Z}}$, there is a protocol in $LQICC_{\mathcal{Z}} \subset GOIA_{\mathcal{Z}}$ which allows the recovery of some amount of coherence. Hence, there is no bound coherence or entanglement in $GOIA_{\mathcal{Z}}$.

A monotone for $C_{\mathcal{Z}}^{REC}$

A next natural step in the resource theory is to introduce a monotone that quantifies the distance to the free states. A particularly suitable measure is provided by the relative entropy:

$$\Delta_{\mathcal{Z}}(\rho) = \min_{\sigma \in CQ_{\mathcal{Z}}} S(\rho \parallel \sigma) = S(\rho') - S(\rho), \quad (6)$$

where $S(\rho \parallel \sigma) = \text{Tr}[\rho(\log_2(\rho) - \log_2(\sigma))]$, $S(\rho) = -\text{Tr}[\rho \log_2 \rho]$ is the von Neumann entropy and $\rho' = \sum_c |c\rangle\langle c| \otimes \mathbb{1} \rho |c\rangle\langle c| \otimes \mathbb{1}$ is the state obtained from ρ by completely decohering with respect to the basis \mathcal{Z} (see lemma 1 in the [appendix](#)).

The functional $\Delta_{\mathcal{Z}}$ is additive, convex, and monotonic under $GOIA_{\mathcal{Z}}$ on average. Proofs of these properties are presented in the [appendix](#) in lemma 2, 3 and proposition 1. Most importantly, it upper bounds $C_{\mathcal{Z}}^{REC}$ via (see the [appendix](#) for a proof).

$$\Delta_{\mathcal{Z}}(\rho) \geq C_{\mathcal{Z}}^{REC}(\rho). \quad (7)$$

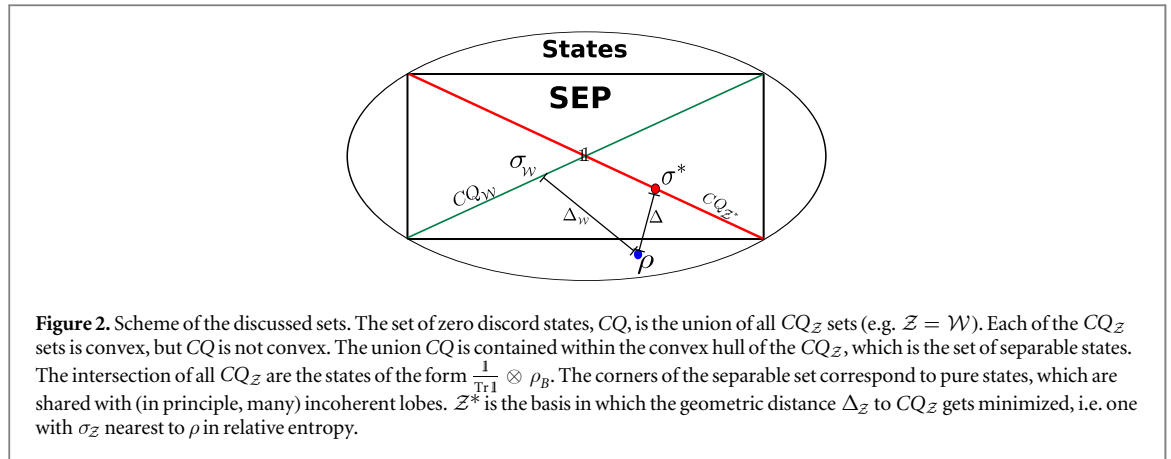
This sharpens a similar result of [9], where the free operations defining $C_{\mathcal{Z}}^{REC}$ on the right-hand side were the more restrictive $LQICC_{\mathcal{Z}}$ operations. Still, because $LQICC_{\mathcal{Z}}$ is strictly included in $GOIA_{\mathcal{Z}}$, the bounds derived in [9, 11] are valid for our framework and we get that equation (7) is tight for maximally correlated states ($\rho = \sum_{cc'} \rho_{cc'} |c\rangle\langle c'| \otimes |c\rangle\langle c'|$ [36, 37]) and for product states [9] (where the recoverable coherence is just the distillable coherence on the A -part calculated in [2]), as well as for general pure states [11] (as the proofs simplify in our framework, we show them nonetheless in the [appendix](#)). The bound is also tight for quantum–classical states. We have to leave open the question of whether the bound can be reached in general.

Basis-independent recoverable coherence and discord

In the previous section, we presented a framework that specifies coherence in some fixed basis \mathcal{Z} . However, it might be useful in some contexts to work without this constraint. The natural extension would then be to ask what is $C_{\mathcal{Z}}^{REC}$ of the state in the most unfavourable case⁷. For product states, it is clear that the choice of the

⁶ For pure states, the protocol described in [35] for entanglement distillation can be performed, as it requires full quantum control just on one side. This shows that the entanglement entropy provides a lower bound.

⁷ At first glance, the maximum recoverable coherence might also seem to be a meaningful quantity. However, it depends strongly on the dimensionality of the basis, and would be saturated for any pure state by choosing as the incoherent basis the one conjugate to the local Schmidt basis.



eigenbasis of ρ_A is the worst case. In general, this does not need to be the case. For instance, consider the state

$$\rho = \epsilon |\uparrow\rangle\langle\uparrow| \otimes |\uparrow\rangle\langle\uparrow| + \frac{1-\epsilon}{2} (|\leftarrow\rangle\langle\leftarrow| \otimes |\uparrow\rangle\langle\uparrow| + |\rightarrow\rangle\langle\rightarrow| \otimes |\downarrow\rangle\langle\downarrow|).$$

In the limit $\epsilon \rightarrow 0$, $C_Z^{REC} \rightarrow 1$ using the local eigenbasis $Z = \{|\downarrow\rangle, |\uparrow\rangle\}$, yet $C_{Z'}^{REC} \rightarrow 0$ for the choice $Z' = \{|\leftarrow\rangle, |\rightarrow\rangle\}$. With this in mind, we define the *basis-independent recoverable coherence*

$$C_{\min}^{REC}[\rho] = \min_Z C_Z^{REC}(\rho), \tag{8}$$

as the minimum recoverable coherence regarding the most unfavourable basis. Due to equation (7), we obtain

$$C_{\min}^{REC}[\rho] \leq \min_Z \Delta_Z(\rho) = \Delta^{A \rightarrow B}(\rho). \tag{9}$$

That is, the basis-independent recoverable coherence is upper bounded by the thermal discord $\Delta^{A \rightarrow B}(\rho)$ (also called one-way information deficit). Thermal discord represents the difference between the work that can be extracted from a system in the state ρ by performing either global or local operations on A [38, 39]. Additionally, it corresponds to a particular case of a measure of *discord*, a type of non-classicality of a quantum state beyond the notion of entanglement [22–25], quantifying how much a given state fails to belong to the set of Classical-Quantum or pointer states [22, 40]:

$$CQ := \bigcup_Z CQ_Z. \tag{10}$$

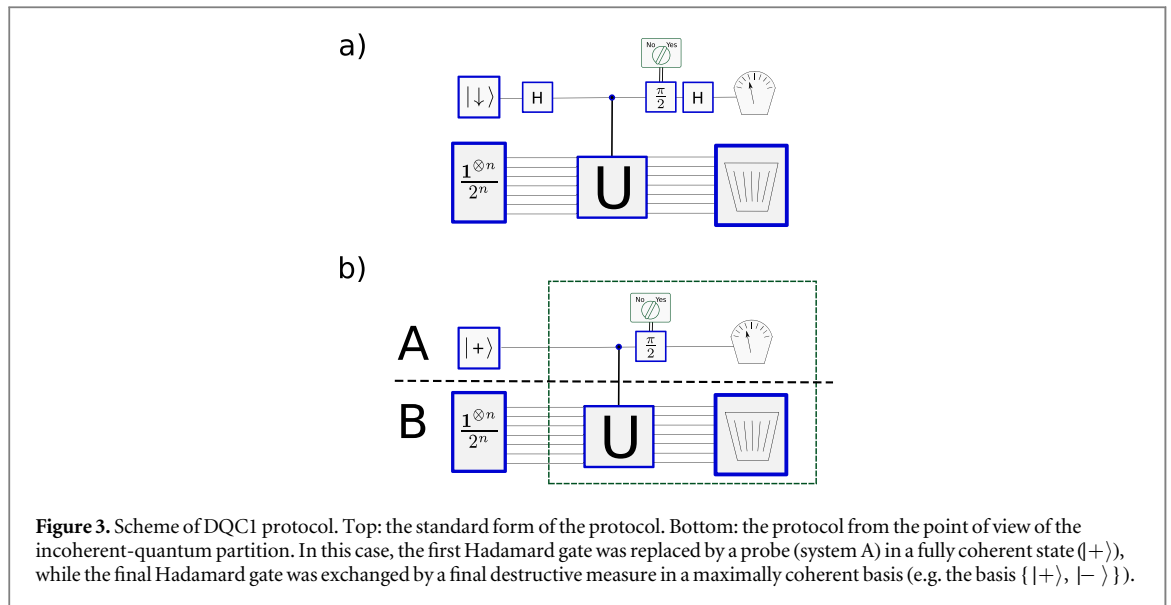
See figure 2 for a picture of the relevant sets. The most prominent features of discord quantifiers are [24] their

- Vanishing, if the state is in CQ, and
- Invariance under local unitaries.

Therefore, discord quantifiers are asymmetric with respect to the swap of A and B . One may also ask that a discord quantifier is non-negative, bounded from above by the entropy of ρ_A and suitably normalized, such that the measure coincides with the entanglement for the singlet state in the qubit case. We note that the basis-independent recoverable coherence C_{\min}^{REC} is also a discord quantifier, as it has the above-mentioned properties. For pure states, distillable entanglement is the same as thermal discord [35], which is an upper bound for the basis-independent recoverable coherence, which in turn is an upper bound for entanglement as noted above. So, for pure states, these quantities all coincide (also see [9] for a different argument).

Application to the DQC1 protocol

In this section, we apply the above-mentioned results to analyse the resources involved in the DQC1 protocol [26, 29]. The goal of DQC1 is to determine the trace of a n -qubit unitary operator U , which is a very challenging task in the realm of classical physics. The DQC1 protocol accomplishes this task by making use of a maximally coherent control qubit $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ as a probe and a maximally mixed state on the remaining target system (see figure 3). After the action of the controlled unitary $|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U$, the state of the probe encodes the trace of the unitary in the coherent bases $\left(\left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\} \text{ and } \left\{ \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \right\} \right)$. Measuring the probe in these bases ends the protocol. Of course, to read out the result, we need to perform repeated measurements of the final state, implying that we need to repeat the protocol many times to gain a certain degree of accuracy. If the initial state is not maximally coherent, we are still able to perform the algorithm, but we need a



larger number of runs to reach the same precision [30]. Interestingly, the protocol remains efficient also in the case of probes in a highly mixed state, even when the bipartite entanglement between the probe and any part of the system is small or even vanishes during the entire protocol. This observation provided motivation to look at different measures of quantumness, such as multipartite entanglement [27] and quantum discord [14, 29]. But while it is not clear why one should look for multipartite entanglement in a setting that physically is bipartite, quantum discord is problematic as a resource because the zero discord set is not convex, thus mixing two zero discord states (which amounts to forgetting which of the two one prepared) can provide some non-zero discord state (see figure 2). On the other hand, as was pointed out in [14], the minimal requirement for the DQC1 protocol to work is the presence of some amount of coherence in the probe. We can make this statement more precise by remembering that, to obtain the expectation value which encodes $\text{Tr } U$, the protocol should be performed many times, consuming on each run a fresh qubit probe [29]. The number of runs needed to reach some desired precision depends directly on the degree of coherence of the probe. Suppose we have m copies of the joint initial state $\rho = \rho_0 \otimes \mathbb{1}_{\text{target}}/\text{dim}$, where dim is the dimension of the target system and ρ_0 is the (general) qubit state of the probe before applying the controlled unitary. We show in the appendix that the precision (i.e. the number of binary significant digits) of the estimated $\text{Tr } U$ is (up to a constant) given by a function of $C_{\mathcal{Z}}^{\text{REC}}$, i.e.:

$$\text{prec}(\text{Tr } U) \approx -\log_2 \left| \text{SE} \left(\frac{\text{Tr } U}{\text{dim}} \right) \right| \approx \frac{1}{2} \log_2 (C_{\mathcal{Z}}^{\text{REC}}(\rho_0)), \quad (11)$$

where $\text{SE}(\hat{x})$ denotes the *standard error of the mean* [41] associated to the random variable \hat{x} .

Notice that in the present formalism, entanglement and coherence are interconvertible, so the amount of bipartite entanglement that can be produced during the protocol between the probe and any part of the target system is bounded by $C_{\mathcal{Z}}^{\text{REC}}(\rho)$ for any state ρ of the total system at any stage of the protocol. We note that if at any point in the protocol any discord quantifier is non-zero, this implies that the state is not quantum–classical and therefore $C_{\mathcal{Z}}^{\text{REC}}$ is non-zero. By the monotonicity of $C_{\mathcal{Z}}^{\text{REC}}$ under $\text{GOIA}_{\mathcal{Z}}$, we find that the state of the probe at the beginning cannot have been incoherent. Therefore, any discord quantifier is a witness for recoverable coherence and the applicability of the DQC1 protocol.

Conclusion

In this work, a framework for the description of incoherent systems controlling quantum systems is proposed. The set of operations over the composite system ($\text{GOIA}_{\mathcal{Z}}$), together with its associated minimal invariant set, define a formal resource theory in which the resource is the amount of coherence that can be recovered on the control side. Using the connections with other frameworks [7–14], we extend many of the previous results to the $\text{GOIA}_{\mathcal{Z}}$ framework and show that the associated resources, the recoverable coherence, and recoverable entanglement are equivalent. We upper bounded $C_{\mathcal{Z}}^{\text{REC}}$ by a geometric functional and found that the latter is a monotone of the theory. By looking at the least favourable choice of the incoherent basis, the amount of resource associated to a given state is a discord quantifier. This quantifier is bounded from above by the thermal discord of

the state. Finally, we exemplified our findings by calculating the precision of the DQC1 protocol with a mixed control qubit and stated it in terms of the resource of our theory—the recoverable coherence.

Acknowledgments

We gratefully acknowledge discussions with Andrea Smirne and Antony Milne. M M is supported by CONICET. D E, N K and M B P are supported by an Alexander von Humboldt Professorship, the ERC Synergy Grant BioQ, and the EU project QUCHIP and EQUAM.

Appendix. Related works

One of the first papers relating coherence with entanglement was [7], in which the authors looked at how one can restrict coherence theory further by splitting the space of free states into two incoherent parts. This gives rise to control operations, and thus allowed operations that can produce entanglement by using up coherence. This line of thought was further developed in [8], where the authors showed an equality between symmetric discord [42] and coherence in such a framework. Another approach was taken in [6], relating a more general form of superpositions than coherence to entanglement via control gates. In [9] the authors instead looked at possible extensions of coherence theory and introduced the framework of local operations and classical communication ($LQICC_{\mathcal{Z}}$). This and modifications thereof were subsequently discussed in [10, 11], which were mostly concerned with the relation of coherence to entanglement and structure of the respective theories. After these [12, 13] analysed steering-induced coherence in the $LQICC_{\mathcal{Z}}$ framework and defined a measurement induced disturbance measure for coherence, to some extent related to discord. Finally, [14] defined the set of quantum operations that preserve the form of incoherent-quantum states. In a subsequent work [32], a subset of these operations was analysed independently of this letter.

Choice of the incoherent operations

In our theory of coherent control of a quantum system, we need to choose which theory inside quantum mechanics corresponds best to a classical theory of labels, i.e. we need to specify the theory of coherence we choose to model the free operations on the ‘classical’ side A of our set-up. Clearly, we need to ensure that no coherence is produced, i.e. we only consider maps which, starting from an arbitrary incoherent state, result in yet another incoherent state (even after a possible postselection). This leads to the coherence theory defined in [1] and used here. One could now argue that one should restrict the allowed operations further. Indeed, there is by now an entire hierarchy of proposals of possible theories (see e.g. the appendix of [43] for an overview), but the discussion of which is the most meaningful is far from settled yet (and context-dependent). We adopted our current choice of model principally because it allows for a particularly wide class of operations and hence will give particularly strict bounds in the sense that a process that is impossible under this set will also be impossible under essentially all other possible choices of coherence theory.

A totally different choice would be the theory of $U(1)$ -covariance [15], which has been successfully applied in the context of thermal operations (see e.g. [19]). The reason we do not use it here is simple: permutations are not allowed operations there (unless on degenerate subspaces), but as this only requires changing labels in our setting, it should be allowed.

Proofs

Here, the proofs of the properties presented in the main text are shown.

Lemma 1 (Minimal relative entropy to $CQ_{\mathcal{Z}}$ — equation (6). Also see [9] based on arguments of [42]). Let $\{\Pi_c = |c\rangle\langle c| \otimes \mathbb{1}\}$ be the set of projectors on the incoherent basis \mathcal{Z} on A . Then:

$$\Delta_{\mathcal{Z}}(\rho) = S\left(\rho \left\| \sum_c \Pi_c \rho \Pi_c\right.\right). \quad (12)$$

Proof. We start by observing that $S(\rho||\sigma)$ is a convex function of σ (for fixed ρ), and hence, the global minimum σ^* is the unique stationary point of that function (and it exists). Let us start the calculation of the stationary points, by parameterising σ by an exponential map: let $\{\mathbf{o}_k\}$ be a basis for the sub-algebra of (zero trace)

hermitian operators in AB satisfying the condition $[\Pi_c, \mathbf{o}_k] = 0$. It is clear that any full-rank state $\sigma \in CQ_Z$ can be written as $\sigma = \exp(-\mathbf{h})/Z$, with $Z = \text{Tr} \exp(-\mathbf{h})$ and $\mathbf{h} = \sum_k \lambda_k \mathbf{o}_k$. Notice that non-full-rank states can be reached as a limit. In this parameterisation, the stationary conditions reduce to

$$\text{Tr}(\rho \mathbf{o}_k) - \text{Tr}(\sigma^* \mathbf{o}_k) = 0.$$

This implies that for the global minimum σ^* , and for any observable \mathbf{O} , $\text{Tr}[\rho \sum_c \Pi_c \mathbf{O} \Pi_c] = \text{Tr}[\sum_c \Pi_c \rho \Pi_c \mathbf{O}]$ has to equal $\text{Tr}[\sigma^* \mathbf{O}]$. Therefore, the global minimum is $\sigma^* = \sum_c \Pi_c \rho \Pi_c$. □

Properties of Δ_Z — Notice that from lemma 1, it follows that the monotone Δ_Z is the same as the recoverable coherence in the basis Z by incoherent operations [2] $\Delta_Z(\rho_A \otimes \rho_B) = C_Z(\rho_A)$ and that the monotone is additive:

Lemma 2 Additivity.

$$\Delta(\rho^n) = n\Delta(\rho). \tag{13}$$

Proof.

$$\begin{aligned} \Delta(\rho^{\otimes n}) &= S\left(\rho^{\otimes n} \left\| \sum_{c_1, c_2, \dots, c_n} \Pi_{c_1, c_2, \dots, c_n} \rho^{\otimes n} \Pi_{c_1, c_2, \dots, c_n}\right.\right) \\ &= S\left(\rho^{\otimes n} \left\| \left(\sum_c \Pi_c \rho \Pi_c\right)^{\otimes n}\right.\right) \\ &= nS\left(\rho \left\| \left(\sum_c \Pi_c \rho \Pi_c\right)\right.\right) = n\Delta(\rho). \end{aligned}$$

□

We can also verify that Δ_Z is convex:

Lemma 3 Convexity.

$$\Delta_Z\left(\sum_i p_i \rho_i\right) \leq \sum_i p_i \Delta_Z(\rho_i). \tag{14}$$

Proof. For each i , $\Delta_Z(\rho_i) = S(\rho_i \|\sigma_i)$ for certain $\sigma_i \in CQ_Z$, therefore

$$\begin{aligned} \Delta_Z\left(\sum_i p_i \rho_i\right) &= \min_{\sigma \in CQ_Z} S\left(\sum_i p_i \rho_i \left\| \sigma\right.\right) \\ &\leq S\left(\sum_i p_i \rho_i \left\| \sum_i p_i \sigma_i\right.\right) \\ &\leq \sum_i p_i S(\rho_i \|\sigma_i). \end{aligned}$$

□

Now, we can show that this quantity is non-increasing under $GOIA_Z$:

Proposition 1 (Monotonicity on average).

$$\Delta_Z(\Lambda(\rho)) \leq \Delta_Z(\rho) \quad \forall \Lambda \in GOIA_Z, \text{ CPTP}. \tag{15}$$

Proof. We start noticing that if Λ is in $GOIA_Z$, $\Lambda(CQ_Z) \subset CQ_Z$. Therefore,

$$\begin{aligned} \Delta_Z(\Lambda(\rho)) &= \min_{\sigma \in CQ_Z} S(\Lambda(\rho) \|\sigma) \\ &\leq \min_{\sigma \in \Lambda(CQ_Z)} S(\Lambda(\rho) \|\sigma) \\ &= \min_{\sigma \in CQ_Z} S(\Lambda(\rho) \|\Lambda(\sigma)) \\ &\leq \min_{\sigma \in CQ_Z} S(\rho \|\sigma) = \Delta_Z(\rho), \end{aligned}$$

where the last inequality follows from the monotonicity of the relative entropy under CPTP maps [44]. □

Proof of the geometric upper bound (equation (7))

Here, we present the proof of equation (7), stating that the geometric monotone defined by the relative entropy to the free states, upper bounds $C_{\mathcal{Z}}^{REC}$.

Proof. Let Λ_n be the optimal $GOIA_{\mathcal{Z}}$ map that produces from the state ρ , m_n copies of the state $|\Psi\rangle$, ϵ -near in fidelity to $|+\rangle$:

$$\Lambda_n(\rho^n) = |\Psi\rangle\langle\Psi|^{\otimes m_n}.$$

Now, we observe that up to order ϵ (using the continuity of the fidelity and of the von Neumann entropy as functions of the state):

$$\begin{aligned} m_n &= S\left(\text{Tr}_R \Lambda(\rho^{\otimes n}) \left\| \text{Tr}_R \sum_c \Pi_c \Lambda(\rho^{\otimes n}) \Pi_c\right.\right) \\ &\leq S\left(\Lambda(\rho^{\otimes n}) \left\| \sum_c \Pi_c \Lambda(\rho^{\otimes n}) \Pi_c\right.\right) \\ &= \Delta_{\mathcal{Z}}(\Lambda(\rho^{\otimes n})) \\ &\leq \Delta_{\mathcal{Z}}(\rho^{\otimes n}) \\ &= n\Delta_{\mathcal{Z}}(\rho). \end{aligned}$$

The first line follows from the definition of the relative entropy and the second line from the monotonicity of this quantity under the partial trace. The third line follows from the definition of $\Delta_{\mathcal{Z}}$, the fourth line from the monotonicity under $GOIA_{\mathcal{Z}}$ and the last line from additivity (lemma 2).

Now, from the definition of $C_{\mathcal{Z}}^{REC}(\rho)$ (definition 4) we obtain

$$C_{\mathcal{Z}}^{REC}(\rho) = \lim_{\epsilon \rightarrow \infty} \lim_{n \rightarrow \infty} \max_{\Lambda \in GOIA_{\mathcal{Z}}} \frac{m(\Lambda, \rho^n)}{n} \leq \Delta_{\mathcal{Z}}(\rho).$$

□

Lower bounds

A lower bound for $C_{\mathcal{Z}}^{REC}$ is provided by looking at the final coherence obtained after a specific protocol. A subfamily of such protocols consists on performing a measurement on the B side, communicating the outcome, and adding a label to the classical side:

$$\Lambda(\rho_{AB}) = \sum_m |k\rangle\langle k| \otimes ((\mathbb{1} \otimes M_k) \rho_{AB} (\mathbb{1} \otimes M_k)^\dagger),$$

where $\{M_k\}$ defines a POVM. Tracing out B we obtain for the relative entropy of coherence of the final state:

$$C_{\mathcal{Z}}(\text{Tr}_B \Lambda(\rho)) = \sum_k p_k C_{\mathcal{Z}}(\rho_k),$$

with $p_k = \text{Tr}(M_k^\dagger M_k \rho)$, $\rho_k = |k\rangle\langle k| \otimes \text{Tr}_B(M_k^\dagger M_k \rho)$. We can also see that this is the maximum amount of coherence that can be recovered by local means (i.e. in the $LQICC_{\mathcal{Z}}$ framework). Noticing that $C_{\mathcal{Z}}(\text{Tr}_B \Lambda(\rho))$ is a concave function on the set of POVMs on B , we can see that its maximum is attained on the boundary of the set. Following a similar reasoning as in the optimization of discord-like quantities [45], we can reduce the optimization problem to find a set of rank-1 projectors. Moreover, if $\text{rank}(\text{Tr}_B \rho) = r$, the maximum is attained for a POVM with at most r^2 elements.

As a corollary, we can notice that for the set of ‘Quantum–Classical states’ $\rho = \sum_k p_k \rho_k^A \otimes |k\rangle\langle k|_B$ the lower bound coincides with the upper bound $\Delta_{\mathcal{Z}}(\rho)$ and hence, $C_{\mathcal{Z}}^{REC}(\rho) = \Delta_{\mathcal{Z}}(\rho)$.

Non equivalence for $C_{\mathcal{Z}}^{REC}(\rho)$ and $\Delta_{\mathcal{Z}}(\rho)$ in the general case. An open question about $C_{\mathcal{Z}}^{REC}$ is related to its numerical equivalence with the geometric measure for general mixed states. To illustrate the problem, let us consider the mixed state

$$\rho = \frac{|\phi\rangle\langle\phi|_A}{2} \otimes |0\rangle\langle 0|_B + \frac{|\varphi\rangle\langle\varphi|_A}{2} \otimes |+\rangle\langle +|_B$$

with $|\phi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|\varphi\rangle = \frac{|1\rangle+|2\rangle}{\sqrt{2}}$. For this state, $\Delta_{\mathcal{Z}}(\rho) \approx 0.8925$ while $C_{\mathcal{Z}}(\text{Tr}_B \rho) \approx 0.6887$. A better lower bound is given by the previous local protocol involving the optimal measurement on B , followed by adding an ancilla on A . By numerical optimisation over projective measurements on B , a lower bound of $C_{\mathcal{Z}}(\text{Tr}_B \Lambda_{loc} \rho) \approx 0.8167$ was obtained. This number is the best we can obtain by local means in a single shot

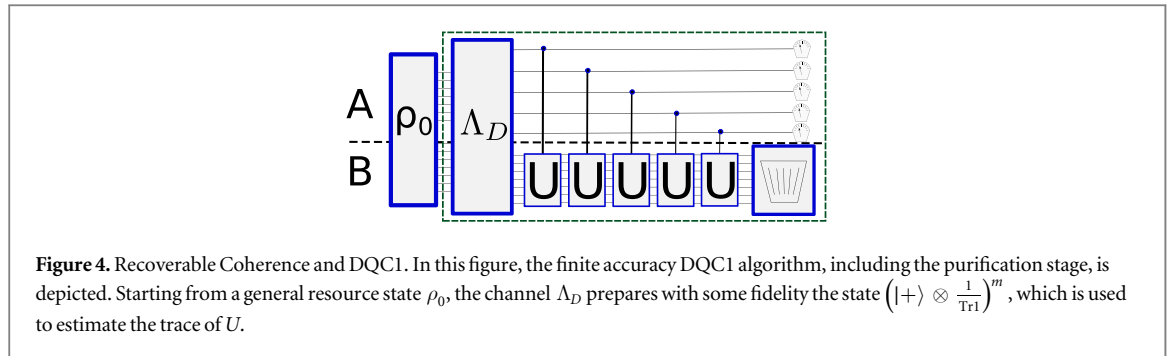


Figure 4. Recoverable Coherence and DQC1. In this figure, the finite accuracy DQC1 algorithm, including the purification stage, is depicted. Starting from a general resource state ρ_0 , the channel Λ_D prepares with some fidelity the state $(|+\rangle \otimes \frac{1}{\text{Tr}U})^m$, which is used to estimate the trace of U .

protocol. However, to evaluate $C_Z^{REC}(\rho)$, we should exhaust every protocol using infinite many copies, which would be possible only by providing a specific upper bound for ρ , and a protocol that saturates it.

Lemma 4 (Recoverable coherence for pure states, also see [11]). If $\rho_{AB} = |\psi\rangle\langle\psi|$ $C_Z^{REC}(\rho_{AB}) = \Delta_Z(\rho_{AB})$.

Proof. We start by noticing that, due to the Schmidt decomposition theorem $|\Psi\rangle = \sum_{\alpha} \lambda_{\alpha} |\alpha\rangle_A |\alpha\rangle_B$ for certain constants $\{\lambda_{\alpha}\}$ and local orthogonal basis $\{|\alpha\rangle_A\}, \{|\alpha\rangle_B\}$. We can bring this state to a locally incoherent maximally correlated state $|\psi'\rangle$ by adding an ancilla on B in a reference state $|0\rangle_B$, followed by the application of a controlled translation operation $T_c = \sum_i |i\rangle\langle i|_A \otimes 1_B \otimes \sum_k |i \oplus k\rangle\langle k|_{B'}$. Because both T_c and its inverse are free operations (being controlled unitaries with incoherent control), by the monotonicity of the upper bound under $GOIA_Z$ -operations we get that, $\Delta_Z(|\psi'\rangle\langle\psi'|) = \Delta_Z(T_c(\rho_{AB} \otimes |0\rangle\langle 0|)T_c^\dagger) = \Delta_Z(\rho_{AB} \otimes |0\rangle\langle 0|) = \Delta_Z(\rho_{AB})$. It follows from the tightness of the bound for maximally correlated states that $\Delta_Z(\rho_{AB}) = \Delta_Z(|\psi'\rangle\langle\psi'|) = C_Z^{REC}(|\psi'\rangle\langle\psi'|) \leq C_Z^{REC}(|\psi\rangle\langle\psi|) \leq \Delta_Z(\rho_{AB})$, and the equality is shown. \square

Proof of equation (11)

In this section we prove equation (11) of the main text,

$$prec\left(\frac{\text{Tr}U}{\text{dim}}\right) \approx -\log_2\left(\text{SE}\left(\frac{\text{Tr}U}{\text{dim}}\right)\right) \approx \frac{1}{2} \log_2(C_Z^{REC}(\rho_0)),$$

We find it instructive to first consider a slight generalisation of the DQC1 protocol, where instead of a source of maximally coherent probes, a general state $\rho_{AB}^{\otimes m}$ is provided (see figure 4). From this state (in the asymptotic limit), we can prepare $n \approx C_Z^{REC}(\rho_{AB}^{\otimes m}) = mC_Z^{REC}(\rho_{AB})$ maximally coherent probes. In DQC1, the estimation of the trace is given by $\frac{\text{Tr}U}{\text{dim}} = \langle\sigma_x\rangle + i\langle\sigma_y\rangle$, being $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$ the x, y Pauli matrices and $\langle\dots\rangle$ the expectation values. If the number of available probes n is large, $\langle\dots\rangle$ can be approximated by the average over the results of the outcomes of the n independent runs of the algorithm $\langle\dots\rangle_n$. In the asymptotic limit, the error introduced by replacing $\langle\dots\rangle$ by $\langle\dots\rangle_n$ is given by the Standard Error of the Mean

$\text{SE}[\sigma_{\mu}] = \sqrt{\frac{\langle\sigma_{\mu}^2\rangle - \langle\sigma_{\mu}\rangle^2}{n}} = \sqrt{\frac{1 - \langle\sigma_{\mu}\rangle^2}{n}}$ with probability $\geq 68\%$ [41]. From this it is straightforward to see that in the asymptotic limit, the precision (i.e. the number of significant (binary) digits) of a number x , $|x| < 1$ goes like:

$$prec(\hat{x}) \approx -\log_2(\text{SE}(\hat{x})).$$

In the same way, we can bound the norm of the error in the estimation of $\frac{\text{Tr}U}{\text{dim}}$ by

$$\text{SE}\left(\frac{\text{Tr}U}{\text{dim}}\right) \approx \sqrt{\text{SE}(\sigma_x)^2 + \text{SE}(\sigma_y)^2} = \sqrt{2 - \left(\left|\frac{\text{Tr}U}{\text{dim}}\right|\right)^2} / \sqrt{n} = \sqrt{2 - \left(\left|\frac{\text{Tr}U}{\text{dim}}\right|\right)^2} / \sqrt{C_Z^{REC}(\rho_{AB}^{\otimes m})}. \text{ But}$$

$1 \leq \sqrt{2 - \left(\left|\frac{\text{Tr}U}{\text{dim}}\right|\right)^2} \leq \sqrt{2}$ and hence $prec \approx -\log_2(\text{SE}(\text{Tr}U/\text{dim})) \approx \frac{1}{2} \log_2 C_Z^{REC}(\rho_{AB}^{\otimes m})$, using this generalized algorithm.

To see that this is indeed the maximum attainable precision for the standard algorithm without the recovering step, let us consider m probes in the general state $\rho_{\text{probe}} = \begin{pmatrix} p & \alpha \\ \alpha & 1-p \end{pmatrix}$, where without loss of generality we

assume $\alpha \geq 0$. For these probes, $\frac{\text{Tr}U}{\text{dim}} = \frac{\langle\sigma_x\rangle + i\langle\sigma_y\rangle}{\alpha}$ while $\text{SE}\left(\frac{\text{Tr}U}{\text{dim}}\right) = \sqrt{\frac{2 - \alpha^2 \left|\frac{\text{Tr}U}{\text{dim}}\right|^2}{\alpha^2 m}}$. Thus,

$$prec_{\alpha} \approx -\log_2\left(\left|\text{SE}\frac{\text{Tr}U}{\text{dim}}\right|\right) \approx -\log_2\frac{\sqrt{2 - |\alpha|^2 \left|\frac{\text{Tr}U}{\text{dim}}\right|^2}}{\sqrt{\alpha^2 m}}.$$

But $m = C_Z^{REC}(\rho_{\text{probe}}^{\otimes m})/C_Z^{REC}(\rho_{\text{probe}})$ and hence,

$$prec_\alpha \approx \frac{1}{2} \log_2(C_Z^{REC}(\rho_{\text{probe}}^{\otimes m})) + \log_2 \sqrt{\frac{\alpha^2 / C_Z^{REC}(\rho_{\text{probe}})}{\left(2 - |\alpha|^2 \left| \frac{\text{Tr} U}{\text{dim}} \right|^2\right)}}.$$

But the second term is a number less or equal than 0 since $\alpha^2 \leq C_Z(\rho_{\text{probe}}) = C_Z^{REC}(\rho_{\text{probe}})$. As this term is finite and independent of m , the correction can be neglected in the asymptotic limit.

References

- [1] Baumgratz T, Cramer M and Plenio M B 2014 Quantifying coherence *Phys. Rev. Lett.* **113** 140401
- [2] Winter A and Yang D 2016 Operational resource theory of coherence *Phys. Rev. Lett.* **116** 120404
- [3] Yuan X, Zhou H, Cao Z and Ma X 2015 Intrinsic randomness as a measure of quantum coherence *Phys. Rev. A* **92** 022124
- [4] Du S, Bai Z and Qi X 2015 Coherence measures and optimal conversion for coherent states *Quant. Inf. Comput.* **15** 1307–16
- [5] Xi Z, Li Y and Fan H 2015 Quantum coherence and correlations in quantum system *Sci. Rep.* **5** 10922
- [6] Killoran N, Steinhoff F E S and Plenio M B 2016 Converting nonclassicality into entanglement *Phys. Rev. Lett.* **116** 080402
- [7] Streltsov A, Singh U, Dhar H S, Bera M N and Adesso G 2015 Measuring quantum coherence with entanglement *Phys. Rev. Lett.* **115** 020403
- [8] Yao Y, Xiao X, Ge L and Sun C P 2015 Quantum coherence in multipartite systems *Phys. Rev. A* **92** 022112
- [9] Chitambar E, Streltsov A, Rana S, Bera M N, Adesso G and Lewenstein M 2016 Assisted distillation of quantum coherence *Phys. Rev. Lett.* **116** 070402
- [10] Chitambar E and Hsieh M-H 2016 Relating the resource theories of entanglement and quantum coherence *Phys. Rev. Lett.* **117** 020402
- [11] Streltsov A, Rana S, Bera M N and Lewenstein M 2015 Hierarchies of incoherent quantum operations arXiv:1509.07456
- [12] Hu X, Milne A, Zhang B and Fan H 2016 Quantum coherence of steered states *Sci. Rep.* **6** 19365
- [13] Hu X and Fan H 2015 Coherence extraction from measurement-induced disturbance arXiv:1508.01978
- [14] Ma J, Yadin B, Girolami D, Vedral V and Gu M 2016 Converting coherence to quantum correlations *Phys. Rev. Lett.* **116** 160407
- [15] Marvian I and Spekkens R W 2014 Modes of asymmetry: the application of harmonic analysis to symmetric quantum dynamics and quantum reference frames *Phys. Rev. A* **90** 062110
- [16] Åberg J 2014 Catalytic coherence *Phys. Rev. Lett.* **113** 150402
- [17] Bartlett S D, Rudolph T and Spekkens R W 2007 Reference frames, superselection rules, and quantum information *Rev. Mod. Phys.* **79** 555–609
- [18] Gour G and Spekkens R W 2008 The resource theory of quantum reference frames: manipulations and monotones *New J. Phys.* **10** 033023
- [19] Lostaglio M, Jennings D and Rudolph T 2015 Description of quantum coherence in thermodynamic processes requires constraints beyond free energy *Nat. Comms.* **6** 6383
- [20] Plenio M B and Virmani S 2007 An introduction to entanglement measures *Quant. Inf. Comput.* **7** 1–51
- [21] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865–942
- [22] Ollivier H and Zurek W H 2001 Quantum discord: a measure of the quantumness of correlations *Phys. Rev. Lett.* **88** 017901
- [23] Henderson L and Vedral V 2001 Classical, quantum and total correlations *Journal of Physics A: Mathematical and General* **34** 6899
- [24] Modi K, Brodutch A, Cable H, Paterek T and Vedral V 2012 The classical-quantum boundary for correlations: discord and related measures *Rev. Mod. Phys.* **84** 1655–707
- [25] Streltsov A 2015 Quantum correlations beyond entanglement *Quantum Correlations Beyond Entanglement: and Their Role in Quantum Information Theory* (Cham: Springer International Publishing) pp 17–22 doi:10.1007/978-3-319-09656-8_4
- [26] Knill E and Laflamme R 1998 Power of one bit of quantum information *Phys. Rev. Lett.* **81** 5672–5
- [27] Parker S and Plenio M B 2002 Entanglement simulations of shor’s algorithm *J. Mod. Opt.* **49** 1325–53
- [28] Datta A, Flammia S T and Caves C M 2005 Entanglement and the power of one qubit *Phys. Rev. A* **72** 042316
- [29] Datta A, Shaji A and Caves C M 2008 Quantum discord and the power of one qubit *Phys. Rev. Lett.* **100** 050502
- [30] Lanyon B P, Barbieri M, Almeida M P and White A G 2008 Experimental quantum computing without entanglement *Phys. Rev. Lett.* **101** 200501
- [31] Ali M 2014 Quantum dissonance and deterministic quantum computation with a single qubit *International Journal of Quantum Information* **12** 1450037
- [32] Yadin B, Ma J, Girolami D, Gu M and Vedral V 2015 Quantum processes which do not use coherence arXiv:1512.02085
- [33] Eisert J, Jacobs K, Papadopoulos P and Plenio M B 2000 Optimal local implementation of nonlocal quantum gates *Phys. Rev. A* **62** 052317
- [34] Vidal G 2000 Entanglement monotones *J. Mod. Opt.* **47** 355–76
- [35] Bennett C H, Bernstein H J, Popescu S and Schumacher B 1996 Concentrating partial entanglement by local operations *Phys. Rev. A* **53** 2046–52
- [36] Rains E M 1999 Bound on distillable entanglement *Phys. Rev. A* **60** 179–84
- [37] Hiroshima T and Hayashi M 2004 Finding a maximally correlated state: simultaneous Schmidt decomposition of bipartite pure states *Phys. Rev. A* **70** 030302
- [38] Zurek W H 2003 Quantum discord and Maxwell’s demons *Phys. Rev. A* **67** 012320
- [39] Horodecki M, Horodecki P, Horodecki R, Oppenheim J, Sen(De) A, Sen U and Synak-Radtke B 2005 Local versus nonlocal information in quantum-information theory: Formalism and phenomena *Phys. Rev. A* **71** 062307
- [40] Dakić B, Vedral V and Brukner i c v 2010 Necessary and sufficient condition for nonzero quantum discord *Phys. Rev. Lett.* **105** 190502
- [41] Peck R, Olsen C and Devore J L 2008 *Introduction to Statistics and Data Analysis* 3rd edn (Boston, MA: Cengage Learning)
- [42] Modi K, Paterek T, Son W, Vedral V and Williamson M 2010 Unified view of quantum and classical correlations *Phys. Rev. Lett.* **104** 080501
- [43] Streltsov A 2015 Genuine quantum coherence arXiv:1511.08346
- [44] Lindblad G 1974 Expectations and entropy inequalities for finite quantum systems *Commun. Math. Phys.* **39** 111–9
- [45] Hamieh S, Kobes R and Zaraket H 2004 Positive-operator-valued measure optimization of classical correlations *Phys. Rev. A* **70** 052325