

Resource engines

Hanna Wojewódka-Ściążko^{1,2}, Zbigniew Puchała², and Kamil Korzekwa³

¹Institute of Mathematics, University of Silesia in Katowice, Bankowa 14, 40-007 Katowice, Poland

²Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland

³Faculty of Physics, Astronomy and Applied Computer Science, Jagiellonian University, 30-348 Kraków, Poland

January 5, 2024

In this paper we aim to push the analogy between thermodynamics and quantum resource theories one step further. Previous inspirations were based predominantly on thermodynamic considerations concerning scenarios with a single heat bath, neglecting an important part of thermodynamics that studies heat engines operating between two baths at different temperatures. Here, we investigate the performance of resource engines, which replace the access to two heat baths at different temperatures with two arbitrary constraints on state transformations. The idea is to imitate the action of a two-stroke heat engine, where the system is sent to two agents (Alice and Bob) in turns, and they can transform it using their constrained sets of free operations. We raise and address several questions, including whether or not a resource engine can generate a full set of quantum operations or all possible state transformations, and how many strokes are needed for that. We also explain how the resource engine picture provides a natural way to fuse two or more resource theories, and we discuss in detail the fusion of two resource theories of thermodynamics with two different temperatures, and two resource theories of coherence with respect to two different bases.

1 Introduction

Thermodynamics occupies a distinguished place among physical theories: it permeates all other fields and finds applicability everywhere, from astrophysics [1] and biophysics [2] to condensed matter [3] and physics of computation [4]. The reason for this is that thermodynamics actually forms a meta-theory that employs statistical reasoning to tell us which state transformations are allowed, and which are probabilistically impossible. In other words, thermodynamics can be seen as a field studying the accessibility and inaccessibility of one physical state from another [5], abstracting away whether these states describe electromagnetic radiation, a gas of spin particles or electrons in an atom.

This perspective inspired the development of quantum resource theories [6], where one investigates allowed

transformations between quantum states under general, not necessarily thermodynamic, constraints. The best-known example is given by the theory of entanglement [7], where bipartite system transformations are constrained to local operations and classical communication, and one is interested in the possible manipulations of entangled states. Other widely studied examples include state transformations under operations that are incoherent [8], symmetric [9] or Clifford [10]. In all these theories, clear parallels with thermodynamic considerations have been made. Similarly as every thermodynamic transition can be made possible by investing enough work, universal resources in other theories (such as ebits [11], rebits [12] or coherent bits [13]) have also been identified and their optimal manipulations have been investigated. Also, the thermodynamic concept of catalysis was extended to general resource theories, where catalysts are given by ancillary systems that make otherwise forbidden transitions possible, while being unchanged in the process [14, 15]. Finally, probably the most important link between thermodynamics and other resource theories is through the second law of thermodynamics [16], where general resource monotones [17], such as entropy of entanglement [7] or relative entropy of coherence [8], play the role of monotonically decreasing thermodynamic free energy, and the questions concerning reversibility and irreversibility of a given resource theory are central to the field [18–21].

Given how fruitful the thermodynamic inspirations have been so far for quantum resource theories, in this paper we aim at pushing this analogy one step further. So far most of such inspirations have been based on thermodynamic considerations concerning scenarios with a single heat bath. Notable exception is given by the resource theory thermodynamics itself, where the efficiency and performance of quantum heat engines [22–24] and more general autonomous thermal machines [25, 26] working between two baths at different temperatures were studied from a resource-theoretic perspective. However, the approach to general resource theories neglects this very important part of thermodynamics with access to two heat baths. It is true that, from a purely resource-theoretic perspective, having access to two infinite baths at different temperatures in some sense trivialises the theory, as one can then perform infinite amount of work, and so every state transformation becomes possible (at least in the semi-classical regime of energy-incoherent states [27]).

Hanna Wojewódka-Ściążko: hanna.wojewodka@us.edu.pl

However, the physics of heat engines is far from being trivial, one just needs to ask different questions. Instead of looking for the amount of work that can be extracted from a given non-equilibrium state, one rather asks about the optimal efficiency of converting heat into work, or about the maximum power of a heat engine.

We thus propose to investigate the performance of *resource engines*, which generalise the concept of heat engines by replacing the access to two heat baths at different temperatures with two arbitrary constraints on state transformations. More precisely, we consider two agents (traditionally referred to as Alice and Bob), each of which is facing a different constraint, meaning that each of them can only prepare a subset of free states, F_A and F_B , and can only perform quantum operations from a subset of free operations, \mathcal{F}_A and \mathcal{F}_B . Now, the idea is to imitate the action of a two-stroke heat engine: instead of subsequently connecting the system to the hot and cold bath, it is sent to Alice and Bob in turns and they can perform any operation on it from their constrained sets \mathcal{F}_A and \mathcal{F}_B . Since the free states and operations of Alice will generally be resourceful with respect to Bob's constraints (and vice versa), a number of such communication rounds with local constrained operations (i.e., strokes of a resource engine) may generate quantum states outside of F_A and F_B . Thus, by fusing two resource theories described by (F_A, \mathcal{F}_A) and (F_B, \mathcal{F}_B) , one can obtain a new resource theory with free operations $\mathcal{F}_{AB} \supseteq \mathcal{F}_A \cup \mathcal{F}_B$ and free states $F_{AB} \supseteq F_A \cup F_B$.

A number of natural questions then arise. First, can a resource engine defined by given two constraints generate a full set of quantum operations, or at least approach every element of this set arbitrarily well with the number of strokes going to infinity? Alternatively, can it achieve all possible final states starting from states belonging to F_A or F_B ? If the answer to these questions is yes, then can we bound the number of strokes needed to generate every operation or state? And if there exists a state that is maximally resourceful with respect to both Alice's and Bob's constraints, what is the minimal number of strokes needed to create it? Note that given that each stroke takes a fixed amount of time, this effectively corresponds to studying the optimal power of a resource engine. One can also ask about the equivalent of engine's efficiency. Namely, whenever Bob gets a state from Alice and transforms it using an operation from \mathcal{F}_B , he necessarily decreases the resource content of the state with respect to his constraint, but may increase it with respect to Alice's constraint. Thus, one may investigate the optimal trade-off, i.e., the efficiency of transforming his resource into Alice's resource.

In this paper, we start with our resource-theoretic perspective on standard heat engines in Sec. 2, where Alice and Bob are constrained to having access to heat baths at different temperatures. More precisely, in Sec. 2.1, we recall the necessary notions of thermal operations and thermomajorisation, set the notation, and formally state the main problems of athermality engines we want to investigate. Next, in Sec. 2.2, we fully solve these problems for

an elementary example of a two-level system. Section 2.3 contains our main results for athermality engines with arbitrary d -dimensional systems, where we lower and upper bound the set of achievable states F_{AB} , as well as find its exact form in the limit of the hotter bath having infinite temperature. We then proceed to Sec. 3 that is devoted to the concept of unitary coherence engines, where Alice and Bob are constrained to only performing unitary operations diagonal in their fixed bases, so that coherence with respect to these bases is a resource for them. First, in Sec. 3.1, we set the scene by recalling the necessary formalism, fixing the notation and stating the problems. Next, as in the athermality case, we fully solve these problems for the simplest case of a two-level system in Sec. 3.2. In Sec. 3.3, we then derive and discuss the conditions under which the full set of unitary operations can be performed jointly by Alice and Bob, i.e., when \mathcal{F}_{AB} becomes the full set of unitary operations. We analyse the number of strokes N needed to get all these operations in Sec. 3.4, presenting both lower and upper bounds for N . Finally, in Sec. 3.5, we discuss the problem of using the resource engine to produce a state that is simultaneously maximally resourceful for both Alice and Bob. We end the paper in Sec. 4, where we discuss relations between resource engines and known problems within quantum information, and outline opportunities for future research.

2 Athermality engine

2.1 Setting the scene

In the resource-theoretic approach to thermodynamics [28], one assumes there is a single agent A that has access to a thermal heat bath at inverse temperature $\alpha = 1/(kT_A)$, with k denoting the Boltzmann constant, and is allowed to unitarily couple the system of interest to the bath in an energy-conserving way. More formally, given a quantum system in a state ρ and described by a Hamiltonian H , the set of operations \mathcal{F}_A that the agent can perform consists of *thermal operations* \mathcal{E} with respect to α defined by [28, 29]

$$\mathcal{E}(\rho) = \text{Tr}_E (U(\rho \otimes \gamma_E)U^\dagger), \quad (1)$$

where

$$\gamma_E = \frac{\exp(-\alpha H_E)}{\text{Tr}(\exp(-\alpha H_E))} \quad (2)$$

is a thermal Gibbs state of the environment described by an arbitrary Hamiltonian H_E , and U is a joint system-bath unitary preserving the total energy, i.e.,

$$[U, H \otimes \mathbb{1}_E + \mathbb{1} \otimes H_E] = 0. \quad (3)$$

The central question is then given by the following interconversion problem: which final states σ are achievable from a given initial state ρ via thermal operations? Note that the only free state that any state can be mapped to is the system's thermal Gibbs state γ (defined by Eq. (2) with H_E replaced by H), and all other states are treated

as resources. In other words, the free set F_A consists of a single element γ .

Here, we will focus on the quasi-classical version of the interconversion problem with initial and final states of the system commuting with γ . This case is usually referred to as incoherent thermodynamics, since one then focuses on interconversion between states that do not have quantum coherence between different energy eigensectors. Instead of representing quantum states as density matrices of size d , one can then use a simpler representation using d -dimensional probability distributions describing occupations of different energy levels. We will thus denote the initial, final and Gibbs states by probability vectors \mathbf{p} , \mathbf{q} and γ , respectively.

The main reason why we restrict to the incoherent setting is because then the necessary and sufficient conditions for the existence of a thermal operation mapping \mathbf{p} to \mathbf{q} are known to be fully characterised by a thermomajorisation condition $\mathbf{p} \succ_{\gamma} \mathbf{q}$ [28] (also known as d -majorisation [30]). For a full review of this subject, we refer the reader to Ref. [31], while in Appendix A we summarise the bits of the theory necessary for our purposes. Here, we only note that a thermomajorisation curve (also known as the Lorenz curve) of \mathbf{p} with respect to γ is a piece-wise linear and concave curve on a plane starting at the origin and consisting of segments with the horizontal x length given by γ_i and vertical y lengths given by p_i (note that concavity of the curve enforces a particular ordering of these segments). Then, we say that \mathbf{p} thermomajorises \mathbf{q} , $\mathbf{p} \succ_{\gamma} \mathbf{q}$, if and only if the thermomajorisation curve of \mathbf{p} lies above that of \mathbf{q} everywhere.

Now, our aim is to study a modified setting with two agents, A and B , that can exchange the processed system between each other, and with each of the agents being constrained to only performing thermal operation with respect to their (unequal) temperatures[†]. More precisely, we consider the set of free operations \mathcal{F}_A to be given by thermal operations with inverse temperature α and the corresponding free state given by γ with

$$\gamma_k = \frac{e^{-\alpha E_k}}{Z_{\alpha}}, \quad Z_{\alpha} = \sum_{i=1}^d e^{-\alpha E_i}, \quad (4)$$

where $\{E_i\}$ denotes the energy levels of the system; and the free set of operations \mathcal{F}_B to be given by thermal operations with inverse temperature $\beta < \alpha$ and the corresponding free state given by Γ with

$$\Gamma_k = \frac{e^{-\beta E_k}}{Z_{\beta}}, \quad Z_{\beta} = \sum_{i=1}^d e^{-\beta E_i}. \quad (5)$$

The main question that we will investigate is: what is the resulting set F_{AB} of achievable states if each of the agents is constrained to their own set of free states and

[†]Note the difference with a typical approach to autonomous thermal machines, where the system is constantly connected to two baths, but the interaction with them is constrained (fixed). Here, the system interacts only with one bath at a time, but its interaction is unconstrained (i.e., any thermal operation on the system can be performed).

operations (so that together they can generate any operation from the set \mathcal{F}_{AB})? In other words, we look for all states $\mathbf{p}^{(N-1)}$ (and their convex combinations via randomised strategies) that can be obtained via a sequence of thermomajorisations either from γ or Γ , i.e., that satisfy one of the following:

$$\gamma =: \mathbf{p}^{(0)} \succ_{\Gamma} \mathbf{p}^{(1)} \succ_{\gamma} \mathbf{p}^{(2)} \succ_{\Gamma} \mathbf{p}^{(3)} \succ_{\gamma} \dots \mathbf{p}^{(N-1)}, \quad (6a)$$

$$\Gamma =: \mathbf{p}^{(0)} \succ_{\gamma} \mathbf{p}^{(1)} \succ_{\Gamma} \mathbf{p}^{(2)} \succ_{\gamma} \mathbf{p}^{(3)} \succ_{\Gamma} \dots \mathbf{p}^{(N-1)}, \quad (6b)$$

for a given value of N (set of states $F_{AB}^{(N)}$ achievable after N strokes) or for $N \rightarrow \infty$ (set F_{AB} of all achievable states). Note that in the investigated setting we assume that the agents exchange the total system that is fixed, so that all ancillary systems (like a battery) need to be explicitly modelled and the system's Hilbert space does not change. More generally, once the free set F_{AB} resulting from fusing two resource theories is known, one can also investigate allowed resource transformations in this new theory. In other words, one can ask what final states can be achieved via \mathcal{F}_{AB} when the initial state is outside of F_{AB} .

2.2 Elementary qubit example

We start with the simplest case of a two-level system that will serve us as an example to illustrate problems at hand. The two thermal states are then simply given by

$$\Gamma = (\Gamma, 1 - \Gamma), \quad \gamma = (\gamma, 1 - \gamma), \quad (7)$$

with $\gamma \geq \Gamma$. In what follows, we will denote a thermal state by $\mathbf{g} = (g, 1 - g)$, without specifying whether $\mathbf{g} = \gamma$ or $\mathbf{g} = \Gamma$. The set of all states achievable from a given state \mathbf{p} via thermal operations (i.e., the set of states \mathbf{q} such that $\mathbf{p} \succ_{\mathbf{g}} \mathbf{q}$) is convex and its extremal points have been characterised in Ref. [32] by studying the thermomajorisation order (see Lemma 12 therein). For $d = 2$, there are just two extremal states achievable from \mathbf{p} : the state \mathbf{p} itself and

$$\mathbf{q} = \Pi_{\mathbf{g}} \mathbf{p}, \quad \Pi_{\mathbf{g}} = \begin{pmatrix} 1 - \frac{1-g}{g} & 1 \\ \frac{1-g}{g} & 0 \end{pmatrix}. \quad (8)$$

Importantly, applying two such non-trivial extremal transformations $\Pi_{\mathbf{g}}$ in a row with respect to the same \mathbf{g} does not produce an extremal point. It is thus clear that the extremal states achievable from \mathbf{p} by two agents after $N = 2m + k$ strokes will have one of the following two forms

$$\Pi_{\Gamma}^k (\Pi_{\gamma} \Pi_{\Gamma})^m \mathbf{p}, \quad \Pi_{\gamma}^k (\Pi_{\Gamma} \Pi_{\gamma})^m \mathbf{p}, \quad (9)$$

with $k \in \{0, 1\}$ and $m \in \mathbb{N}$. We then note that the fixed points of the composition of extremal maps are given by (see Fig. 1a):

$$(\Pi_{\gamma} \Pi_{\Gamma}) \tilde{\gamma} = \tilde{\gamma} = (\tilde{\gamma}, 1 - \tilde{\gamma}), \quad \tilde{\gamma} = \frac{(2\gamma - 1)\Gamma}{\Gamma + \gamma - 1}, \quad (10a)$$

$$(\Pi_{\Gamma} \Pi_{\gamma}) \tilde{\Gamma} = \tilde{\Gamma} = (\tilde{\Gamma}, 1 - \tilde{\Gamma}), \quad \tilde{\Gamma} = \frac{(2\Gamma - 1)\gamma}{\Gamma + \gamma - 1}. \quad (10b)$$

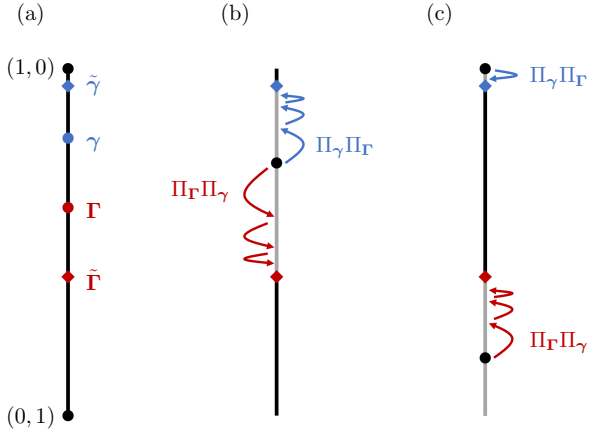


Figure 1: Two-level athermality engine. (a) The space of incoherent states of a two-level system is given by a one-dimensional simplex with extremal points $(1, 0)$ and $(0, 1)$, corresponding to the ground and excited states, respectively. Thermal states with respect to the cold and hot temperatures are indicated by γ and Γ , whereas fixed points of transformations $\Pi_\gamma \Pi_\Gamma$ and $\Pi_\Gamma \Pi_\gamma$ are denoted by $\tilde{\gamma}$ and $\tilde{\Gamma}$. Crucially, $\tilde{\gamma}$ ($\tilde{\Gamma}$) is always closer to the ground (excited) state than γ (Γ) is. (b) For initial states lying in the simplex between the fixed points $\tilde{\gamma}$ and $\tilde{\Gamma}$, the transformations $(\Pi_\gamma \Pi_\Gamma)^m$ and $(\Pi_\Gamma \Pi_\gamma)^m$ bring the initial state towards these fixed points “from the inside”. (c). For initial states lying in the simplex outside the segment connecting the fixed points $\tilde{\gamma}$ and $\tilde{\Gamma}$, the transformations $(\Pi_\gamma \Pi_\Gamma)^m$ and $(\Pi_\Gamma \Pi_\gamma)^m$ bring the initial state towards these fixed points “from the outside”.

Note that

$$\Pi_\Gamma \tilde{\gamma} = \tilde{\Gamma}, \quad \Pi_\gamma \tilde{\Gamma} = \tilde{\gamma}, \quad (11)$$

so that the fixed points can be mapped between each other by setting $k = 1$ in Eq. (9). Moreover, it is a straightforward calculation to show that as m grows, these fixed points are approached exponentially in m inside the probability simplex, always from the side of the initial point as illustrated in Figs. 1b-1c. More precisely, for every $\mathbf{p} = (p, 1 - p)$ and m we have

$$(\Pi_\gamma \Pi_\Gamma)^m \mathbf{p} = (q, 1 - q), \quad (\Pi_\Gamma \Pi_\gamma)^m \mathbf{p} = (r, 1 - r) \quad (12)$$

with

$$q = \left(\frac{(1 - \gamma)(1 - \Gamma)}{\gamma\Gamma} \right)^m (p - \tilde{\gamma}) + \tilde{\gamma}, \quad (13a)$$

$$r = \left(\frac{(1 - \gamma)(1 - \Gamma)}{\gamma\Gamma} \right)^m (p - \tilde{\Gamma}) + \tilde{\Gamma}, \quad (13b)$$

which allows one to completely characterise the set $F_{AB}^{(N)}$ of states achievable after N strokes.

Given all of the above, it is then clear that when the initial state \mathbf{p} belongs to

$$F_{AB} = \{ \mathbf{f} : \mathbf{f} = (1 - \lambda)\tilde{\gamma} + \lambda\tilde{\Gamma} \text{ with } 0 \leq \lambda \leq 1 \}, \quad (14)$$

then the set of achievable states after arbitrarily large number of strokes is given by F_{AB} . On the other hand, if $\mathbf{p} \notin F_{AB}$ then there are two cases. If \mathbf{p} is closer to $\tilde{\gamma}$

in total variation distance than it is to $\tilde{\Gamma}$, then the set of achievable states is given by

$$R_\Gamma(\mathbf{p}) = \{ \mathbf{r} : \mathbf{r} = (1 - \lambda)\mathbf{p} + \lambda\Pi_\Gamma \mathbf{p} \text{ with } 0 \leq \lambda \leq 1 \}, \quad (15)$$

Otherwise, it is given by

$$R_\gamma(\mathbf{p}) = \{ \mathbf{r} : \mathbf{r} = (1 - \lambda)\mathbf{p} + \lambda\Pi_\gamma \mathbf{p} \text{ with } 0 \leq \lambda \leq 1 \}. \quad (16)$$

Since both sets of original free states, $F_A = \{\gamma\}$ and $F_B = \{\Gamma\}$, are subsets of F_{AB} , we see that starting from either γ or Γ one can achieve any state belonging to F_{AB} . We thus conclude that F_{AB} can be interpreted as the free set of the new resource theory that arises from fusing two resource theories of quantum thermodynamics with different temperatures. Moreover, any state \mathbf{p} outside F_{AB} can be considered as a resource and its transformations are governed by Eqs. (15)-(16), which can be used to rigorously order states according to their resourcefulness. Finally, we want to emphasise that unless $\Gamma = 1/2$ (which corresponds to the hot bath being at infinite temperature), the set F_{AB} is not a full probability simplex. This means that fusing two thermodynamic resource theories results in a new non-trivial resource theory.

2.3 Bounding the set of achievable qudit states

Beyond the simple qubit case, the problem of fully characterising the set of achievable states F_{AB} quickly becomes intractable due to the scaling of the number of conditions one needs to verify. More precisely, during one stroke, a given initial state \mathbf{p} can be generally transformed to $d! - 1$ other extremal states [32]. Each of these states can then itself be an initial state of a system during the subsequent stroke, and so we see that, as the number N of strokes grows, the number of states one needs to consider explodes as $(d! - 1)^N$. Numerically, one can reduce the number of extremal states that need to be tracked by taking their convex hull after each stroke, and keeping only the extremal points thereof. This allows us to numerically consider large N for $d \in \{3, 4\}$, as we later discuss.

However, we would also like to get some analytic insight into the set of states F_{AB} achievable with the considered resource engine. Thus, in this section we first prove that there is an upper bound on F_{AB} , i.e., no matter how many strokes N we allow for, there exist states that cannot be produced by a resource engine. Then, we provide an analytically simple construction of the lower bound of F_{AB} , i.e., we characterise a polytope of states that forms a subset of F_{AB} . Finally, we prove that for one bath with finite temperature and the other in the limit of infinite temperature, $\alpha > 0$ and $\beta = 0$, the full set of states becomes achievable, i.e., F_{AB} is the whole probability simplex.

2.3.1 Upper bound

In this section we will generalise the qubit result, showing that the set of free states F_{AB} for a resource theory

arising from fusing two resource theories of thermodynamics with different temperatures is generally a proper subset of the probability simplex. To achieve this, we will prove the following slightly more general theorem that constrains the possible final populations of the highest excited state under transformations \mathcal{F}_{AB} .

Theorem 1. *Given an initial incoherent state \mathbf{p} and a set of operations \mathcal{F}_{AB} arising from fusing two resource theories of thermodynamics with different temperatures, all achievable final states \mathbf{q} satisfy*

$$q_d \leq M(\mathbf{p}) := \max\{p_d, \Gamma_d/\Gamma_{d-1}\}, \quad (17)$$

with $\mathbf{\Gamma}$ denoting the thermal state of the system with respect to the higher temperature. Thus, $M(\mathbf{p})$ is a monotone of the resulting resource theory.

Proof. We start by introducing the following notation. For a set of d -dimensional incoherent states X and a thermal state γ , we denote by $\mathcal{T}_\gamma(X)$ a convex hull of all states that can be obtained from the elements of X via thermal operations with a thermal state γ , i.e.,

$$\mathcal{T}_\gamma(X) := \text{conv}\{\{\mathbf{q} \mid \exists \mathbf{p} \in X : \mathbf{p} \succ_\gamma \mathbf{q}\}\}. \quad (18)$$

We will use analogous notation for the thermal state given by $\mathbf{\Gamma}$. Moreover, for any incoherent state \mathbf{p} , we denote by $\bar{\mathbf{p}}$ its version transformed in the following way:

$$\bar{\mathbf{p}} = (0, \dots, 0, 1 - p_d, p_d) \quad (19)$$

The crucial thing about this transformation is that

$$\mathbf{p} \succ_\gamma \mathbf{q} \Rightarrow \bar{\mathbf{p}} \succ_\gamma \mathbf{q} \quad \text{and} \quad \mathbf{p} \succ_{\mathbf{\Gamma}} \mathbf{q} \Rightarrow \bar{\mathbf{p}} \succ_{\mathbf{\Gamma}} \mathbf{q}, \quad (20)$$

which is a simple consequence of the thermomajorisation order (see Appendix B for details).

With the introduced notation, it is then clear that:

$$\begin{aligned} \mathcal{T}_\gamma(\mathcal{T}_{\mathbf{\Gamma}}(\mathbf{p})) &\subset \mathcal{T}_\gamma(\mathcal{T}_{\mathbf{\Gamma}}(\bar{\mathbf{p}})) = \mathcal{T}_\gamma(\{\mathbf{q} \mid \mathbf{q} \in \mathcal{T}_{\mathbf{\Gamma}}(\bar{\mathbf{p}})\}) \quad (21a) \\ &\subset \mathcal{T}_\gamma(\{\bar{\mathbf{q}} \mid \mathbf{q} \in \mathcal{T}_{\mathbf{\Gamma}}(\bar{\mathbf{p}})\}), \quad (21b) \end{aligned}$$

where, for brevity, single-element sets $\{\mathbf{p}\}$ and $\{\bar{\mathbf{p}}\}$ are denoted by \mathbf{p} and $\bar{\mathbf{p}}$, respectively. Using the definition of thermomajorisation, one can also show for $d \geq 3$ that (see Appendix B for details):

$$\max_{\mathbf{q}}\{q_d \mid \mathbf{q} \in \mathcal{T}_{\mathbf{g}}(\bar{\mathbf{r}})\} = \begin{cases} r_d & \text{for } r_d \geq \frac{g_d}{g_{d-1} + g_d}, \\ \frac{g_d(1-r_d)}{g_{d-1}} & \text{for } r_d \leq \frac{g_d}{g_{d-1} + g_d}, \end{cases} \quad (22a)$$

$$\min_{\mathbf{q}}\{q_d \mid \mathbf{q} \in \mathcal{T}_{\mathbf{g}}(\bar{\mathbf{r}})\} = 0, \quad (22b)$$

for \mathbf{g} given by either γ or $\mathbf{\Gamma}$.

Using Eqs. (21a)-(21b) and (22a)-(22b), we can now upper bound the final population q_d of the highest energy level after arbitrary one sequential interaction with two

baths:

$$\max_{\mathbf{q}}\{q_d \mid \mathbf{q} \in \mathcal{T}_\gamma(\mathcal{T}_{\mathbf{\Gamma}}(\mathbf{p}))\} \quad (23a)$$

$$\leq \max_{\mathbf{q}}\{q_d \mid \mathbf{q} \in \mathcal{T}_\gamma(\{\bar{\mathbf{r}} \mid \mathbf{r} \in \mathcal{T}_{\mathbf{\Gamma}}(\bar{\mathbf{p}})\})\} \quad (23b)$$

$$= \max_{\mathbf{q}} \max_{\mathbf{r} \in \mathcal{T}_{\mathbf{\Gamma}}(\bar{\mathbf{p}})}\{q_d \mid \mathbf{q} \in \mathcal{T}_\gamma(\bar{\mathbf{r}})\} \quad (23c)$$

$$= \max_{\mathbf{r} \in \mathcal{T}_{\mathbf{\Gamma}}(\bar{\mathbf{p}})} \max_{\mathbf{q}}\{q_d \mid \mathbf{q} \in \mathcal{T}_\gamma(\bar{\mathbf{r}})\} \quad (23d)$$

$$= \max_{\mathbf{r} \in \mathcal{T}_{\mathbf{\Gamma}}(\bar{\mathbf{p}})} \begin{cases} r_d & \text{for } r_d \geq \frac{\gamma_d}{\gamma_{d-1} + \gamma_d} \\ \frac{\gamma_d(1-r_d)}{\gamma_{d-1}} & \text{for } r_d \leq \frac{\gamma_d}{\gamma_{d-1} + \gamma_d} \end{cases} \quad (23e)$$

$$\leq \max \left\{ \max_{\mathbf{r} \in \mathcal{T}_{\mathbf{\Gamma}}(\bar{\mathbf{p}})} r_d, \frac{\gamma_d}{\gamma_{d-1}} \left(1 - \min_{\mathbf{r} \in \mathcal{T}_{\mathbf{\Gamma}}(\bar{\mathbf{p}})} r_d\right) \right\} \quad (23f)$$

$$\leq \max \left\{ p_d, (1 - p_d) \frac{\Gamma_d}{\Gamma_{d-1}}, \frac{\gamma_d}{\gamma_{d-1}} \right\} \quad (23g)$$

$$\leq \max \left\{ p_d, \frac{\Gamma_d}{\Gamma_{d-1}}, \frac{\gamma_d}{\gamma_{d-1}} \right\} = \max \left\{ p_d, \frac{\Gamma_d}{\Gamma_{d-1}} \right\}. \quad (23h)$$

Since after one sequential interaction the final population of the highest energy level is bounded by either the initial population of this level or by a constant, we conclude that the same bound holds after arbitrarily many repetitions (strokes). \square

Using the above theorem it is then straightforward to prove the following.

Corollary 2 (Upper bound on F_{AB}). *The set F_{AB} of free states arising from fusing two resource theories of thermodynamics with two different temperatures is bounded by*

$$\forall \mathbf{p} \in F_{AB} : \quad p_d \leq \frac{\Gamma_d}{\Gamma_{d-1}}, \quad (24)$$

where $\mathbf{\Gamma}$ denotes the thermal state corresponding to higher temperature.

As a final remark note that, as in the two-level case, when $\mathbf{\Gamma}$ corresponds to a thermal state in the infinite temperature limit, the above bound trivialises. As we will show later, in this limit all states belong to F_{AB} .

2.3.2 Lower bound

In this section we first present a simple analytical construction of a subset of the full set of achievable states F_{AB} for a resource theory arising from fusing two resource theories of thermodynamics with different temperatures. It is based on an iterative application of the modified qubit construction we saw in Sec. 2.2. We then also prove that, when the temperatures of the cold and hot bath satisfy certain conditions, F_{AB} contains non-full-rank states, i.e., the athermality engine can reduce the rank of the initial full-rank thermal state. In particular, we will show when this rank reduction can be maximal, by proving when the ground state belongs to F_{AB} .

We start by introducing a d -dimensional generalisations of the states $\tilde{\gamma}$ and $\tilde{\mathbf{\Gamma}}$ from Eqs. (10a)-(10b). We

define them by setting one component as follows,

$$\tilde{\gamma}_1 = \frac{\Gamma_1(\gamma_1 - \gamma_d)}{\Gamma_1(1 - \gamma_d) - \Gamma_d(1 - \gamma_1)}, \quad (25a)$$

$$\tilde{\Gamma}_d = \frac{\Gamma_d(\gamma_1 - \gamma_d)}{\Gamma_1(1 - \gamma_d) - \Gamma_d(1 - \gamma_1)}, \quad (25b)$$

and leaving the remaining components proportional to thermal distribution:

$$\tilde{\gamma}_k = \frac{1 - \tilde{\gamma}_1}{1 - \gamma_1} \gamma_k, \quad \tilde{\Gamma}_k = \frac{1 - \tilde{\Gamma}_d}{1 - \Gamma_d} \Gamma_k. \quad (26)$$

We then have the following simple lemma, the proof of which can be found in Appendix C.

Lemma 3. *For d -dimensional probability distributions \mathbf{p} and \mathbf{q} satisfying*

$$\Gamma_d \leq p_d \leq \tilde{\Gamma}_d, \quad \gamma_1 \leq q_1 \leq \tilde{\gamma}_1, \quad (27)$$

there exist $\mathbf{p}', \mathbf{p}'', \mathbf{q}', \mathbf{q}''$ such that

$$\mathbf{p} \succ_{\gamma} \mathbf{p}' \succ_{\Gamma} \mathbf{p}'', \quad \mathbf{q} \succ_{\Gamma} \mathbf{q}' \succ_{\gamma} \mathbf{q}'', \quad (28)$$

and

$$p_d'' = \frac{(1 - \gamma_1)\Gamma_d}{(1 - \gamma_d)\Gamma_1} p_d + \frac{(\gamma_1 - \gamma_d)\Gamma_d}{(1 - \gamma_d)\Gamma_1}, \quad (29a)$$

$$q_1'' = \frac{(1 - \gamma_1)\Gamma_d}{(1 - \gamma_d)\Gamma_1} q_1 + \frac{(\gamma_1 - \gamma_d)}{(1 - \gamma_d)}, \quad (29b)$$

so that $p_d \leq p_d'' \leq \tilde{\Gamma}_d$ and $q_1 \leq q_1'' \leq \tilde{\gamma}_1$.

We can now employ the above lemma to prove that the set of achievable states F_{AB} contains both $\tilde{\gamma}$ and $\tilde{\Gamma}$.

Proposition 4. *The set F_{AB} of free states arising from fusing two resource theories of thermodynamics with two different temperatures contains the states $\tilde{\gamma}$ and $\tilde{\Gamma}$. Moreover, the convergence to these states with the number of strokes N is exponential.*

Proof. We will only prove $\tilde{\Gamma} \in F_{AB}$, as the proof of $\tilde{\gamma} \in F_{AB}$ proceeds analogously. The proof is simply based on applying Lemma 3 iteratively m times. Starting with the hot thermal state Γ (preparation of which uses one stroke), we then apply the lemma m times, which uses $2m$ strokes (since each application uses one connection with the cold and one with the hot bath). By a simple application of the recurrence formula, after $N = 2m + 1$ strokes, one generates a state \mathbf{q} with

$$q_d = \left(\frac{(1 - \gamma_1)\Gamma_d}{(1 - \gamma_d)\Gamma_1} \right)^m (\Gamma_d - \tilde{\Gamma}_d) + \tilde{\Gamma}_d, \quad (30)$$

and the remaining components can be thermalised with the hot bath, so that for $k \neq d$:

$$q_k = \frac{1 - q_d}{1 - \Gamma_d} \Gamma_k. \quad (31)$$

Clearly, as $N \rightarrow \infty$, we get that $\mathbf{q} \rightarrow \tilde{\Gamma}$, with the convergence being exponential in m , so also with N . \square

Finally, we can use the above proposition iteratively to produce a whole polytope of states belonging to F_{AB} .

Proposition 5 (Lower bound on F_{AB}). *Within a simplex of d -dimensional probability distributions, consider a polytope P_d with 2^{d-1} extreme points $\{\mathbf{f}^{\mathbf{b}}\}$, each characterised by a bit string $\mathbf{b} = [b_2, \dots, b_d]$ of length $(d - 1)$ via the following:*

$$f_d^{\mathbf{b}} = g_d^{(b_d)}, \quad (32a)$$

$$f_k^{\mathbf{b}} = \left(1 - \sum_{l=k+1}^d f_l^{\mathbf{b}} \right) g_k^{(b_k)} \quad \text{for } k \in \{d-1, \dots, 2\}, \quad (32b)$$

$$f_1^{\mathbf{b}} = \left(1 - \sum_{l=2}^d f_l^{\mathbf{b}} \right), \quad (32c)$$

where

$$g_k^{(0)} := \frac{\gamma_k(\Gamma_1 - \Gamma_k)}{\Gamma_1(1 - \gamma_k) - \Gamma_k(1 - \gamma_1)}, \quad (33a)$$

$$g_k^{(1)} := \frac{\Gamma_k(\gamma_1 - \gamma_k)}{\Gamma_1(1 - \gamma_k) - \Gamma_k(1 - \gamma_1)}. \quad (33b)$$

Then, the set F_{AB} of free states arising from fusing two resource theories of thermodynamics with two different temperatures contains P_d .

Proof. Since the set F_{AB} is convex, we only need to show that F_{AB} contains $\mathbf{f}^{\mathbf{b}}$ for any choice of the bit string \mathbf{b} . Let us then fix \mathbf{b} and note that $g_d^{(0)} = \tilde{\gamma}_d$ and $g_d^{(1)} = \tilde{\Gamma}_d$. Thus, depending on b_d , we start by generating $\tilde{\Gamma}$ or $\tilde{\gamma}$ (by Proposition 4 we can do this, as both of these states belong to F_{AB}). As a result, the occupation of level d is given by $f_d^{\mathbf{b}}$. Next, set $k = 1$ and treat the first $(d - k)$ levels as an unnormalised $(d - k)$ -level state. Depending on b_{d-k} , again using Proposition 4 we generate versions of the states $\tilde{\Gamma}$ or $\tilde{\gamma}$ restricted to these $(d - k)$ levels (and unnormalised). Repeating this for $k \in \{2, \dots, d - 2\}$, we obtain the state with the occupation of the level k given by $f_k^{\mathbf{b}}$. Finally, the occupation of the ground state is given by $f_1^{\mathbf{b}}$ simply by the normalisation condition. \square

In Fig. 2, we present how this lower bound (and the upper bound from the previous section) compares with the full set of achievable states F_{AB} obtained numerically for two examples of three- and four-level athermality engines. As can be seen, in the first case, the numerically obtained F_{AB} contains only full rank states; whereas in the second case, up to numerical precision, F_{AB} seems to contain the rank-1 ground state. Since the pairs of cold and hot temperatures in the two studied examples were different, one may wonder whether the ability of the athermality engine to reduce rank depends on the temperature difference. In the next section we will see that, irrespective of the cold bath, when the hot bath is at infinite temperature, F_{AB} contains all states (so also the ones with the reduced rank). Here, we show that even if the temperature of the hot bath is not infinite, but it is large enough and the cold bath is cold enough, F_{AB} contains a rank-1 ground state (see Appendix D for the proof of the following proposition).

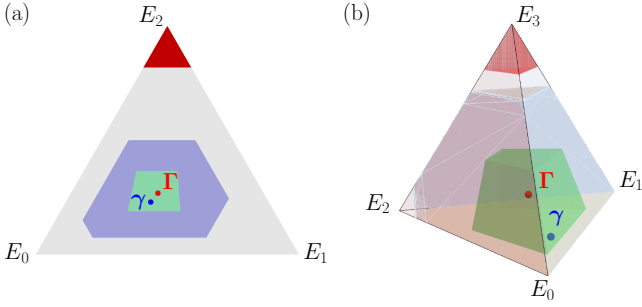


Figure 2: **Three- and four-level athermality engines.** The space of incoherent states of a d -level system is given by a $(d-1)$ -dimensional probability simplex [(a) $d = 3$ and (b) $d = 4$]. The set F_{AB} of states achievable by an athermality engine after $N \rightarrow \infty$ strokes is presented in blue (region obtained numerically for large enough N , so that increasing it does not lead to visible changes), the region excluded from F_{AB} by Corollary 2 is depicted in red, and the lower bound obtained in Proposition 5 is indicated in green. Parameters chosen: (a) $\alpha = 1/3$, $\beta = 1/5$, $E_k = k$; (b) $\alpha = 1$, $\beta = 1/4$, $E_k = k$.

Proposition 6. *Assume α to be large enough and β to be small enough, so that*

$$\gamma_1 > \frac{1}{2} \quad \text{and} \quad \Gamma_1 < \Gamma_d + \Gamma_{d-1}. \quad (34)$$

Then, the set F_{AB} of free states arising from fusing two resource theories of thermodynamics with two different temperatures contains the ground state. Achieving this state requires $N \rightarrow \infty$ strokes.

2.3.3 Full set of achievable states for $\beta = 0$

The upper bound constraining the set F_{AB} from Corollary 2 becomes trivial when $\beta = 0$, i.e., when the hot bath is at infinite temperature. One can then wonder, whether this bound is not tight, or rather in this special case there are no constraints and the set F_{AB} coincides with the full probability simplex. The following theorem shows that the latter is the case.

Theorem 7. *The set F_{AB} of free states arising from fusing two resource theories of thermodynamics, one with finite and the other with infinite temperature, is given by the full probability simplex. Moreover, the convergence to the full simplex with the number of strokes N is exponential.*

Proof. By Proposition 4, $\tilde{\gamma} \in F_{AB}$ and the convergence to this state is exponential in the number of strokes. However, in the limit of infinite temperature $\Gamma_k = 1/d$ for all $k \in \{1, \dots, d\}$, and so, by Eq. (25a),

$$\tilde{\gamma} = (1, 0, \dots, 0). \quad (35)$$

Finally, since

$$(1, 0, \dots, 0) \succ_{\Gamma} \mathbf{p} \quad (36)$$

for every \mathbf{p} , the set F_{AB} contains all probability distributions. \square

We thus see that the set F_{AB} of achievable states trivialises when the hot temperature is infinite ($\beta = 0$), even without cold temperature being zero. One can see this even without analysing the formal proof. Indeed, it suffices to observe the following. Firstly, in the case of $\beta = 0$, the state $\tilde{\gamma}$ given by Eq. (25a), is the ground state $(1, 0, 0, \dots, 0)$. Secondly, $\tilde{\gamma}$ belongs to F_{AB} due to Proposition 4. Thirdly, for $\beta = 0$ the set \mathcal{F}_B contains permutations, and so Bob can transform the ground state to the highest excited state. Finally, since this state, independently of α and β , thermomajorises all other states, one can transform it to any state within the probability simplex.

3 Coherence engine

3.1 Setting the scene

We now depart from athermality engines and switch to investigating engines fueled by the resource of quantum coherence. The theoretical framework established to quantify the amount of coherence present in a state of the system is known under the collective name of resource theories of coherence [8, 33]. Their aim is to quantitatively capture the departure from principles of classical physics due to the quantum superposition principle or, in other words, to quantify the ability of a system to undergo quantum interference effects. As with every resource theory, they are defined by identifying the set of free states and free operations. While all such theories agree on the form of the free states (they are simply given by states diagonal in the distinguished basis), there are plenty of choices for the set of free operations (see Ref. [34] for a review on this subject). To avoid making any specific choices (and also for simplicity), here we will restrict our considerations to a reversible subtheory, where all different resource theories of coherence coincide. Namely, we will only consider unitary transformations, and so the set of free operations will be given by unitaries diagonal in the distinguished basis². To make things even simpler, in our toy theory of coherence engines we will restrict ourselves to pure states. Thus, the only free states of the theory will be given by the distinguished basis states.

More formally, we consider two agents, A and B , that can prepare the following sets of free states

$$F_A = \{|i\rangle\}_{i=1}^d, \quad (37a)$$

$$F_B = \{U^\dagger |i\rangle\}_{i=1}^d, \quad (37b)$$

where $U \in \mathcal{U}_d(\mathbb{C})$ is a fixed unitary of order $d \geq 2$ over the field \mathbb{C} describing the relative orientation of the two bases. To define the sets of free operations, let

$$\mathcal{DU}_d(\mathbb{C}) = \left\{ \sum_{i=1}^d u_{ii} |i\rangle\langle i| : |u_{ii}| = 1 \right\} \quad (38)$$

²Note that, via the Stinespring dilation, this can serve as a starting point for analysing free operations given by more general quantum channels.

denote the subgroup of $\mathcal{U}_d(\mathbb{C})$ consisting of unitary matrices diagonal in the computational basis. Now, the sets of free operations are given by

$$\mathcal{F}_A = \mathcal{DU}_d(\mathbb{C}), \quad (39a)$$

$$\mathcal{F}_B = \{U^\dagger D U : D \in \mathcal{DU}_d(\mathbb{C})\}. \quad (39b)$$

Note that this setup is directly connected to the problem of Hamiltonian control [35]. More precisely, one can imagine having control over a quantum system with an intrinsic Hamiltonian H_1 , and being able to change it at will to H_2 by some external influence. By carefully choosing the timings and lengths of such interventions, one can then perform a sequence of unitaries $e^{iH_1 t_1}, e^{iH_2 t_2}, \dots$. Under the assumption of incommensurable spectra, this is then equivalent to a sequence of arbitrary unitaries diagonal in two different bases (of eigenstates of H_1 and H_2), which is the action of a coherence engine. To give a simple example, consider a spin-1/2 system, initially prepared in an up state along the \hat{z} axis, and two agents, A and B , who can turn on and off the magnetic field along the \hat{z} and \hat{n} axis, respectively. Such control of the magnetic field means that they can rotate the state of the system on the Bloch sphere around these axes. The aim is to have full control of the system's state, i.e., to have a protocol that maps the initial state to any state $|\psi\rangle$, optimally with as few steps as possible. The introduced coherence engine formalism allows to address exactly this problem and to answer whether such a full control is possible and, if so, what is the minimal number of steps needed.

The concept of coherence engines also bears resemblance to the problem of generating universal gate sets in quantum computing [36, 37]. However, there are crucial differences that distinguish the two concepts. Universal gate sets in quantum computing refer to finite sets of quantum gates that, when combined in various ways, can be used to approximate any unitary operation on a quantum computer. These gate sets are typically fixed and predetermined, e.g., all single-qubit gates along with a two-qubit entangling gate (like a CNOT gate). The ability to approximate any unitary operation using these gates is a fundamental requirement for the construction of a quantum computer. On the other hand, coherence engines, while sharing some similarities in terms of their ability to implement general unitary transformations, offer a more flexible and continuous approach. Specifically, two parties can implement any diagonal unitary in two different bases, thus enabling the realization of a continuous set of operations. In the case when the bases are appropriately chosen, the two parties can also approximate any unitary, just like in the case with a universal gate set. The continuous spectrum of operations may give more flexibility, but the number of uses/strokes strongly depends on the ‘‘angle’’ between Alice’s and Bob’s bases. Therefore, it is difficult to determine whether the universal gate set or a coherence engine will give a smaller number of usages to obtain a desired approximation of a general unitary.

Similarly as in the case of athermality engines, fus-

ing two resource theories described by (F_A, \mathcal{F}_A) and (F_B, \mathcal{F}_B) , by means of a coherence engine, leads to a new resource theory with free states $F_{AB} \supseteq F_A \cup F_B$ and free operations $\mathcal{F}_{AB} \supseteq \mathcal{F}_A \cup \mathcal{F}_B$. The main questions that we address here are as follows. First, in Sec. 3.3, we ask when $\mathcal{F}_{AB} = \mathcal{U}_d(\mathbb{C})$, i.e., under what conditions a coherence engine can generate any unitary operation. Next, in Sec. 3.4, we address this question quantitatively by asking about the number of strokes needed to achieve any operation from $\mathcal{U}_d(\mathbb{C})$. We then switch the attention from operations to states and investigate the task of reaching a given pure quantum state via a number of strokes of a resource engine. In particular, in Sec. 3.5, we analyse how quickly one can reach a state that is maximally resourceful (here: mutually coherent) with respect to both Alice’s and Bob’s constraints. However, before we present all of the above, we start with the simplest qubit example in Sec. 3.2 to illustrate problems at hand.

3.2 Elementary qubit example

For the qubit case, it will be convenient to use the Bloch sphere representation of a pure state $|\psi\rangle$:

$$|\psi\rangle\langle\psi| = \frac{\mathbb{1} + \hat{r} \cdot \boldsymbol{\sigma}}{2}, \quad (40)$$

where $\hat{r} = (r_x, r_y, r_z)$ is the Bloch vector satisfying $r_x^2 + r_y^2 + r_z^2 = 1$, and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is a vector of Pauli matrices. Let us also recall that an arbitrary single qubit unitary operator can be written in the form

$$R_{\hat{n}}(\theta) = e^{i\theta\hat{n} \cdot \boldsymbol{\sigma}}, \quad (41)$$

and its action on the Bloch vector \hat{r} is to rotate it by an angle θ around an axis specified by a three-dimensional unit vector \hat{n} .

Without loss of generality, we can then choose Alice’s distinguished basis to be given by the eigenstates of σ_z , and Bob’s to be given by the eigenstates of $\hat{n} \cdot \boldsymbol{\sigma}$ with $\hat{n} = (\sin(\alpha), 0, \cos(\alpha))$. Thus, the set F_A consists of states corresponding to the north and south pole of the Bloch sphere, whereas \mathcal{F}_A is given by rotations $R_{\hat{z}}(\theta)$ around the z axis by an arbitrary angle θ . Similarly, the set F_B consists of states from F_A rotated in the xz plane of the Bloch sphere by an angle α , whereas \mathcal{F}_B is given by rotations $R_{\hat{n}}(\theta)$ around the axis \hat{n} , i.e., around the axis tilted with respect to the z axis by an angle α (see Fig. 3).

Using the Euler angles decomposition, we see that a rotation around any axis \hat{m} by any angle θ can be written as

$$R_{\hat{m}}(\theta) = R_{\hat{z}}(\beta) R_{\hat{z}_\perp}(\gamma) R_{\hat{z}}(\delta), \quad (42)$$

where \hat{z}_\perp denotes a unit vector perpendicular to \hat{z} , and an appropriate choice of $\beta, \delta \in [0, 2\pi]$ and $\gamma \in [0, \pi]$ has to be made. Therefore, if $\hat{n} = \hat{z}_\perp$ (i.e., $\alpha = \pi/2$), Alice and Bob only need to perform three operations alternately (three strokes of a resource engine are needed) to generate arbitrary unitary operation. In other words, if

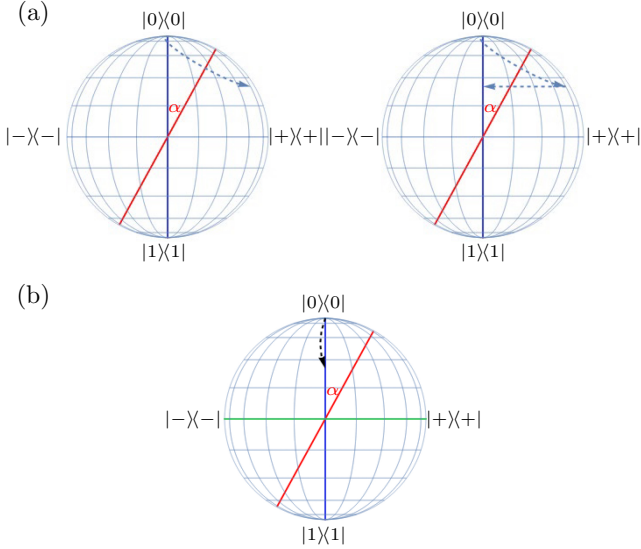


Figure 3: **Two-level coherence engine.** Rotating alternately in the σ_z and the $\hat{n} \cdot \sigma$ eigenbases (i.e., around the \hat{z} and \hat{n} axes, respectively) can generate a single rotation around arbitrary axis, in particular around \hat{y} . (a) Illustration of the right hand side of Eq. (44). (b) Illustration of the left hand side of Eq. (44).

the two distinguished bases are mutually unbiased (and so coherences with respect to them form complementary resources), then any unitary transformation can be generated with three strokes of a coherence engine.

Whenever $\hat{n} \neq \hat{z}_\perp$ (i.e., $\alpha < \pi/2$), the number of strokes increases to $\lceil \pi/\alpha \rceil + 1$. This fact, although studied in a different context, has been established, e.g., in Refs. [38, 39]; cf. also Ref. [40]. Indeed, the first and the last operation in Eq. (42) remain the same, but $R_{\hat{z}_\perp}(\gamma)$ has to be replaced by a product of alternated rotations around vectors \hat{z} and \hat{n} , respectively. In order to justify that it is possible, as well as to estimate the number of necessary alternated rotations, let us again refer to Eq. (42), and observe that for any $\tilde{\theta} \in \mathbb{R}$, there exist some $\tilde{\beta}, \tilde{\delta} \in [0, 2\pi]$ and $\tilde{\gamma} \in [0, \pi]$, depending on both $\tilde{\theta}$ and α , such that

$$R_{\hat{n}}(\tilde{\theta}) = R_{\hat{z}}(\tilde{\beta}) R_{\hat{z}_\perp}(\tilde{\gamma}) R_{\hat{z}}(\tilde{\delta}). \quad (43)$$

As a consequence, we get

$$R_{\hat{z}_\perp}(\tilde{\gamma}) = R_{\hat{z}}(-\tilde{\beta}) R_{\hat{n}}(\tilde{\theta}) R_{\hat{z}}(-\tilde{\delta}). \quad (44)$$

However, it is important to observe that Eq. (44) only holds for these values $\tilde{\gamma}$ which satisfy Eq. (43) with certain $\tilde{\beta}, \tilde{\delta}, \tilde{\theta}$. Intuitively, the smaller the angle α between the vectors \hat{z} and \hat{n} , the smaller the angle $\tilde{\gamma}$, by which we can rotate around the vector \hat{z}_\perp (see Fig. 3). To be more precise, $\tilde{\gamma}$ cannot be greater than 2α . This indicates that to generate $R_{\hat{z}_\perp}(\gamma)$ for an arbitrarily big γ , we need to perform k rotations around \hat{z}_\perp by angles not bigger than 2α in a row, namely

$$R_{\hat{z}_\perp}(\gamma) = R_{\hat{z}_\perp}(\gamma_1) \dots R_{\hat{z}_\perp}(\gamma_k). \quad (45)$$

This, in turn, implies that $k = \lceil \gamma/(2\alpha) \rceil$. Since we aim to estimate the number of necessary rotations to generate any unitary matrix, we have to consider the worst

case scenario, which is $k = \lceil \pi/(2\alpha) \rceil$. Note that, after applying Eq. (44) k times (with $\gamma_i, \beta_i, \theta_i, \delta_i$ in the places of $\tilde{\gamma}, \tilde{\beta}, \tilde{\theta}, \tilde{\delta}$, respectively), we end up with

$$R_{\hat{z}_\perp}(\gamma) = R_{\hat{z}}(-\beta_1) R_{\hat{n}}(\theta_1) R_{\hat{z}}(-\delta_1 - \beta_2) \dots \times R_{\hat{z}}(-\delta_{k-1} - \beta_k) R_{\hat{n}}(\theta_k) R_{\hat{z}}(-\delta_k), \quad (46)$$

which, due to Eq. (42), finally implies

$$R_{\hat{m}}(\theta) = R_{\hat{z}}(\beta - \beta_1) R_{\hat{n}}(\theta_1) R_{\hat{z}}(-\delta_1 - \beta_2) \dots \times R_{\hat{z}}(-\delta_{k-1} - \beta_k) R_{\hat{n}}(\theta_k) R_{\hat{z}}(-\delta_k + \delta). \quad (47)$$

Therefore, the total number of alternated operations from \mathcal{F}_A and \mathcal{F}_B needed to generate an arbitrary unitary operation is equal to $2k + 1 = 2\lceil \pi/(2\alpha) \rceil + 1 \geq \lceil \pi/\alpha \rceil + 1$. For details of this reasoning, see, e.g., Ref. [40]. An even more precise analysis, approaching the problem from the perspective of Lie algebras, is presented in Refs. [38] and [39], and the result obtained there is precisely $\lceil \pi/\alpha \rceil + 1$. We conclude that the incompatibility of the two bases measured by α quantifies the power of a coherence engine.

The analysis to estimate the number of strokes of a resource engine needed to reach any state when starting from a free state (to focus attention – an element of F_A) is very similar. The only crucial difference is that we can now choose to start from this pole of the Bloch sphere that is closer to the final state, and we do not need the initial rotation around \hat{z} (since states from F_A are anyway invariant under such transformations). As a consequence, it is enough to select γ in Eq. (42) from $[0, \pi/2]$ (instead of $[0, \pi]$), which requires $\lceil \pi/2\alpha \rceil$ strokes. This allows Alice and Bob to create a state with arbitrary polar angle, and the final rotation around \hat{z} allows for the choice of arbitrary azimuthal angle, thus getting to all states on the Bloch sphere. In conclusion, being restricted to the sets F_A, F_B of their free states and $\mathcal{F}_A, \mathcal{F}_B$ of their free operations, Alice and Bob can reach any pure quantum state with $\lceil \pi/2\alpha \rceil + 1$ strokes of a resource engine.

Instead of asking how many strokes it takes to get any state (or operation), we can also try to determine what is achievable with just three strokes, i.e., one round of communication between Alice and Bob. In particular, we will be interested in the conditions under which they can generate an optimal state (for both Alice and Bob) in this way. Of course, we first need to define what we mean by optimal in this case. It is natural to see the optimal state as the one that is maximally resourceful for both parties, and as such we can choose a maximally mutually coherent state with respect to Alice's and Bob's bases (see Appendix E or Refs. [41–43]). For two qubit bases given by eigenstates of $\hat{m} \cdot \sigma$ and $\hat{n} \cdot \sigma$, a maximally mutually coherent state is given by a state with a Bloch vector $\hat{r} \propto \hat{m} \times \hat{n}$, where \times denotes the cross product. Thus, in our case with $\hat{m} = \hat{z}$ and $\hat{n} = (\sin(\alpha), 0, \cos(\alpha))$, it is an eigenstate of σ_y , which corresponds to a state described by a Bloch vector with the polar angle $\pi/2$ and the azimuthal angle $\pi/2$. Now, note that the first stroke just prepares one of the two states from F_A , and the third

stroke is an operation from \mathcal{F}_A that cannot change the polar angle of a state. We thus see that in order to create the optimal state in three strokes, an operation from \mathcal{F}_B must transform the polar angle of the state from F_A (with polar angles 0 or π) to $\pi/2$. Since a rotation around an axis tilted by α with respect to the initial Bloch vector can at most create an angle 2α between the initial and final vectors, we see that this is possible if and only if $\alpha \in [\frac{\pi}{4}, \frac{3\pi}{4}]$. Therefore, as long as the largest absolute value of the overlap between the distinguished basis states is smaller or equal than $\cos(\pi/8)$, a coherence engine can produce a maximally mutually resourceful state in just three strokes. For a step-by-step analytical proof of the presented argument, see Appendix E.

3.3 Condition on getting all operations

For the elementary case of a qubit system, we have seen that, as long as the distinguished bases of Alice and Bob do not coincide, a coherence engine can generate an arbitrary unitary operation. For higher-dimensional systems, however, this is no longer the case. Thus, the aim of this section is to formulate conditions under which Alice and Bob, restricted to performing operations from \mathcal{F}_A and \mathcal{F}_B , respectively, are able to generate an arbitrary unitary. In other words, we ask under what conditions \mathcal{F}_{AB} becomes the full set of unitary operations.

For a given $U \in \mathcal{U}_d(\mathbb{C})$, let us introduce a matrix $P_U = (p_{ij})_{i,j=1}^d$ over the field \mathbb{R}_+ , which corresponds to U in the following sense:

$$p_{ij} = \begin{cases} 0 & \text{for } u_{ij} = 0, \\ 1 & \text{for } u_{ij} \neq 0. \end{cases} \quad (48)$$

Next, let us formulate the following two conditions on a matrix $U \in \mathcal{U}_d(\mathbb{C})$:

(H1) There exist a constant $M \in \mathbb{N}$ and matrices $D_1, \dots, D_{2M} \in \mathcal{DU}_d(\mathbb{C})$ such that

$$D_1 U^\dagger D_2 U D_3 U^\dagger D_4 U \dots D_{2M-1} U^\dagger D_{2M} U \quad (49)$$

is a matrix with all non-zero entries.

(H2) There exists a constant $M \in \mathbb{N}$ such that

$$(P_U^T P_U)^M \quad (50)$$

is a matrix with all non-zero entries.

Obviously, hypothesis (H2) is much easier to verify in practise than hypothesis (H1). However, in Appendix F, we prove the following.

Proposition 8. *Hypotheses (H1) and (H2) are equivalent.*

We will also need the following lemma, which follows from [44, Lemmas 2 and 3], and has been initially made in the proof of [45, Proposition 7].

Lemma 9. *A subgroup \mathcal{V} in $\mathcal{U}_d(\mathbb{C})$ containing $\mathcal{DU}_d(\mathbb{C})$ and a matrix $W = (w_{ij})_{i,j=1}^d$, such that $w_{ij} \neq 0$ for any $i, j \in \{1, \dots, d\}$, is a full unitary group.*

We can now state and prove the main result of this section.

Theorem 10. *If $U \in \mathcal{U}_d(\mathbb{C})$, appearing in the definition of \mathcal{F}_B , satisfies (H2), then any unitary matrix can be written as a product comprised of unitary matrices from \mathcal{F}_A and from \mathcal{F}_B .*

Proof. Let $M \in \mathbb{N}$ and $D_1, \dots, D_{2M} \in \mathcal{DU}_d(\mathbb{C})$ be such that (H2) holds. Then, using Proposition 8, the matrix

$$D_1 U^\dagger D_2 U D_3 U^\dagger D_4 U \dots D_{2M-1} U^\dagger D_{2M} U \quad (51)$$

has all non-zero entries. Note that this matrix is a product comprised of M matrices from \mathcal{F}_A and M matrices from \mathcal{F}_B . Next, using Lemma 9, we obtain that any unitary matrix can be written as a product of a number of matrices from Eq. (51) and a number of appropriately chosen diagonal unitary matrices. \square

Remark 11. According to [44, Lemmas 2 and 3], we do not even need to demand in Lemma 9 that \mathcal{V} contains a matrix with all non-zero entries. Instead we can only assume that \mathcal{V} contains a matrix $Q = (q_{ij})_{i,j=1}^d$ such that

$$\forall_{k,l \in \{1, \dots, d\}} \exists_{m \in \{1, \dots, d\}} q_{km} \neq 0 \text{ and } q_{lm} \neq 0. \quad (52)$$

This would, however, yield (due to [44, Lemmas 2 and 3]) that some matrix W with all non-zero entries also belongs to \mathcal{V} .

To see that there exist both unitary matrices for which condition (H2) is satisfied and unitary matrices for which it is violated, let us refer to the theory of finite Markov chains (see Appendix G for a brief review of the subject). For a chosen finite Markov chain, let T denote its transition matrix. It is well known that in the case of T being irreducible and aperiodic [46], e.g.,

$$T = 0.1 \begin{bmatrix} 5 & 2 & 2 & 1 & 0 & 0 \\ 2 & 5 & 2 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 2 & 4 \\ 2 & 2 & 1 & 1 & 1 & 3 \\ 0 & 0 & 3 & 4 & 1 & 2 \\ 0 & 0 & 1 & 2 & 6 & 1 \end{bmatrix}, \quad (53)$$

there exists a finite constant M such that for every $m \geq M$ the m -th step transition matrix T^m consists only of non-zero elements (cf. Proposition 25 in Appendix G).

Keeping this in mind, one can try to find a unitary matrix $U \in \mathcal{U}_d(\mathbb{C})$ such that $P_U^T P_U$ (with P_U induced by U via Eq. (48)) has the same pattern of zero and non-zero elements as some irreducible and aperiodic transition matrix T , e.g., in the case of T given by Eq. (53) one can think of

$$U = \frac{1}{2} \begin{bmatrix} 0 & 0 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 0 & 0 \\ -\sqrt{2} & \sqrt{2} & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{2} & -\sqrt{2} \\ 0 & 0 & 1 & -1 & 1 & 1 \end{bmatrix}. \quad (54)$$

We then immediately get that U enjoys (H2) (for U given by Eq. (54), condition (H2) holds with $M = 2$). Another example, illustrating how to find in practice the number M appearing in (H2) (and not only claim that such a number exists and is finite), is provided in Appendix G.

Proceeding now to “negative” examples, one shall take into account that both assumptions in Proposition 25 in Appendix G concerning finite Markov chains (i.e. irreducibility and aperiodicity of a transition matrix T) are essential. Hence, we may conclude the following:

1. Any unitary matrix U such that $P_U^T P_U$ is reducible violates condition (H2).
2. Any unitary matrix U such that $P_U^T P_U$ is periodic violates condition (H2). Note, however, that for $U \in \mathcal{U}_d(\mathbb{C})$ every diagonal element of $P_U^T P_U$ is positive, whence $P_U^T P_U$ cannot be periodic unless it is reducible – cf. Propositions 26 and 27 in Appendix G – and thus we end up in case 1.

Now, it suffices to observe that all matrices $U \in \mathcal{U}_d(\mathbb{C})$, which become block-diagonal after being multiplied by an appropriate permutation matrix (possibly also the identity matrix), violate condition (H2) (we conjecture that these are the only matrices violating condition (H2)). As precise examples we can either provide block-diagonal unitary matrices, such as

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}, \quad \begin{bmatrix} -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \quad (55)$$

or non-block-diagonal unitary matrices, such as

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}, \quad (56)$$

which can be transformed to block-diagonal matrices by multiplying them by appropriate permutation matrices.

3.4 Bounds on the number of strokes to get all operations

We start with a statement on the lower bound on the number of resource engine’s strokes needed to produce any unitary operation, the proof of which can be found in Appendix H.

Proposition 12. *Let $d \geq 3$ and suppose that the sets \mathcal{F}_A and \mathcal{F}_B are given by Eqs. (39a)-(39b) with an arbitrarily fixed matrix $U \in \mathcal{U}_d(\mathbb{C})$. The number N of resource engine’s strokes (i.e., the number $2M$ of alternated Alice’s and Bob’s operations) needed to generate an arbitrary operation $V \in \mathcal{U}_d(\mathbb{C})$ is bounded from below by*

$$N \geq \frac{2 \log(d-1)}{\log((d-2)c_U + 1)}, \quad (57)$$

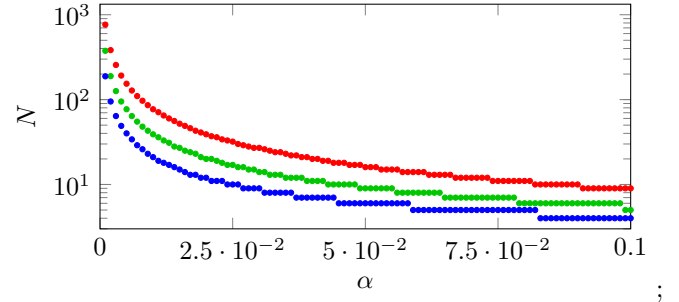


Figure 4: **Lower bound.** The lower bound from Proposition 12 for the number of coherence engine’s strokes needed to generate every unitary transformation, when the unitary U defining \mathcal{F}_B is given by F_d^α , with F_d denoting the d -dimensional Fourier matrix, and the three plots correspond to $d = 3$ (top red), $d = 5$ (middle green) and $d = 10$ (bottom blue).

where

$$\begin{aligned} c_U &:= \max_{a,b \in \{1, \dots, d\}: a \neq b} \sum_{j=1}^d |\bar{u}_{j,a}| |u_{j,b}| \\ &= \max_{a,b \in \{1, \dots, d\}: a \neq b} \langle a | (X_U^T X_U) | b \rangle \end{aligned} \quad (58)$$

and $[X_U]_{i,j} = |u_{i,j}|$ for all $i, j \in \{1, \dots, d\}$.

While the above lower bound is not tight (which can be seen by noting that for two mutually unbiased bases with $c_U = 1$, the bound states $N \geq 2$, and we know that already for $d = 2$ one needs 3 strokes), it nevertheless provides useful information when Alice’s and Bob’s bases do not differ much and so more strokes are required. This is illustrated in Fig. 4, where we plot this bound for a family of unitaries U defining \mathcal{F}_B continuously connecting the identity matrix with the Fourier matrix.

The upper bound on the number of strokes needed to produce any operation $V \in \mathcal{U}_d(\mathbb{C})$ (with an arbitrary positive even number d) will be implicitly expressed by means of the number N_F of strokes needed to generate the Fourier matrix.

Proposition 13. *Let $d \geq 4$ be an arbitrary even number and suppose that the sets \mathcal{F}_A and \mathcal{F}_B are given by Eqs. (39a)-(39b) with an arbitrarily fixed matrix $U \in \mathcal{U}_d(\mathbb{C})$. Moreover, let N_F denote the number of resource engine’s strokes needed to generate the Fourier matrix F_d of order d . Then, the number N of resource engine’s strokes needed to generate an arbitrary operation $V \in \mathcal{U}_d(\mathbb{C})$ is bounded from above by*

$$N \leq 6d(N_F + 1) + 1. \quad (59)$$

Proof. In Ref. [47], an analytical and deterministic procedure to design an implementation of an arbitrary unitary transformation is provided with the use of Fourier transforms and phase masks. According to the results established there, an arbitrary unitary of order d requires, in the case of d being an even number, $6d$ Fourier matrices and $6d+1$ diagonal unitary matrices (implemented by phase masks). The assertion of this proposition is then a straightforward consequence of this fact. \square

In the end let us indicate that, according to Ref. [45], every $U \in \mathcal{U}_d(\mathbb{C})$ (no matter whether d is even or odd) can be decomposed as a sequence of unitary circulant and unitary diagonal matrices. What is more, it can further be written as a product comprised of unitary diagonal matrices and the discrete Fourier transforms (since any circulant matrix can be written as a product of the Fourier matrix, some diagonal matrix, and the inverse of a Fourier matrix). However, to the best of our knowledge, there are no other results, apart from Ref. [47], to which we refer in the proof above, on the number of unitary diagonal matrices and Fourier matrices needed to generate a given unitary matrix. In Ref. [48], the authors prove that an arbitrary complex matrix can be written as a product of circulant and diagonal (but not necessarily unitary) matrices with the number of factors being $2d-1$ at most.

3.5 Condition on getting the optimal state

In this section, we focus on the problem of using a coherence engine to generate a maximally mutually coherent state $|\psi_*\rangle$ with respect to Alice's and Bob's distinguished bases. Such a state has the following form,

$$|\psi_*\rangle = \frac{1}{\sqrt{d}} (e^{i\alpha_1}|1\rangle + \dots + e^{i\alpha_d}|d\rangle) \quad (60a)$$

$$= \frac{1}{\sqrt{d}} (e^{i\beta_1}U^\dagger|1\rangle + \dots + e^{i\beta_d}U^\dagger|d\rangle), \quad (60b)$$

and we discuss their existence for arbitrary d -dimensional systems in Appendix E. In particular, we ask for which matrices U (which determine the set \mathcal{F}_B), the state $|\psi_*\rangle$ can be generated in only three strokes (i.e., Alice prepares a state from \mathcal{F}_A , sends it to Bob who transforms it via one of the unitaries belonging to \mathcal{F}_B , and finally sends it back to Alice, who performs a unitary from \mathcal{F}_A). A set of necessary conditions for this task is given by the following result.

Proposition 14. *Let $U = (u_{ij})_{i,j=1}^d \in \mathcal{U}_d(\mathbb{C})$. The following conditions are necessary for a coherence engine to produce a maximally mutually coherent state with just three strokes:*

$$\exists_l \forall_m \max_i |\bar{u}_{im}u_{il}| \leq \frac{1}{2} \left(\sum_{j=1}^d |\bar{u}_{jm}u_{jl}| + \frac{1}{\sqrt{d}} \right), \quad (61)$$

where $l, m, i \in \{1, \dots, d\}$. Equivalently,

$$\max_l \min_m \left(\sum_{j=1}^d \frac{|\bar{u}_{jm}u_{jl}|}{2} - \max_i |\bar{u}_{im}u_{il}| \right) \geq -\frac{1}{2\sqrt{d}}. \quad (62)$$

Detailed proof of the above proposition can be found in Appendix E and here we briefly explain the idea behind it. First, one notes that the task of generating a maximally mutually coherent state $|\psi_*\rangle$ (using just three strokes of a coherence engine) is possible if there exist $l \in \{1, \dots, d\}$ and $D \in \mathcal{DU}_d(\mathbb{C})$ such that for a given $U = (u_{ij})_{i,j=1}^d \in \mathcal{U}_d(\mathbb{C})$ the matrix $U^\dagger D U$ has

a flat l -th column (cf. Eqs. (117) and (118) in Appendix E). Note that this requirement can be rewritten as follows: there are $l \in \{1, \dots, d\}$, $\xi_1, \dots, \xi_d \in (0, 2\pi]$ and $\kappa_1, \dots, \kappa_d \in (0, 2\pi]$ such that

$$\forall_{m \in \{1, \dots, d\}} \sum_{j=1}^d e^{i\xi_j} \bar{u}_{jm} u_{jl} = e^{i\kappa_m} \frac{1}{\sqrt{d}}. \quad (63)$$

The generalised polygon inequalities then imply the assertion of Proposition 14.

The obvious consequence of Proposition 14 is the following corollary.

Corollary 15. *If $U = (u_{ij})_{i,j=1}^d \in \mathcal{U}_d(\mathbb{C})$, appearing in the definition of \mathcal{F}_B , is such that*

$$\min_i \max_j |u_{ij}|^2 > \sqrt{\frac{1 + \frac{1}{\sqrt{d}}}{2}}, \quad (64)$$

then one of the necessary conditions from Eq. (61) (namely the one with $m = l$) is violated, and thus Alice and Bob are not able to generate a maximally mutually coherent state with just three strokes of a coherence engine.

It is also interesting to observe that whenever a matrix $U \in \mathcal{U}_d(\mathbb{C})$ is, in a certain sense, too close to the some permutation matrix, then at least one of the necessary conditions given in Eq. (61) is violated. This is more formally captured by the following.

Proposition 16. *Let $U = (u_{ij})_{i,j=1}^d \in \mathcal{U}_d(\mathbb{C})$ be a matrix defining \mathcal{F}_B via Eq. (39b). If for some permutation matrix $\Pi \in \mathcal{U}_d(\mathbb{C})$ and some $D \in \mathcal{DU}_d(\mathbb{C})$, we have*

$$\|U - D\Pi\|_{HS}^2 < 2 - 2\sqrt{\frac{1 + \frac{1}{\sqrt{d}}}{2}}, \quad (65)$$

where $\|\cdot\|_{HS}$ denotes the Hilbert-Schmidt norm, then Alice and Bob are not be able to generate a maximally mutually coherent state with just two resource engine's strokes.

Proof. First of all, note that

$$\begin{aligned} \|U - D\Pi\|_{HS}^2 &= \text{Tr}((U - D\Pi)(U - D\Pi)^\dagger) \\ &= \text{Tr}(UU^\dagger + D\Pi(D\Pi)^\dagger - 2\text{Re}(U\Pi^\dagger D)) \\ &= 2d - 2\text{Re}\left(\sum_{k=1}^d \langle k|U\Pi^\dagger D|k\rangle\right) \\ &= 2d - 2\sum_{k=1}^d \text{Re}(u_{k\Pi^{-1}(k)}) e^{i\theta_k}, \end{aligned} \quad (66)$$

which, for appropriately chosen diagonal matrix D and appropriately chosen permutation matrix Π , is equal to

$$2d - 2\sum_{k=1}^d |u_{k\Pi^{-1}(k)}| = 2d - 2\sum_{k=1}^d \max_{j \in \{1, \dots, d\}} |u_{kj}|. \quad (67)$$

Assumption from Eq. (65) therefore implies

$$d - \sum_{k=1}^d \max_{j \in \{1, \dots, d\}} |u_{kj}| < 1 - \sqrt{\frac{1 + \frac{1}{\sqrt{d}}}{2}}, \quad (68)$$

whence

$$\sum_{k=1}^d \max_{j \in \{1, \dots, d\}} |u_{kj}| > (d-1) + \sqrt{\frac{1 + \frac{1}{\sqrt{d}}}{2}}. \quad (69)$$

Now, it suffices to observe the following general fact: for any $|x_1|, \dots, |x_d| \in [0, 1]$ such that

$$\sum_{i=1}^d |x_i| > (d-1) + \delta \quad \text{for some } \delta > 0, \quad (70)$$

we have

$$|x_i| > \delta \quad \text{for all } i \in \{1, \dots, d\}. \quad (71)$$

Indeed, let $|x_1|, \dots, |x_d| \in [0, 1]$ be such that they satisfy Eq. (70), and suppose (contrary to the above claim) that there exists $i_0 \in \{1, \dots, d\}$ such that $|x_{i_0}| \leq \delta$. Then

$$\sum_{i=1}^d |x_i| \leq \delta + \sum_{i \in \{1, \dots, d\} \setminus \{i_0\}} |x_i| \leq (d-1) + \delta, \quad (72)$$

which contradicts the undertaken assumption in Eq. (70).

Applying the above to $\{|u_{kj}|\}_{j=1}^d$, which enjoys Eq. (70) with $\delta = \sqrt{(1 + 1/\sqrt{d})/2}$, we obtain, due to Eq. (71), the following:

$$\max_{j \in \{1, \dots, d\}} |u_{kj}| > \sqrt{\frac{1 + \frac{1}{\sqrt{d}}}{2}} \quad \text{for any } k \in \{1, \dots, d\}. \quad (73)$$

Equivalently,

$$\min_{k \in \{1, \dots, d\}} \max_{j \in \{1, \dots, d\}} |u_{kj}| > \sqrt{\frac{1 + \frac{1}{\sqrt{d}}}{2}}. \quad (74)$$

According to Corollary 15, we therefore obtain the assertion of this proposition. \square

4 Outlook

In this work we have introduced the notion of a resource engine and used it to analyse the possibility and complexity of generating quantum states and channels from two different sets of free states and operations. The main motivation behind introducing and investigating the resource engine was due to the fact that it provides a natural way of fusing two (or more) resource theories, in the spirit of recent works on multi-resource theories [49]. In a sense, it allows one to study how compatible various constraints on allowed transformations are. What we have done here is just to start this kind of research by

introducing ideas and analysing simple toy examples, but we hope that a formal mathematical framework allowing for fusing arbitrary resource theories can be developed. Two potential ways to achieve this could be to extend to multiple resources the framework of general convex resource theories [50], or the very recent framework for quantifying resource-dependent complexity of quantum channels [51].

We also want to point out that the resource engine perspective may provide a unified framework to study seemingly unrelated problems within the field of quantum information. First, as explained in Sec. 3.1, our toy example, given by a setting with two agents being constrained to performing unitaries diagonal in two different bases, can be directly related to the problem of compiling universal quantum circuits via Hamiltonian control [35–37]. Thus, the results on resource engines could be applied to optimise quantum control and circuit compilation. Moreover, as discussed in the paper, a similar connection can be made with the problem of performing arbitrary optical linear transformations [47, 52] (e.g., Alice can be restricted to performing only phase masks, while Bob can only perform Fourier transforms or beam splitters).

Another potential use of resource engines is in the area of quantum error correction. Here, transversal gates are crucial for fault-tolerant quantum computation because of their robustness to noise, as well as their simplicity. The problem is that no quantum error correcting code can transversely implement a universal gate set [53]. However, by combining two error correcting codes with complementary transversal gate sets (so that together they are universal) via a method known as code switching [54, 55], one can achieve fault-tolerance. Therefore, studies of resource engines with two restricted sets corresponding to two transversal gate sets, can allow for optimising fault-tolerant quantum computation based on code switching.

Finally, one can also find applications for resource engines in analysing the generation and distribution of entanglement in quantum networks [56–58]. Such a network is represented by a graph with vertices corresponding to communicating parties and edges denoting connections between parties via quantum channels. Thus, generating a specific multipartite entangled state in a network can be decomposed into steps, where at each step two parties connected via a channel can process their part of the state. The simplest scenario of a linear network with three nodes (so A connected with B and B connected with C), can then be investigated using our resource engine with two constraints given by local operations on AB and local operations on BC . Extending the resource engine to more constraints (equivalent of a heat engine having access to baths at various temperatures) would allow onto deal with more complex quantum networks and could help in analysing optimal protocols for generating particular entangled states (e.g., minimising the number of communication rounds).

Acknowledgements

HW-S and ZP acknowledge financial support from SONATA BIS programme of National Science Centre Poland (grant no. 2016/22/E/ST6/00062), while KK was supported by the Foundation for Polish Science through TEAM-NET project (contract no. POIR.04.04.00-00-17C1/18-00).

References

- [1] Paul CW Davies. “Thermodynamics of black holes”. *Rep. Prog. Phys.* **41**, 1313 (1978).
- [2] Daniel M Zuckerman. “Statistical physics of biomolecules: An introduction”. *CRC Press*. (2010).
- [3] Evgenii Mikhailovich Lifshitz and Lev Petrovich Pitaevskii. “Statistical physics: Theory of the condensed state”. *Volume 9*. Elsevier. (1980).
- [4] Charles H Bennett. “The thermodynamics of computation—a review”. *Int. J. Theor. Phys.* **21**, 905–940 (1982).
- [5] Robin Giles. “Mathematical foundations of thermodynamics”. *Pergamon Press*. (1964).
- [6] Eric Chitambar and Gilad Gour. “Quantum resource theories”. *Rev. Mod. Phys.* **91**, 025001 (2019).
- [7] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. “Quantum entanglement”. *Rev. Mod. Phys.* **81**, 865–942 (2009).
- [8] T. Baumgratz, M. Cramer, and M. B. Plenio. “Quantifying coherence”. *Phys. Rev. Lett.* **113**, 140401 (2014).
- [9] I. Marvian. “Symmetry, asymmetry and quantum information”. PhD thesis. University of Waterloo. (2012). url: <https://uwspace.uwaterloo.ca/handle/10012/7088>.
- [10] Victor Veitch, SA Hamed Mousavian, Daniel Gottesman, and Joseph Emerson. “The resource theory of stabilizer quantum computation”. *New J. Phys.* **16**, 013009 (2014).
- [11] Charles H Bennett, Herbert J Bernstein, Sandu Popescu, and Benjamin Schumacher. “Concentrating partial entanglement by local operations”. *Phys. Rev. A* **53**, 2046 (1996).
- [12] SJ van Enk. “Quantifying the resource of sharing a reference frame”. *Phys. Rev. A* **71**, 032339 (2005).
- [13] Eric Chitambar and Min-Hsiu Hsieh. “Relating the resource theories of entanglement and quantum coherence”. *Phys. Rev. Lett.* **117**, 020402 (2016).
- [14] Daniel Jonathan and Martin B Plenio. “Entanglement-assisted local manipulation of pure quantum states”. *Phys. Rev. Lett.* **83**, 3566 (1999).
- [15] Kaifeng Bu, Uttam Singh, and Junde Wu. “Catalytic coherence transformations”. *Phys. Rev. A* **93**, 042326 (2016).
- [16] Michał Horodecki, Jonathan Oppenheim, and Ryszard Horodecki. “Are the laws of entanglement theory thermodynamical?”. *Phys. Rev. Lett.* **89**, 240403 (2002).
- [17] Tomáš Gonda and Robert W Spekkens. “Monotones in general resource theories”. *Compositionality* **5** (2023).
- [18] Fernando GSL Brandao and Martin B Plenio. “Entanglement theory and the second law of thermodynamics”. *Nat. Phys.* **4**, 873–877 (2008).
- [19] Wataru Kumagai and Masahito Hayashi. “Entanglement concentration is irreversible”. *Phys. Rev. Lett.* **111**, 130407 (2013).
- [20] Kamil Korzekwa, Christopher T Chubb, and Marco Tomamichel. “Avoiding irreversibility: Engineering resonant conversions of quantum resources”. *Phys. Rev. Lett.* **122**, 110403 (2019).
- [21] Ludovico Lami and Bartosz Regula. “No second law of entanglement manipulation after all”. *Nat. Phys.* **19**, 184–189 (2023).
- [22] Nelly Huei Ying Ng, Mischa Prebin Woods, and Stephanie Wehner. “Surpassing the Carnot efficiency by extracting imperfect work”. *New J. Phys.* **19**, 113005 (2017).
- [23] Hiroyasu Tajima and Masahito Hayashi. “Finite-size effect on optimal efficiency of heat engines”. *Phys. Rev. E* **96**, 012128 (2017).
- [24] Mohit Lal Bera, Maciej Lewenstein, and Manabendra Nath Bera. “Attaining Carnot efficiency with quantum and nanoscale heat engines”. *Npj Quantum Inf.* **7** (2021).
- [25] Friedemann Tonner and Günter Mahler. “Autonomous quantum thermodynamic machines”. *Phys. Rev. E* **72**, 066118 (2005).
- [26] Mark T Mitchison. “Quantum thermal absorption machines: Refrigerators, engines and clocks”. *Contemp. Phys.* **60**, 164–187 (2019).
- [27] M. Lostaglio, D. Jennings, and T. Rudolph. “Description of quantum coherence in thermodynamic processes requires constraints beyond free energy”. *Nat. Commun.* **6**, 6383 (2015).
- [28] M. Horodecki and J. Oppenheim. “Fundamental limitations for quantum and nanoscale thermodynamics”. *Nat. Commun.* **4**, 2059 (2013).
- [29] D. Janzing, P. Wocjan, R. Zeier, R. Geiss, and Th. Beth. “Thermodynamic cost of reliability and low temperatures: tightening Landauer’s principle and the second law”. *Int. J. Theor. Phys.* **39**, 2717–2753 (2000).
- [30] E. Ruch, R. Schraner, and T.H. Seligman. “Generalization of a theorem by Hardy, Littlewood, and Pólya”. *J. Math. Anal. Appl.* **76**, 222–229 (1980).
- [31] Matteo Lostaglio, David Jennings, and Terry Rudolph. “Thermodynamic resource theories, non-commutativity and maximum entropy principles”. *New J. Phys.* **19**, 043008 (2017).
- [32] Matteo Lostaglio, Álvaro M Alhambra, and Christopher Perry. “Elementary thermal operations”. *Quantum* **2**, 52 (2018).
- [33] J. Åberg. “Quantifying superposition” (2006). [arXiv:quant-ph/0612146](https://arxiv.org/abs/quant-ph/0612146).
- [34] Alexander Streltsov, Gerardo Adesso, and Martin B

- Plenio. “Colloquium: Quantum coherence as a resource”. *Rev. Mod. Phys.* **89**, 041003 (2017).
- [35] Viswanath Ramakrishna, Kathryn L. Flores, Herschel Rabitz, and Raimund J. Ober. “Quantum control by decompositions of $SU(2)$ ”. *Phys. Rev. A* **62**, 053409 (2000).
- [36] Seth Lloyd. “Almost any quantum logic gate is universal”. *Phys. Rev. Lett.* **75**, 346 (1995).
- [37] Nik Weaver. “On the universality of almost every quantum logic gate”. *J. Math. Phys.* **41**, 240–243 (2000).
- [38] F. Lowenthal. “Uniform finite generation of the rotation group”. *Rocky Mt. J. Math.* **1**, 575–586 (1971).
- [39] F. Lowenthal. “Uniform finite generation of $SU(2)$ and $SL(2, \mathbb{R})$ ”. *Canad. J. Math.* **24**, 713–727 (1972).
- [40] M. Hamada. “The minimum number of rotations about two axes for constructing an arbitrarily fixed rotation”. *R. Soc. Open Sci.* **1** (2014).
- [41] K. Korzekwa, D. Jennings, and T. Rudolph. “Operational constraints on state-dependent formulations of quantum error-disturbance trade-off relations”. *Phys. Rev. A* **89**, 052108 (2014).
- [42] Martin Idel and Michael M. Wolf. “Sinkhorn normal form for unitary matrices”. *Linear Algebra Appl.* **471**, 76–84 (2015).
- [43] Z. Puchała, Ł. Rudnicki, K. Chabuda, M. Paraniak, and K. Życzkowski. “Certainty relations, mutual entanglement, and nondisplaceable manifolds”. *Phys. Rev. A* **92**, 032109 (2015).
- [44] Z.I. Borevich and S.L. Krupetskij. “Subgroups of the unitary group that contain the group of diagonal matrices”. *J. Sov. Math.* **17**, 1718–1730 (1981).
- [45] M. Schmid, R. Steinwandt, J. Müller-Quade, M. Rötteler, and T. Beth. “Decomposing a matrix into circulant and diagonal factors”. *Linear Algebra Appl.* **306**, 131–143 (2000).
- [46] O. Häggström. “Finite Markov chains and algorithmic applications”. *London Mathematical Society Student Texts*. Cambridge University Press. (2002).
- [47] Víctor López Pastor, Jeff Lundeen, and Florian Marquardt. “Arbitrary optical wave evolution with Fourier transforms and phase masks”. *Opt. Express* **29**, 38441–38450 (2021).
- [48] Marko Huhtanen and Allan Perämäki. “Factoring matrices into the product of circulant and diagonal matrices”. *J. Fourier Anal. Appl.* **21**, 1018–1033 (2015).
- [49] Carlo Sparaciari, Lídia Del Rio, Carlo Maria Scandolo, Philippe Faist, and Jonathan Oppenheim. “The first law of general quantum resource theories”. *Quantum* **4**, 259 (2020).
- [50] Ryuji Takagi and Bartosz Regula. “General resource theories in quantum mechanics and beyond: Operational characterization via discrimination tasks”. *Phys. Rev. X* **9**, 031053 (2019).
- [51] Roy Araiza, Yidong Chen, Marius Junge, and Peixue Wu. “Resource-dependent complexity of quantum channels” (2023). [arXiv:2303.11304](https://arxiv.org/abs/2303.11304).
- [52] Luciano Pereira, Alejandro Rojas, Gustavo Cañas, Gustavo Lima, Aldo Delgado, and Adán Cabello. “Minimum optical depth multi-port interferometers for approximating any unitary transformation and any pure state” (2020). [arXiv:2002.01371](https://arxiv.org/abs/2002.01371).
- [53] Bryan Eastin and Emanuel Knill. “Restrictions on transversal encoded quantum gate sets”. *Phys. Rev. Lett.* **102**, 110502 (2009).
- [54] Jonas T Anderson, Guillaume Duclos-Cianci, and David Poulin. “Fault-tolerant conversion between the Steane and Reed-Muller quantum codes”. *Phys. Rev. Lett.* **113**, 080501 (2014).
- [55] Tomas Jochym-O’Connor and Raymond Laflamme. “Using concatenated quantum codes for universal fault-tolerant quantum gates”. *Phys. Rev. Lett.* **112**, 010505 (2014).
- [56] Antonio Acín, J Ignacio Cirac, and Maciej Lewenstein. “Entanglement percolation in quantum networks”. *Nat. Phys.* **3**, 256–259 (2007).
- [57] H Jeff Kimble. “The quantum internet”. *Nature* **453**, 1023–1030 (2008).
- [58] Sébastien Perseguers, GJ Lapeyre, D Cavalcanti, M Lewenstein, and A Acín. “Distribution of entanglement in large-scale quantum networks”. *Rep. Prog. Phys.* **76**, 096001 (2013).
- [59] C.-H. Cho. “Holomorphic discs, spin structures, and Floer cohomology of the Clifford torus”. *Int. Math. Res. Notices* **2004**, 1803–1843 (2004).
- [60] S.A. Marcon. “Markov chains: A graph theoretical approach”. Master’s thesis. University of Johannesburg. (2012). url: <https://ujcontent.uj.ac.za/explore/outputs/999849107691>.

A Thermomajorisation

Consider a d -dimensional quantum system described by a Hamiltonian H with eigenvalues $E_1 \leq \dots \leq E_d$. Denote a fixed inverse temperature of the environment by β . Then, the thermal Gibbs distribution of the system is given by

$$\gamma = \frac{1}{Z} (e^{-\beta E_1}, \dots, e^{-\beta E_d}), \quad Z = \sum_{i=1}^d e^{-\beta E_i}. \quad (75)$$

In order to construct a thermomajorisation curve of a probability vector \mathbf{p} (which describes the occupations of different energy levels in a given energy-incoherent state), one first needs to reorder the entries of \mathbf{p} according to the so-called β -order. To do so, denote by $\boldsymbol{\pi}(\mathbf{p})$ the reordering of $\{1, \dots, d\}$ that sorts p_i/γ_i in a non-increasing order,

$$\frac{p_{\pi_i(\mathbf{p})}}{\gamma_{\pi_i(\mathbf{p})}} \geq \frac{p_{\pi_{i+1}(\mathbf{p})}}{\gamma_{\pi_{i+1}(\mathbf{p})}}. \quad (76)$$

The β -ordered version of \mathbf{p} is then given by \mathbf{p}^β with $p_i^\beta = p_{\pi_i(\mathbf{p})}$. Next, the thermomajorisation curve of \mathbf{p} relative to γ is given by a piecewise linear concave curve on a plane that connects the points $\mathbf{l}^{(j)}$ given by

$$\mathbf{l}^{(j)} = \left(\sum_{i=1}^j \gamma_{\pi_i(\mathbf{p})}, \sum_{i=1}^j p_{\pi_i(\mathbf{p})} \right) \quad (77)$$

for $j \in \{0, \dots, d\}$, where $\mathbf{l}^{(0)} := (0, 0)$. Finally, \mathbf{p} is said to thermomajorise \mathbf{q} (relative to γ), denoted $\mathbf{p} \succ_\gamma \mathbf{q}$, when the thermomajorisation curve of \mathbf{p} is never below that of \mathbf{q} .

B Missing details in the proof of Theorem 1

We first need to show that Eq. (20) holds, i.e.,

$$\mathbf{p} \succ_\gamma \mathbf{q} \Rightarrow \bar{\mathbf{p}} \succ_\gamma \mathbf{q} \quad \text{and} \quad \mathbf{p} \succ_\Gamma \mathbf{q} \Rightarrow \bar{\mathbf{p}} \succ_\Gamma \mathbf{q}. \quad (78)$$

Without loss of generality, we can just prove the first of the above keeping γ general. The way to prove it is to show that $\bar{\mathbf{p}} \succ_\gamma \mathbf{p}$ which, due to transitivity of thermomajorisation order, leads to $\bar{\mathbf{p}} \succ_\gamma \mathbf{q}$. For $d = 2$ this is trivial, since $\bar{\mathbf{p}} = \mathbf{p}$. For $d \geq 3$, first consider two energy levels $E_i \leq E_j$, and a state \mathbf{r} with $r_i = 0$ and $r_j > 0$. Then, there exists a Gibbs-preserving operation that, on the two-dimensional subspace spanned by energy levels E_i and E_j , achieves an arbitrary occupation $(a, r_j - a)$ for $a \in [0, r_j]$. It is explicitly given by a matrix

$$T = \begin{bmatrix} 1 - \frac{\gamma_j a}{\gamma_i r_j} & \frac{a}{r_j} \\ \frac{\gamma_j a}{\gamma_i r_j} & 1 - \frac{a}{r_j} \end{bmatrix} \oplus \mathbb{1}_{\setminus(i,j)}, \quad (79)$$

where $\mathbb{1}_{\setminus(i,j)}$ denotes the $(d-2) \times (d-2)$ identity matrix on the subspace of all energy levels except E_i and E_j . In other words, it is always possible to move probability down the energy ladder to unoccupied levels. Since the first $(d-2)$ levels of $\bar{\mathbf{p}}$ are unoccupied, a sequence of such operations can move the occupations from \bar{p}_{d-1} down to all the energy levels, leading to a final distribution \mathbf{p} .

Next, we proceed to demonstrating that Eqs. (22a)-(22b) hold, i.e., that for $d \geq 3$ we have

$$\max_{\mathbf{q}} \{q_d | \mathbf{q} \in \mathcal{T}_{\mathbf{g}}(\bar{\mathbf{r}})\} = \begin{cases} r_d & \text{for } r_d \geq \frac{g_d}{g_{d-1} + g_d}, \\ \frac{g_d(1-r_d)}{g_{d-1}} & \text{for } r_d \leq \frac{g_d}{g_{d-1} + g_d}, \end{cases} \quad (80a)$$

$$\min_{\mathbf{q}} \{q_d | \mathbf{q} \in \mathcal{T}_{\mathbf{g}}(\bar{\mathbf{r}})\} = 0. \quad (80b)$$

We start with the second statement. It can be simply proved by observing that for $d \geq 3$ we have (by definition) $\bar{r}_1 = 0$, and so using T from Eq. (79) with $i = 1$, $j = d$ and $a = r_d$, all the occupation of level d can be moved to level 1. Since probabilities must be non-negative, the achieved value of $q_d = 0$ is minimal.

To prove Eq. (80a), we need to resort to thermomajorisation curves. Since $\bar{\mathbf{r}}$ has only two non-zero entries, its thermomajorisation curve is given by three points, the first one being $(0, 0)$ and the third one being $(1, 1)$. The middle point is given by (g_d, r_d) if $r_d \geq g_d/(g_{d-1} + g_d)$ and by $(g_{d-1}, 1 - r_d)$ otherwise. In the first case, for the thermomajorisation curve of \mathbf{q} to lie below that of $\bar{\mathbf{r}}$, its y component must be no higher than r_d at the x component g_d . Given that the thermomajorisation curve is concave, this means that $q_d \leq r_d$. In the second case, the y component of the thermomajorisation curve of \mathbf{r} at x component g_d is given by $(1 - r_d)g_d/g_{d-1}$. Therefore, for the thermomajorisation curve of \mathbf{q} to lie below that of $\bar{\mathbf{r}}$, the maximum value of q_d must be upper bounded by $(1 - r_d)g_d/g_{d-1}$. Moreover, this upper bound can be achieved by simply choosing \mathbf{q} with that value of q_d and all others proportional to the entries of the Gibbs state, i.e., $q_i = g_i(1 - q_d)/(1 - g_d)$ for $i < d$.

C Proof of Lemma 3

Proof. We start from proving the first half of the lemma (related to distributions \mathbf{p} , \mathbf{p}' and \mathbf{p}''). Consider a state $\check{\mathbf{p}}$ obtained from \mathbf{p} by thermalising the first $(d-1)$ levels of the system with respect to the cold bath, i.e.,

$$\check{\mathbf{p}} = \left(\frac{1 - p_d}{1 - \gamma_d} \gamma_1, \frac{1 - p_d}{1 - \gamma_d} \gamma_2, \dots, \frac{1 - p_d}{1 - \gamma_d} \gamma_{d-1}, p_d \right). \quad (81)$$

Clearly, $\mathbf{p} \succ_\gamma \check{\mathbf{p}}$, as thermalising a subset of states is a thermal operation. Since

$$\check{p}_d = p_d \geq \Gamma_d \geq \gamma_d, \quad (82)$$

and the remaining entries \check{p}_i are proportional to the entries of the thermal distribution γ , the thermomajorisation curve of $\check{\mathbf{p}}$ with respect to γ is defined by three points: $(0, 0)$, (γ_d, p_d) and $(1, 1)$. Thus, for the x component γ_1 , its y component is given by

$$p'_1 = p_d + \frac{\gamma_1 - \gamma_d}{1 - \gamma_d} (1 - p_d) = \frac{1 - \gamma_1}{1 - \gamma_d} p_d + \frac{\gamma_1 - \gamma_d}{1 - \gamma_d}. \quad (83)$$

This means that $\check{\mathbf{p}}$ can be transformed to \mathbf{p}' with the above occupation of the ground state p'_1 and the remaining occupations p'_i simply chosen to be proportional to the entries of the thermal distribution γ . Finally, since thermomajorisation is transitive, we have $\mathbf{p} \succ_\gamma \mathbf{p}'$.

The next step is to start with \mathbf{p}' and thermalise levels $\{2, \dots, d\}$ with respect to the hot bath, resulting in

$$\check{\mathbf{p}}' = \left(p'_1, \frac{1 - p'_1}{1 - \Gamma_1} \Gamma_2, \dots, \frac{1 - p'_1}{1 - \Gamma_1} \Gamma_d \right). \quad (84)$$

Again, it is clear that $\mathbf{p}' \succ_\Gamma \check{\mathbf{p}}'$. Since

$$\check{p}'_1 = p'_1 \geq \gamma_1 \geq \Gamma_1, \quad (85)$$

and the remaining entries \check{p}'_i are proportional to entries of the thermal distribution Γ , the thermomajorisation curve of $\check{\mathbf{p}}'$ with respect to Γ is defined by three points: $(0, 0)$, (Γ_1, p'_1) and $(1, 1)$. Thus, for the x component Γ_d , its y component is given by

$$p''_d = \frac{\Gamma_d}{\Gamma_1} p'_1 = \frac{(1 - \gamma_1) \Gamma_d}{(1 - \gamma_d) \Gamma_1} p_d + \frac{(\gamma_1 - \gamma_d) \Gamma_d}{(1 - \gamma_d) \Gamma_1}. \quad (86)$$

This means that $\check{\mathbf{p}}'$ can be transformed to \mathbf{p}'' with the above occupation of the highest state p''_d and the remaining occupations p''_i simply chosen to be proportional to the entries of the thermal distribution Γ . Since thermomajorisation is transitive, we have $\mathbf{p}' \succ_\Gamma \mathbf{p}''$. Combining everything together and using again the transitivity property of thermomajorisation, we end up with Eq. (28) (its half concerning \mathbf{p} , \mathbf{p}' and \mathbf{p}'') with \mathbf{p}'' satisfying Eq. (29a). Finally, to show that $p''_d \geq p_d$ and $p''_d \leq \tilde{\Gamma}_d$, one simply needs to use the assumption that $\Gamma_d \leq p_d \leq \tilde{\Gamma}_d$.

Now, let us switch to the second part of the lemma. Consider a state $\check{\mathbf{q}}$ obtained from \mathbf{q} by thermalising the levels $\{2, \dots, d\}$ of the system with respect to the hot bath, i.e.,

$$\check{\mathbf{q}} = \left(q_1, \frac{1 - q_1}{1 - \Gamma_1} \Gamma_2, \dots, \frac{1 - q_1}{1 - \Gamma_1} \Gamma_d \right). \quad (87)$$

Clearly, $\mathbf{q} \succ_\Gamma \check{\mathbf{q}}$, as thermalising a subset of states is a thermal operation. Since

$$\check{q}_1 = q_1 \geq \gamma_1 \geq \Gamma_1, \quad (88)$$

and the remaining entries \check{q}_i are proportional to the entries of the thermal distribution Γ , the thermomajorisation curve of $\check{\mathbf{q}}$ with respect to Γ is defined by three points: $(0, 0)$, (Γ_1, q_1) and $(1, 1)$. Thus, for the x component Γ_d , its y component is given by

$$q'_d = \frac{\Gamma_d}{\Gamma_1} q_1. \quad (89)$$

This means that $\check{\mathbf{q}}$ can be transformed to \mathbf{q}' with the above occupation of the highest excited state q'_d and the remaining occupations q'_i simply chosen to be proportional to the entries of the thermal distribution Γ . Finally, since thermomajorisation is transitive, we have $\mathbf{q} \succ_\Gamma \mathbf{q}'$.

The next step is to start with \mathbf{q}' and thermalise levels $\{1, \dots, d - 1\}$ with respect to the cold bath, resulting in

$$\check{\mathbf{q}}' = \left(\frac{1 - q'_d}{1 - \gamma_d} \gamma_1, \dots, \frac{1 - q'_d}{1 - \gamma_d} \gamma_{d-1}, q'_d \right). \quad (90)$$

Again, it is clear that $\mathbf{q}' \succ_\gamma \check{\mathbf{q}}'$. Since

$$\check{q}'_d = q'_d \geq \Gamma_d \geq \gamma_d, \quad (91)$$

and the remaining entries \check{q}'_i are proportional to entries of the thermal distribution γ , the thermomajorisation curve of $\check{\mathbf{q}}'$ with respect to γ is defined by three points: $(0, 0)$, (γ_d, q'_d) and $(1, 1)$. Thus, for the x component γ_1 , its y component is given by

$$q''_1 = q'_d + \frac{\gamma_1 - \gamma_d}{1 - \gamma_d} (1 - q'_d) = \frac{(1 - \gamma_1) \Gamma_d}{(1 - \gamma_d) \Gamma_1} q_1 + \frac{\gamma_1 - \gamma_d}{1 - \gamma_d}. \quad (92)$$

This means that $\check{\mathbf{q}}'$ can be transformed to \mathbf{q}'' with the above occupation of the ground state q''_1 and the remaining occupations q''_i simply chosen to be proportional to the entries of the thermal distribution γ . Since thermomajorisation is transitive, we have $\mathbf{q}' \succ_\gamma \mathbf{q}''$. Combining everything together and using again the transitivity property of thermomajorisation, we end up with Eq. (28) (its half concerning \mathbf{q} , \mathbf{q}' and \mathbf{q}'') with \mathbf{q}'' satisfying Eq. (29b). Finally, to show that $q''_1 \geq q_1$ and $q''_1 \leq \tilde{\gamma}_1$, one simply needs to use the assumption that $\gamma_1 \leq q_1 \leq \tilde{\gamma}_1$. \square

D Proof of Proposition 6

The proof is based on the following crucial lemma.

Lemma 17. *Assume γ and Γ satisfy the requirements of Proposition 6 from Eq. (34), and the initial state \mathbf{p} satisfies*

$$\forall k : \quad \frac{p_k}{\gamma_k} \geq \frac{p_{k+1}}{\gamma_{k+1}}. \quad (93)$$

Then,

$$\mathbf{p} \succ_{\Gamma} \mathbf{q} \succ_{\gamma} \mathbf{r}, \quad (94)$$

with

$$q_1 = p_d + \frac{\Gamma_1 - \Gamma_d}{\Gamma_{d-1}} p_{d-1}, \quad q_k = \frac{\Gamma_k}{1 - \Gamma_1} (1 - q_1), \quad (95a)$$

$$r_1 = 1 - \frac{1 - \gamma_1}{\gamma_1} q_1, \quad r_k = \frac{\gamma_k}{\gamma_1} q_1, \quad (95b)$$

for $k > 1$. Moreover,

$$\forall k : \quad \frac{r_k}{\gamma_k} \geq \frac{r_{k+1}}{\gamma_{k+1}}. \quad (96)$$

For the sake of clarity of the argument, we defer the proof of the above lemma to the end of this appendix. The lemma tells us that a sequential interaction of the initial state \mathbf{p} with a hot and a cold bath can transform it to a final state \mathbf{r} . Since the final state \mathbf{r} satisfies Eq. (96), one can apply Lemma 17 iteratively, starting from $\mathbf{p}[1] = \gamma$. Thus, given a vector $\mathbf{p}[n]$ satisfying Eq. (93), we can transform it to $\mathbf{p}[n+1]$ also satisfying Eq. (93) and with

$$p_1[n+1] = 1 - \frac{1 - \gamma_1}{\gamma_1} \left(p_d[n] + \frac{\Gamma_1 - \Gamma_d}{\Gamma_{d-1}} p_{d-1}[n] \right), \quad (97)$$

$$p_k[n+1] = \frac{\gamma_k}{\gamma_1} \left(p_d[n] + \frac{\Gamma_1 - \Gamma_d}{\Gamma_{d-1}} p_{d-1}[n] \right), \quad (98)$$

for $k > 1$. Now, we have

$$p_d[n+1] + p_{d-1}[n+1] = \frac{\gamma_d + \gamma_{d-1}}{\gamma_1} \left(p_d[n] + \frac{\Gamma_1 - \Gamma_d}{\Gamma_{d-1}} p_{d-1}[n] \right) \leq \frac{\gamma_d + \gamma_{d-1}}{\gamma_1} (p_d[n] + p_{d-1}[n]), \quad (99)$$

where we have used the assumption $\Gamma_1 < \Gamma_d + \Gamma_{d-1}$ from Eq. (34). We thus have

$$p_d[n+1] + p_{d-1}[n+1] \leq \left(\frac{\gamma_d + \gamma_{d-1}}{\gamma_1} \right)^n (p_d[1] + p_{d-1}[1]), \quad (100)$$

and because the exponentiated prefactor on the right hand side is strictly smaller than 1 (again, due to the assumption from Eq. (34)), we get

$$\lim_{n \rightarrow \infty} (p_d[n] + p_{d-1}[n]) = 0. \quad (101)$$

Obviously both $p_d[n]$ and $p_{d-1}[n]$ are positive, and so they both independently tend to zero as $n \rightarrow \infty$. Through Eq. (97), this then means that

$$\lim_{n \rightarrow \infty} p_1[n] = 1, \quad (102)$$

which proves Proposition 6. Note that because the convergence is exponential, the ground state is only achieved in the limit $n \rightarrow \infty$. The last remaining thing to show is to prove Lemma 17.

Proof of Lemma 17. For \mathbf{p} satisfying Eq. (93), it is straightforward to show that it also satisfies

$$\forall k : \quad \frac{p_k}{\Gamma_k} \geq \frac{p_{k+1}}{\Gamma_{k+1}}. \quad (103)$$

Given the above, the thermomajorisation curve of \mathbf{p} with respect to the hot bath Γ is given by the following elbow points:

$$\{(0, 0), (\Gamma_1, p_1), \dots, (1 - \Gamma_d - \Gamma_{d-1}, 1 - p_d - p_{d-1}), (1 - \Gamma_d, 1 - p_d), (1, 1)\}. \quad (104)$$

Since, by assumption from Eq. (34), we have

$$1 - \Gamma_d - \Gamma_{d-1} \leq 1 - \Gamma_1 \leq 1 - \Gamma_d, \quad (105)$$

the thermomajorisation curve of \mathbf{p} at the x position $(1 - \Gamma_1)$ takes the value

$$1 - q_1 = 1 - p_d - p_{d-1} + \frac{\Gamma_d + \Gamma_{d-1} - \Gamma_1}{\Gamma_{d-1}} p_{d-1} = 1 - p_d - \frac{\Gamma_1 - \Gamma_d}{\Gamma_{d-1}} p_{d-1}. \quad (106)$$

Clearly then, a piecewise linear concave curve defined by the following elbow points,

$$\{(0, 0), (1 - \Gamma_1, 1 - q_1), (1, 1)\}, \quad (107)$$

lies below the thermomajorisation curve of \mathbf{p} . As can be verified by direct calculation, such a curve is a thermomajorisation curve of a state \mathbf{q} from Eq. (95a), which satisfies

$$\forall k : \quad \frac{q_k}{\Gamma_k} \leq \frac{q_{k+1}}{\Gamma_{k+1}}. \quad (108)$$

This proves the first part of the lemma.

To prove the second part, we start by noting that Eq. (108) implies

$$\forall k : \quad \frac{q_k}{\gamma_k} \leq \frac{q_{k+1}}{\gamma_{k+1}}. \quad (109)$$

Given the above, the thermomajorisation curve of \mathbf{q} with respect to the cold bath γ is given by the following elbow points:

$$\{(0, 0), (\gamma_d, q_d), (\gamma_d + \gamma_{d-1}, q_d + q_{d-1}), \dots, (1 - \gamma_1, 1 - q_1), (1, 1)\}. \quad (110)$$

Since, by assumption from Eq. (34), we have

$$1 - \gamma_1 \leq \gamma_1 \leq 1, \quad (111)$$

the thermomajorisation curve of \mathbf{q} at the x position γ_1 takes the value

$$r_1 = 1 - q_1 + \frac{2\gamma_1 - 1}{\gamma_1} q_1 = 1 - \frac{1 - \gamma_1}{\gamma_1} q_1. \quad (112)$$

Clearly then, a piecewise linear concave curve defined by the following elbow points,

$$\{(0, 0), (\gamma_1, r_1), (1, 1)\}, \quad (113)$$

lies below the thermomajorisation curve of \mathbf{q} . As can be verified by direct calculation, such a curve is a thermomajorisation curve of a state \mathbf{r} from Eq. (95b), which satisfies

$$\forall k : \quad \frac{r_k}{\gamma_k} \geq \frac{r_{k+1}}{\gamma_{k+1}}. \quad (114)$$

This completes the proof. □

E Maximally mutually coherent states

Existence and generation in three strokes

Let us start by recalling a known result about the existence of maximally mutually coherent states exist for any two given bases and in any dimension (see Ref. [42], whose results imply the statement; cf. also Refs. [41] and [43]).

Theorem 18 ([41, Theorem 1]). *For any two bases $\{|j\rangle\}_{j=1}^d$ and $\{U^\dagger|j\rangle\}_{j=1}^d$ of a d -dimensional Hilbert space there exist at least 2^{d-1} states $|\psi_*\rangle$ that are unbiased in both these bases, that is,*

$$|\langle j|\psi_*\rangle| = |\langle j|U|\psi_*\rangle| = \frac{1}{\sqrt{d}} \quad \text{for all } j \in \{1, \dots, d\}, \quad (115)$$

which, in turn, implies that

$$|\psi_*\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^d e^{i\alpha_j} |j\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^d e^{i\beta_j} U^\dagger |j\rangle. \quad (116)$$

Moreover, any state $|\psi_*\rangle$ satisfying Eq. (115) is a zero-noise, zero-disturbance state, also called a mutually coherent (or maximally mutually coherent) state (see Ref. [43]).

Remark 19. The assertion of Theorem 18 follows from the fact that a great torus T_{d-1} embedded in a complex projective space $\mathbb{C}P^{d-1}$ is *non-displaceable* with respect to transformations by a unitary matrix $U \in \mathcal{U}_d(\mathbb{C})$ (cf. [59]), meaning that the image of torus resulting from the action of U must intersect the original torus, in at least 2^{d-1} points (for a more detailed explanation see, e.g., Ref. [43]).

Next, consider the problem of generating a maximally mutually coherent state by performing only three operations (preparation of $|l\rangle$ by Alice, transformation $U^\dagger D_1 U$ by Bob, and transformation D_2 by Alice). From what has been said above, this task can be reduced to guaranteeing the existence of $l \in \{1, \dots, d\}$ and $D_1, D_2 \in \mathcal{DU}_d(\mathbb{C})$ such that $U^\dagger D_1 U$ has a flat l -th column, i.e.,

$$|\langle m | U^\dagger D_1 U | l \rangle| = \frac{1}{\sqrt{d}} \quad \text{for all } m \in \{1, \dots, d\}, \quad (117)$$

and

$$D_2 U^\dagger D_1 U | l \rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^d e^{i\alpha_j} | j \rangle = |\psi_*\rangle. \quad (118)$$

Note that D_2 is only responsible for fitting the phases α_j , $j \in \{1, \dots, d\}$.

Qubit case

Before we proceed to the proof of Proposition 14, which deals with a general problem of generating a maximally mutually coherent state using just three strokes of a coherence engine, let us first show how the problem is solved in the case of a qubit (simple heuristics have been already presented in Sec. 3.2, however this analytical proof can be more easily generalised to higher dimensions).

Proposition 20. *Suppose that Alice and Bob are restricted to the sets F_A, F_B of their free states and $\mathcal{F}_A, \mathcal{F}_B$ of their free operations, respectively. Let $U \in \mathcal{U}_2(\mathbb{C})$, appearing in the definition of \mathcal{F}_B in Eq. (39b), be of the general form*

$$U = e^{i\phi} \begin{bmatrix} e^{i\varphi_0} \cos(\varphi) & -e^{-i\varphi_1} \sin(\varphi) \\ e^{i\varphi_1} \sin(\varphi) & e^{-i\varphi_0} \cos(\varphi) \end{bmatrix}. \quad (119)$$

Then, the parties can generate a maximally mutually coherent state with only three resource engine's strokes if and only if $\varphi \in [\pi/8, 3\pi/8]$.

Proof. Let $D := \text{diag}(e^{i\theta_0}, e^{i\theta_1})$, with $\theta_0, \theta_1 \in [0, 2\pi)$, be an arbitrary diagonal unitary matrix. Due to Eq. (119), we obviously have

$$\langle 0 | U^\dagger D U | 0 \rangle = e^{i\theta_0} \cos^2(\varphi) + e^{i\theta_1} \sin^2(\varphi) \quad \text{and} \quad \langle 1 | U^\dagger D U | 0 \rangle = \sin(\varphi) \cos(\varphi) e^{i(\varphi_0 + \varphi_1)} (-e^{i\theta_0} + e^{i\theta_1}). \quad (120)$$

It follows from the previous subsection that one can generate a maximally mutually coherent state with just three resource engine's strokes if and only if either

$$\exists_{\theta_2, \theta_3 \in (0, 2\pi]} \quad \langle 0 | U^\dagger D U | 0 \rangle = e^{i\theta_2} \frac{1}{\sqrt{2}} \quad \text{and} \quad \langle 1 | U^\dagger D U | 0 \rangle = e^{i\theta_3} \frac{1}{\sqrt{2}} \quad (121)$$

or

$$\exists_{\theta_2, \theta_3 \in (0, 2\pi]} \quad \langle 0 | U^\dagger D U | 1 \rangle = e^{i\theta_2} \frac{1}{\sqrt{2}} \quad \text{and} \quad \langle 1 | U^\dagger D U | 1 \rangle = e^{i\theta_3} \frac{1}{\sqrt{2}}. \quad (122)$$

If we now compare Eq. (120) with Eq. (121) (the reasoning for Eq. (122) is analogous), we get

$$\exists_{\theta_0, \theta_1, \theta_2, \theta_3 \in [0, 2\pi]} \quad e^{i\theta_0} \cos^2(\varphi) + e^{i\theta_1} \sin^2(\varphi) - \frac{e^{i\theta_2}}{\sqrt{2}} = 0, \quad \sin(\varphi) \cos(\varphi) e^{i(\varphi_0 + \varphi_1)} (e^{i\theta_1} - e^{i\theta_0}) - \frac{e^{i\theta_3}}{\sqrt{2}} = 0. \quad (123)$$

To verify when the above holds, let us consider two triangles (in the complex plane) with vertices:

$$\begin{aligned} (1) : & \{0, -e^{i\theta_0} \sin(\varphi) \cos(\varphi), -e^{i\theta_0} \sin(\varphi) \cos(\varphi) + e^{i\theta_1} \sin(\varphi) \cos(\varphi)\}, \\ (2) : & \{0, e^{i\theta_0} \cos^2(\varphi), e^{i\theta_0} \cos^2(\varphi) + e^{i\theta_1} \sin^2(\varphi)\}, \end{aligned} \quad (124)$$

where $\varphi, \theta_0, \theta_1 \in [0, 2\pi)$. One can easily observe that triangle (1) is isosceles with legs of length $\sin(\varphi) \cos(\varphi)$. The base of this triangle can have length $1/\sqrt{2}$ only if $2 \sin(\varphi) \cos(\varphi) \geq 1/\sqrt{2}$ (the triangle inequality), which yields

$$\frac{\pi}{8} \leq \varphi \leq \frac{3\pi}{8}. \quad (125)$$

If we denote the measure of the angles at the base by α , then the third angle obviously has measure $\pi - 2\alpha$. Note that for a fixed value of φ , where $\varphi \in [\pi/8, 3\pi/8]$, there is only one possible value of α , namely

$$\alpha = \arccos\left(\frac{1}{2\sqrt{2} \sin(\varphi) \cos(\varphi)}\right). \quad (126)$$

Analysis similar to the above one (based on applying triangle inequalities) indicates that the third side of triangle (2) has length $1/\sqrt{2}$ if and only if φ and α (being half of the angle between the sides of triangle (2), of lengths $\cos^2(\varphi)$ and $\sin^2(\varphi)$) satisfy Eqs. (125) and (126), respectively. As a consequence, we obtain the following: for any $\varphi, \varphi_0, \varphi_1 \in [0, 2\pi)$, Eq. (123) holds if and only if $\varphi \in [\pi/8, 3\pi/8]$, which completes the proof. \square

Proof of Proposition 14

Using the intuition from the case of a qubit, let us now conduct the proof of Proposition 14.

Proof of Proposition 14. The necessary condition in the case of $d = 2$ (namely, $\pi/8 \leq \varphi \leq 3\pi/8$) follows just from the triangle inequalities. For an arbitrary $d \in \mathbb{N} \setminus \{1, 2\}$ the reasoning is analogous (with the difference that in higher dimensions the necessary conditions are no longer the sufficient ones). As already mentioned at the beginning of this appendix, to solve the given task, it suffices to find a matrix $U = (u_{i,j})_{i,j=1}^d \in \mathcal{U}_d(\mathbb{C})$ for which Eq. (117) is satisfied with some $|l\rangle$, $l \in \{1, \dots, d\}$, and some $D_1 \in \mathcal{DU}_n(\mathbb{C})$, i.e.,

$$\exists_{l \in \{1, \dots, d\}} \exists_{\kappa_1, \dots, \kappa_d \in (0, 2\pi]} \forall_{m \in \{1, \dots, d\}} \langle m | U^\dagger D_1 U | l \rangle = e^{i\kappa_m} \frac{1}{\sqrt{d}}. \quad (127)$$

Writing it differently, we obtain (for $D = \text{diag}(e^{i\xi_1}, \dots, e^{i\xi_d})$)

$$\exists_{l \in \{1, \dots, d\}} \exists_{\kappa_1, \dots, \kappa_d \in (0, 2\pi]} \forall_{m \in \{1, \dots, d\}} \sum_{j=1}^d e^{i\xi_j} \bar{u}_{jm} u_{jl} = e^{i\kappa_m} \frac{1}{\sqrt{d}}, \quad (128)$$

which is kind of an equivalent of Eq. (123). The generalised polygon inequalities then imply the assertion of Proposition 14. \square

F Proof of Proposition 8

In Sec. 3.3, for any $U \in \mathcal{U}_d(\mathbb{C})$, we have defined a matrix P_U , whose entries are zero whenever the corresponding entries of U are zero, otherwise they are equal to 1 (cf. Eq. (48)). Here, it is convenient to additionally introduce a matrix $R_U = (r_{ij})_{i,j=1}^d$ over the field \mathbb{R}_+ , which corresponds to U in the following sense:

$$r_{ij} = \begin{cases} 0 & \text{for } u_{ij} = 0, \\ \text{some positive number } r_{ij} & \text{for } u_{ij} \neq 0. \end{cases} \quad (129)$$

The aim of this appendix is to prove that hypotheses (H1) and (H2) are equivalent. For this, we shall first establish a few auxiliary facts.

Lemma 21. *Let $A = (a_{ij})_{i,j=1}^d$ and $D = \text{diag}(d_1, \dots, d_d)$ with $d_i \neq 0$ for any $i \in \{1, \dots, d\}$. Then, for $AD = (b_{ij})_{i,j=1}^d$ and any $k, l \in \{1, \dots, d\}$*

$$a_{kl} = 0 \quad \Leftrightarrow \quad b_{kl} = 0. \quad (130)$$

Proof. Note that for any $k, l \in \{1, \dots, d\}$ we have $b_{kl} = a_{kl} d_l$, which immediately yields the assertion of Lemma 21. \square

Lemma 22. *Let $U = (u_{ij})_{i,j=1}^d, V = (v_{ij})_{i,j=1}^d \in \mathcal{U}_d(\mathbb{C})$, and let $R_U = (r_{ij})_{i,j=1}^d, R_V = (s_{ij})_{i,j=1}^d$ be the corresponding matrices, with entries in \mathbb{R}_+ , satisfying Eq. (129). Then, there exists $D = (d_{ij})_{i,j=1}^d \in \mathcal{DU}_d(\mathbb{C})$ such that for all $k, l \in \{1, \dots, d\}$*

$$(R_U R_V)_{kl} \neq 0 \quad \Leftrightarrow \quad (UDV)_{kl} \neq 0. \quad (131)$$

Proof. Let $D \in \mathcal{DU}_d(\mathbb{C})$, and let $k, l \in \{1, \dots, d\}$ be arbitrary. We shall first prove the simpler direction, i.e.,

$$(UDV)_{kl} \neq 0 \quad \Rightarrow \quad (R_U R_V)_{kl} \neq 0. \quad (132)$$

Observe that $(UDV)_{kl} \neq 0$ if and only if $\sum_{m=1}^d u_{km} d_m v_{ml} \neq 0$. This, however, implies that there exists at least one $m_0 \in \{1, \dots, d\}$ such that $u_{km_0} v_{m_0 l} \neq 0$. Further, referring to Eq. (129), we get that $r_{km_0} s_{m_0 l} > 0$. Keeping in mind that $r_{ij}, s_{ij} \geq 0$ for all $i, j \in \{1, \dots, d\}$, we finally obtain $(R_U R_V)_{kl} = \sum_{m=1}^d r_{km} s_{ml} > 0$, which completes the proof of Eq. (132).

We now proceed to the harder direction, i.e., to proving that for any $(k, l) \in \{1, \dots, d\}$

$$(R_U R_V)_{kl} \neq 0 \quad \Rightarrow \quad (UDV)_{kl} \neq 0. \quad (133)$$

Let us define

$$I = \{(k, l) : k, l \in \{1, \dots, d\}, (R_U R_V)_{kl} \neq 0\}. \quad (134)$$

We shall construct a matrix $D \in \mathcal{DU}_d(\mathbb{C})$ such that

$$(UDV)_{kl} \neq 0 \quad \text{for all } (k, l) \in I. \quad (135)$$

Note that $(R_U R_V)_{kl} \neq 0$ if and only if $\sum_{m=1}^d r_{km} s_{ml} \neq 0$. Since the matrices R_U and R_V satisfy Eq. (129), we further get that there exists at least one $m_0 \in \{1, \dots, d\}$ such that $u_{km_0} v_{m_0 l} \neq 0$.

For any $(k, l) \in I$ let us define a vector

$$\mathbf{w}^{(kl)} = \left(w_m^{(kl)} \right)_{m=1}^d \quad \text{with } w_m^{(kl)} = u_{km} v_{ml} \quad \text{for all } m \in \{1, \dots, d\}. \quad (136)$$

Further, let us also introduce

$$\mathcal{W} = \left\{ \mathbf{w}^{(kl)} : (k, l) \in I \right\}, \quad (137)$$

the subsets G_N of \mathcal{W} given by

$$G_N = \{ \mathbf{w} \in \mathcal{W} : w_1 = \dots = w_{N-1} = 0, w_N \neq 0 \} \quad \text{for } N \in \{1, \dots, d\}, \quad (138)$$

and the corresponding sets of indexes

$$I_N = \left\{ (k, l) \in I : \mathbf{w}^{(kl)} \in G_N \right\} \quad \text{for } N \in \{1, \dots, d\}. \quad (139)$$

Note that $\{G_N\}_{N=1}^d$ and $\{I_N\}_{N=1}^d$ constitute partitions of the sets \mathcal{W} and I , respectively.

The construction of the matrix $D \in \mathcal{DU}_d(\mathbb{C})$ for which Eq. (135) holds now proceeds as follows. Define

$$D^{(1)} := \text{diag} \left(d_1^{(1)}, \dots, d_d^{(1)} \right) \quad \text{with } d_m^{(1)} = \begin{cases} e^{i\varphi_1} & \text{if } m = 1 \\ 1 & \text{if } m \neq 1 \end{cases}, \quad \varphi_1 \in (0, 2\pi). \quad (140)$$

If $(k, l) \in I_1$, then $\mathbf{w}^{(kl)} \in G_1$, and

$$\sum_{m=1}^d w_m^{(kl)} d_m^{(1)} = e^{i\varphi_1} w_1^{(kl)} + \sum_{m=2}^d w_m^{(kl)} = (e^{i\varphi_1} - 1) w_1^{(kl)} + \sum_{m=1}^d w_m^{(kl)}. \quad (141)$$

Hence, for $(k, l) \in I_1$, we have

$$\left(UD^{(1)}V \right)_{kl} = \sum_{m=1}^d u_{km} d_m^{(1)} v_{ml} = \sum_{m=1}^d w_m^{(kl)} d_m^{(1)} \neq 0 \quad (142)$$

if and only if

$$e^{i\varphi_1} \neq 1 - \frac{1}{w_1^{(kl)}} \sum_{m=1}^d w_m^{(kl)}. \quad (143)$$

Note that $w_1^{(kl)} \neq 0$, since $\mathbf{w}^{(kl)} \in G_1$.

For any $(k, l) \in I_1$ there is at most one value $\varphi_1 \in (0, 2\pi)$ which violates Eq. (143). Since I_1 is a finite set, we see that the set

$$F_1 = \left\{ \varphi_1 \in (0, 2\pi) : \exists_{(k,l) \in I_1} e^{i\varphi_1} = 1 - \sum_{m=1}^d \frac{w_m^{(kl)}}{w_1^{(kl)}} \right\} \quad (144)$$

is also finite. We can therefore easily choose $\varphi_1 \in (0, 2\pi)$ such that Eq. (142) holds for all $(k, l) \in I_1$. In particular, it suffices to take any number φ_1 from the uncountable set $F_1' = (0, 2\pi) \setminus F_1$.

Now, let $N \in \{1, \dots, d-1\}$, and suppose that the matrix $D^{(N)}$ satisfies

$$\left(UD^{(N)}V \right)_{kl} \neq 0 \quad \text{for all } (k, l) \in I_1 \cup \dots \cup I_N. \quad (145)$$

Moreover, assume that $D^{(N)}$ has the following form:

$$D^{(N)} := \text{diag} \left(d_1^{(N)}, \dots, d_d^{(N)} \right) \quad \text{with } d_m^{(N)} = \begin{cases} e^{i\varphi_m} & \text{if } m \in \{1, \dots, N\} \\ 1 & \text{otherwise} \end{cases}, \quad (146)$$

where $\varphi_1, \dots, \varphi_N \in (0, 2\pi)$ are some constants. Then we can introduce matrices

$$D^{(N+1)} := \text{diag} \left(d_1^{(N+1)}, \dots, d_d^{(N+1)} \right) \quad \text{with } d_m^{(N+1)} = \begin{cases} e^{i\varphi_{N+1}} & \text{if } m = N+1 \\ d_m^{(N)} & \text{if } m \neq N+1 \end{cases}, \quad \text{where } \varphi_{N+1} \in (0, 2\pi), \quad (147)$$

The aim now is to prove that the constant φ_{N+1} can be always chosen in such a way that

$$\left(UD^{(N+1)}V \right)_{kl} \neq 0 \quad \text{for all } (k, l) \in \bigcup_{u=1}^{N+1} I_u. \quad (148)$$

Define the sets $F_{(N+1),u}$ with $u \in \{1, \dots, N+1\}$ as

$$F_{(N+1),u} = \left\{ \varphi_{N+1} \in (0, 2\pi) : \exists_{D^{(N+1)} \text{ given by Eq. (147)}} \exists_{(k,l) \in I_u} \left(UD^{(N+1)}V \right)_{kl} = 0 \right\}. \quad (149)$$

Let us prove that for any $u \in \{1, \dots, N+1\}$ the set $F_{(N+1),u}$ is finite. Fix $u \in \{1, \dots, N+1\}$ and $(k, l) \in I_u$ arbitrarily. We have

$$\left(UD^{(N+1)}V \right)_{kl} = \sum_{m=1}^d w_m^{(kl)} d_m^{(N+1)} = \sum_{m=1}^{N+1} (e^{i\varphi_m} - 1) w_m^{(kl)} + \sum_{m=1}^d w_m^{(kl)}, \quad (150)$$

which is equal to zero if and only if

$$(e^{i\varphi_{N+1}} - 1) w_{N+1}^{(kl)} = - \sum_{m=1}^d w_m^{(kl)} - \sum_{m=1}^N (e^{i\varphi_m} - 1) w_m^{(kl)}. \quad (151)$$

If $w_{N+1}^{(kl)} \neq 0$, then Eq. (151) is equivalent to

$$e^{i\varphi_{N+1}} = 1 - \sum_{m=1}^d \frac{w_m^{(kl)}}{w_{N+1}^{(kl)}} - \sum_{m=1}^N (e^{i\varphi_m} - 1) \frac{w_m^{(kl)}}{w_{N+1}^{(kl)}}, \quad (152)$$

which holds for at most one $\varphi_{N+1} \in (0, 2\pi)$. On the other hand, if $w_{N+1} = 0$, then it follows from Eq. (151) that

$$0 = - \sum_{m=1}^d w_m^{(kl)} - \sum_{m=1}^N (e^{i\varphi_m} - 1) w_m^{(kl)} = - \left(UD^{(N)}V \right)_{kl}. \quad (153)$$

This, however, contradicts our assumption from Eq. (145). Hence, we see that for any $u \in \{1, \dots, N+1\}$

$$F_{(N+1),u} = \left\{ \varphi_{N+1} \in (0, 2\pi) : \exists_{(k,l) \in I_u} w_{N+1}^{(kl)} \neq 0 \text{ and } e^{i\varphi_{N+1}} = 1 - \sum_{m=1}^d \frac{w_m^{(kl)}}{w_{N+1}^{(kl)}} - \sum_{m=1}^N (e^{i\varphi_m} - 1) \frac{w_m^{(kl)}}{w_{N+1}^{(kl)}} \right\}, \quad (154)$$

and, since I_u is finite for any $u \in \{1, \dots, N+1\}$, then so is $F_{(N+1),u}$.

Now, choosing

$$\varphi_{N+1} \in F'_{N+1} = (0, 2\pi) \setminus F_{N+1}, \quad \text{where } F_{N+1} = \bigcup_{u=1}^{N+1} F_{(N+1),u}, \quad (155)$$

we can guarantee that condition from Eq. (148) is fulfilled.

Finally, recalling that $I = \bigcup_{m=1}^n I_m$, we can define

$$D := \text{diag}(d_1, \dots, d_d) \quad \text{with } d_m = e^{i\varphi_m}, \quad \varphi_m \in F'_m \quad \text{for } m \in \{1, \dots, d\}, \quad (156)$$

where

$$F'_m = (0, 2\pi) \setminus F_m, \quad F_m = \bigcup_{u=1}^m F_{m,u} \quad (157)$$

and any $F_{m,u}$ is defined as in Eq. (154). The above choice of $\varphi_1, \dots, \varphi_d$ is always possible (if done inductively on d), since the sets F'_1, \dots, F'_d are uncountable. □

As a corollary of Lemmas 21 and 22 we obtain the following statement.

Corollary 23. *Let $U \in \mathcal{U}_d(\mathbb{C})$, and let R_U be an arbitrary matrix over the field \mathbb{R}_+ satisfying Eq. (129) (in particular, it can be P_U , given by Eq. (48)). Then there exist matrices $D_1, D_2 \in \mathcal{DU}_d(\mathbb{C})$ such that for any $k, l \in \{1, \dots, d\}$*

$$(R_U^T R_U)_{kl} = 0 \quad \Leftrightarrow \quad (D_1 U^\dagger D_2 U)_{kl} = 0. \quad (158)$$

To finally prove the equivalence of hypotheses (H1) and (H2) it suffices to establish the following lemma.

Lemma 24. *Let $U \in \mathcal{U}_d(\mathbb{C})$. For any $M \in \mathbb{N}$ there exist matrices $D_1, \dots, D_{2M} \in \mathcal{DU}_d(\mathbb{C})$ such that for any $k, l \in \{1, \dots, d\}$*

$$\left((P_U^T P_U)^M \right)_{kl} = 0 \quad \Leftrightarrow \quad (D_1 U^\dagger D_2 U \dots D_{2M-1} U^\dagger D_{2M} U)_{kl} = 0. \quad (159)$$

Proof. First of all, note that the assertion of Lemma 24 for $M = 1$ immediately follows from Corollary 23. To establish it for all $M \in \mathbb{N}$, we shall conduct an inductive proof. Suppose that the assertion of Lemma 24 holds for some $M \in \mathbb{N}$, i.e., there exist matrices $D_1, \dots, D_{2M} \in \mathcal{DU}_d(\mathbb{C})$ such that for any $k, l \in \{1, \dots, d\}$ Eq. (159) holds. We will prove that, upon this assumption, there exist matrices $D_{2M+1}, D_{2M+2} \in \mathcal{DU}_d(\mathbb{C})$ such that for all $k, l \in \{1, \dots, d\}$ we have

$$\left((P_U^T P_U)^{M+1} \right)_{kl} = 0 \quad \Leftrightarrow \quad (D_1 U^\dagger D_2 U \dots D_{2M+1} U^\dagger D_{2M+2} U)_{kl} = 0. \quad (160)$$

According to Corollary 23 (applied for P_U), there exists $D \in \mathcal{DU}_d(\mathbb{C})$ such that, for all $k, l \in \{1, \dots, d\}$, $(P_U^T P_U)_{kl} = 0$ if and only if $(\mathbb{1} U^\dagger D U)_{kl} = 0$. Now, keeping in mind the inductive assumption and the above, set

$$V := D_1 U^\dagger D_2 U \dots D_{2M-1} U^\dagger D_{2M} U \quad \text{and} \quad W := U^\dagger D U, \quad (161)$$

and note that the matrices $R_V = (P_U^T P_U)^M$ and $R_W = P_U^T P_U$ satisfy Eq. (129) for V and W , respectively. Hence, using Lemma 22, we obtain that there exists $\tilde{D} \in \mathcal{DU}_d(\mathbb{C})$ for which the equivalence

$$\left((P_U^T P_U)^M P_U^T P_U \right)_{kl} = (R_V R_W)_{kl} = 0 \quad \Leftrightarrow \quad (V \tilde{D} W)_{kl} = 0 \quad (162)$$

holds for all $k, l \in \{1, \dots, d\}$. This, however, implies Eq. (160) for $D_{2M+1} = \tilde{D}$ and $D_{2M+2} = D$, since

$$V \tilde{D} W = (D_1 U^\dagger \dots D_{2M} U) \tilde{D} (U^\dagger D U). \quad (163)$$

□

G Relations to Markov chains

For the convenience of the reader, we summarise here certain definitions and facts concerning finite Markov chains, to which we refer in Sec. 3.3. In particular, we focus on irreducible and aperiodic Markov chains (for more details see, e.g., Refs. [46, 60]).

Consider a time-homogenous Markov chain $\mathbf{X} = (X_n)_{n \in \mathbb{N}_0}$ with a countable state space Σ (equipped with a countably generated σ -field $\mathcal{B}(\Sigma)$ on Σ), and let

$$T = \{T_{ij} : i, j \in \Sigma\} \quad \text{with} \quad T_{ij} = \mathbb{P}(X_{n+1} = j | X_n = i) \quad \text{for} \quad n \in \mathbb{N}_0 \quad (164)$$

be its transition matrix. The m -th step transition matrices $T(m) = \{T_{ij}(m) : i, j \in \Sigma\}$ are given by

$$T(0) = \mathbb{1} \quad \text{and} \quad T_{ij}(m) = \sum_{k \in \Sigma} T_{ik} T_{kj}(m-1) \quad \text{for} \quad m \in \mathbb{N}, \quad (165)$$

and they describe the probabilities of getting from one state to another (or the same) in exactly m steps.

We say that a state $i \in \Sigma$ is *accessible* from a state $j \in \Sigma$ if and only if there exists some non-negative constant m such that $T_{ij}(m) > 0$. If i and j are accessible from each other, we call them *communicating*. It shall be noted that the communication relation is an equivalence relation. A Markov chain \mathbf{X} is called *irreducible* if and only if its state space constitutes one communication class. In the graph-representation of the chain, for communicating states i and j there are directed paths from i to j and from j to i . As a consequence, a finite Markov chain is irreducible if and only if its graph representation is a strongly connected graph (a directed graph is *strongly connected* if every vertex is reachable from every other vertex). The *period* $d(i)$ of a state $i \in \Sigma$ of a Markov chain \mathbf{X} is given by $d(i) = \text{GCD}\{n \geq 1 : T_{ii}(n) > 0\}$. We call a state i *aperiodic* if $d(i) = 1$. A Markov chain is *aperiodic* if and only if all its states are aperiodic.

The following well-known facts (whose proofs can be found, e.g., in Ref. [60]; cf. Corollaries 3.3.3 and 3.3.4 therein) shall be useful for our purposes.

Proposition 25. *Let \mathbf{X} be an irreducible and aperiodic Markov chain with finite state space and transition matrix T . Then, there exists a finite constant M such that for all $m \geq M$*

$$T_{ij}(m) > 0 \quad \text{for all states} \quad i, j \in \Sigma, \quad (166)$$

meaning that $T(m)$ is a matrix with all non-zero entries, and so any two states are communicating.

Note that the assertion of Proposition 25 might not hold if we abandon the assumption that a Markov chain is aperiodic. Indeed, there exist irreducible Markov chains such that all matrices $T(m)$ have zero entries (and kind of a block structure). An exemplary transition matrix of such a chain is

$$T = \begin{bmatrix} 0 & 0 & 1/2 & 1/2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}. \quad (167)$$

Proposition 26. *If a Markov chain is irreducible, and additionally its directed graph has a vertex with a loop (which is equivalent to requiring that the transition matrix T of this Markov chain has at least one nonzero diagonal element), then it is also aperiodic.*

As a corollary of Propositions 25 and 26 we obtain the following:

Proposition 27. *If a Markov chain has a directed graph which is strongly connected and has at least one vertex with a loop, then it is both irreducible and aperiodic.*

Using Proposition 27, we can construct a simple example illustrating how to directly approach the problem of estimating the value $m \in \mathbb{N}$ describing the number of steps needed to generate a matrix $T(m)$ with all non-zero entries.

Example 28. Let $U \in \mathcal{U}_d(\mathbb{C})$, and let W be its unistochastic matrix, that is, $W = U \circ \bar{U}$, where \circ represents the entry-wise product (also known as Hadamard or Schur product). Consider a finite Markov chain described by a transition matrix $T = W^T W$ and a directed graph \mathcal{D} with vertices $\{v_1, \dots, v_d\}$. If we assume that \mathcal{D} is strongly connected and one of its vertices, say v_{i_0} , has a loop, then, according to Proposition 27, we obtain the following:

$$\exists M \in \mathbb{N} \quad \forall i, j \in \{1, \dots, d\} \quad \forall m \geq M \quad T_{ij}(m) > 0, \quad (168)$$

where $T(m)$ denotes here a m -th step transition matrix, defined in Eq. (165). Willing to find a constant M for which the above condition holds, we may proceed as follows:

1. Since the graph \mathcal{D} is strongly connected, for any $i, j \in \{1, \dots, d\}$, there exist

$$\alpha_i := \min \{ \alpha \in \mathbb{N} : T_{i i_0}(\alpha) > 0 \} \quad \text{and} \quad \beta_j := \min \{ \beta \in \mathbb{N} : T_{i_0 j}(\beta) > 0 \}, \quad (169)$$

which are finite.

2. Note that for all $i, j \in \{1, \dots, d\}$ and any $m \geq \alpha_i + \beta_j$, we have $T_{ij}(m) > 0$. Indeed, letting $m = \alpha_i + \beta_j + k$ with some $k \in \mathbb{N}$, and recalling that v_{i_0} has a loop, we get $T_{ij}(m) \geq T_{i i_0}(\alpha_i) (T_{i_0 i_0}(1))^k T_{i_0 j}(\beta_j) > 0$.

3. Define $M := 2 \max_{i \in \{1, \dots, d\}} \alpha_i$. Since the matrix $T = W^T W$ is symmetric, we have

$$M = \max_{i \in \{1, \dots, d\}} \alpha_i + \max_{j \in \{1, \dots, d\}} \beta_j. \quad (170)$$

Hence, according to Step 2, we know that for all $i, j \in \{1, \dots, d\}$ and any $m \geq M$

$$T_{ij}(m) \geq T_{i i_0}(\alpha_i) (T_{i_0 i_0}(1))^{m - \alpha_i - \beta_j} T_{i_0 j}(\beta_j) > 0. \quad (171)$$

H Proof of Proposition 12

In order to prove Proposition 12 (identifying the lower bound on the number of coherence engine's strokes needed to produce all operations), let us first formulate and prove two auxiliary lemmas.

Lemma 29. *Let $U \in \mathcal{U}_d(\mathbb{C})$, and let $X_U = (x_{ij})_{i,j=1}^d$ be such that*

$$x_{ij} = |u_{ij}| \quad \text{for any } i, j \in \{1, \dots, d\}. \quad (172)$$

Then, for any $M \in \mathbb{N}$, we have

$$\max_{D_1, \dots, D_{2M} \in \mathcal{D}\mathcal{U}_d(\mathbb{C})} \left| \langle a | D_{2M} U^\dagger D_{2M-1} U \dots D_2 U^\dagger D_1 U | b \rangle \right| \leq \langle a | (X_U^T X_U)^M | b \rangle \quad \text{for all } a, b \in \{1, \dots, d\}. \quad (173)$$

Proof. First of all, note that for any $a, b \in \{1, \dots, d\}$ we have

$$\max_{D_1, D_2 \in \mathcal{D}\mathcal{U}_d(\mathbb{C})} \left| \langle a | D_2 U^\dagger D_1 U | b \rangle \right| = \max_{\theta_1, \dots, \theta_d, \gamma_1, \dots, \gamma_d \in \mathbb{R}} \left| \sum_{j=1}^d \bar{u}_{ja} e^{i\theta_j} u_{jb} e^{i\gamma_j} \right| \leq \sum_{j=1}^d |\bar{u}_{ja}| |u_{jb}| = \langle a | (X_U^T X_U) | b \rangle, \quad (174)$$

where $X_U = (x_{ij})_{i,j=1}^d$ is given by Eq. (172).

The proof then proceeds by induction on $M \in \mathbb{N}$. If for any $M \in \mathbb{N}$ and all $a, b \in \{1, \dots, d\}$

$$\max_{D_1, \dots, D_{2M} \in \mathcal{D}\mathcal{U}_d(\mathbb{C})} \left| \langle a | D_{2M} U^\dagger D_{2M-1} U \dots D_2 U^\dagger D_1 U | b \rangle \right| \leq \langle a | (X_U^T X_U)^M | b \rangle, \quad (175)$$

then also

$$\begin{aligned} & \max_{D_1, \dots, D_{2M+2} \in \mathcal{D}\mathcal{U}_d(\mathbb{C})} \left| \langle a | D_{2M+2} U^\dagger D_{2M+1} U \dots D_1 U | b \rangle \right| \\ &= \max_{D_1, \dots, D_{2M+2} \in \mathcal{D}\mathcal{U}_d(\mathbb{C})} \left| \sum_{k=1}^d \langle a | D_{2M+2} U^\dagger D_{2M+1} U | k \rangle \langle k | D_{2M} U^\dagger \dots D_1 U | b \rangle \right| \\ &\leq \sum_{k=1}^d \left(\max_{D_1, D_2 \in \mathcal{D}\mathcal{U}_d(\mathbb{C})} \left| \langle a | D_2 U^\dagger D_1 U | k \rangle \right| \right) \left(\max_{D_1, \dots, D_{2M} \in \mathcal{D}\mathcal{U}_d(\mathbb{C})} \left| \langle k | D_{2M} U^\dagger \dots D_1 U | b \rangle \right| \right) \\ &\leq \sum_{k=1}^d \langle a | (X_U^T X_U) | k \rangle \langle k | (X_U^T X_U)^M | b \rangle = \langle a | (X_U^T X_U)^{M+1} | b \rangle. \end{aligned} \quad (176)$$

□

Imagine that $U \in \mathcal{U}_d(\mathbb{C})$, appearing in the definition of \mathcal{F}_B , is *close to* a diagonal matrix (meaning that the modulus of non-diagonal elements of U are *small*). Our intuition then tells us that Alice and Bob have to communicate many times before they manage to generate an arbitrary unitary matrix, and this is reflected in the following lemma.

Lemma 30. Let $d \in \mathbb{N} \setminus \{1\}$, and let $V = (v_{ij})_{i,j=1}^d, W = (w_{ij})_{i,j=1}^d \in \mathcal{U}_d(\mathbb{C})$ be such that for all $i, j \in \{1, \dots, d\}$, $i \neq j$, we have

$$|v_{ij}| \leq v \text{ for some } v \in \mathbb{R}_+ \text{ and } |w_{ij}| \leq w \text{ for some } w \in \mathbb{R}_+. \quad (177)$$

Then

$$\max_{a,b \in \{1, \dots, d\}: a \neq b} \max_{D \in \mathcal{DU}_d(\mathbb{C})} |\langle a | VDW | b \rangle| \leq (d-2)vw + v + w. \quad (178)$$

Proof. We have

$$\begin{aligned} \max_{a,b \in \{1, \dots, d\}: a \neq b} \max_{D \in \mathcal{DU}_d(\mathbb{C})} |\langle a | VDW | b \rangle| &= \max_{a,b \in \{1, \dots, d\}: a \neq b} \max_{\theta_1, \dots, \theta_d \in \mathbb{R}} \left| \sum_{j=1}^d v_{aj} e^{i\theta_j} w_{jb} \right| \\ &\leq \max_{ab \in \{1, \dots, d\}: a \neq b} \sum_{j=1}^d |v_{aj}| |w_{jb}| \\ &= \max_{a,b \in \{1, \dots, d\}: a \neq b} \left(\sum_{j \in \{1, \dots, d\} \setminus \{a,b\}} |v_{aj}| |w_{jb}| + |v_{aa}| |w_{ab}| + |v_{ab}| |w_{bb}| \right) \\ &\leq (d-2)vw + v + w. \end{aligned} \quad (179)$$

□

We are now ready to give the proof of Proposition 12.

Proof of Proposition 12. For any $M \in \mathbb{N}$ and any $U \in \mathcal{U}_d(\mathbb{C})$, let us introduce matrices

$$V_U^{(D_1, \dots, D_{2M})} = D_{2M} U^\dagger D_{2M-1} U \dots D_2 U^\dagger D_1 U \quad (180)$$

$$v_U^{(D_1, \dots, D_{2M})} := \max_{i,j \in \{1, \dots, d\}, i \neq j} \left| \langle i | V_U^{(D_1, \dots, D_{2M})} | j \rangle \right|. \quad (181)$$

For all $M \in \mathbb{N} \setminus \{1\}$, we then have

$$\begin{aligned} &\max_{a,b \in \{1, \dots, d\}: a \neq b} \max_{D_1, \dots, D_{2M} \in \mathcal{DU}_d(\mathbb{C})} |\langle a | D_{2M} U^\dagger D_{2M-1} U \dots D_2 U^\dagger D_1 U | b \rangle| \\ &= \max_{a,b \in \{1, \dots, d\}: a \neq b} \max_{D_1, \dots, D_{2M} \in \mathcal{DU}_d(\mathbb{C})} \max_{D \in \mathcal{DU}_d(\mathbb{C})} \left| \langle a | V_U^{(D_3, \dots, D_{2M})} D V_U^{(D_1, D_2)} | b \rangle \right|, \end{aligned} \quad (182)$$

which, due to Lemma 30 applied to $V = V_U^{(D_3, \dots, D_{2M})}$ and $W = V_U^{(D_1, D_2)}$, entails the following:

$$\begin{aligned} &\max_{a,b \in \{1, \dots, d\}: a \neq b} \max_{D_1, \dots, D_{2M} \in \mathcal{DU}_d(\mathbb{C})} |\langle a | D_{2M} U^\dagger D_{2M-1} U \dots D_2 U^\dagger D_1 U | b \rangle| \\ &\leq \max_{D_1, \dots, D_{2M} \in \mathcal{DU}_d(\mathbb{C})} \left((d-2)v_U^{(D_3, \dots, D_{2M})} v_U^{(D_1, D_2)} + v_U^{(D_3, \dots, D_{2M})} + v_U^{(D_1, D_2)} \right). \end{aligned} \quad (183)$$

Further, for any $M \in \mathbb{N}$ and any $U \in \mathcal{U}_d(\mathbb{C})$ define

$$v_{U,M} := \max_{D_1, \dots, D_{2M} \in \mathcal{DU}_d(\mathbb{C})} v_U^{(D_1, \dots, D_{2M})}, \quad (184)$$

and observe that $v_{U,1} = c_U$ with c_U given by Eq. (58). Moreover, for any $M \in \mathbb{N} \setminus \{1, 2\}$ and any $U \in \mathcal{U}_d(\mathbb{C})$, we get

$$v_{U,M} \leq v_{U,M-1} ((d-2)c_U + 1) + c_U, \quad (185)$$

and so

$$v_{U,M} \leq \frac{((d-2)c_U + 1)^M - 1}{d-2} \text{ for any } d \in \mathbb{N} \setminus \{1, 2\}. \quad (186)$$

Now, observe that whenever the right hand side of Eq. (186) is smaller than 1, then obviously also

$$\max_{a,b \in \{1, \dots, d\}: a \neq b} \max_{D_1, \dots, D_{2M} \in \mathcal{DU}_d(\mathbb{C})} |\langle a | D_{2M} U^\dagger D_{2M-1} U \dots D_2 U^\dagger D_1 U | b \rangle| < 1, \quad (187)$$

which, in turn, implies that Alice and Bob are not able to generate any permutation matrix within $N = 2M$ steps (i.e., M Alice's strokes and M Bob's strokes). As a consequence, we may claim that, in order to generate an arbitrary unitary matrix of order d , both Alice and Bob need to perform at least M_{\min} operations, with M_{\min} given as the smallest natural number satisfying

$$\frac{((d-2)c_U + 1)^{M_{\min}} - 1}{d-2} \geq 1 \quad \text{for } d \in \mathbb{N} \setminus \{1, 2\}. \quad (188)$$

Finally, we get

$$M_{\min} \geq \frac{\log(d-1)}{\log((d-2)c_U + 1)} \quad \text{for } d \in \mathbb{N} \setminus \{1, 2\}. \quad (189)$$

Since the minimal number of strokes is given by $N = 2M_{\min}$, this concludes the proof. \square