The Hadamard gate cannot be replaced by a resource state in universal quantum computation

Benjamin D.M. Jones[1,2,3], Noah Linden[2], and Paul Skrzypczyk[1,4]

[1]H. H. Wills Physics Laboratory, University of Bristol, Bristol, BS8 1TL, UK.
[2]School of Mathematics, University of Bristol, Fry Building, Woodland Road, Bristol, BS8 1UG, UK.
[3]Quantum Engineering Centre for Doctoral Training, University of Bristol, Bristol, BS8 1FD UK.
[4]CIFAR Azrieli Global Scholars Program, CIFAR, Toronto Canada.

We consider models of quantum computation that involve operations performed on some fixed resourceful quantum state. Examples that fit this paradigm include magic state injection and measurement-based approaches. We introduce a framework that incorporates both of these cases and focus on the role of coherence (or superposition) in this context, as exemplified through the Hadamard gate. We prove that given access to incoherent unitaries (those that are unable to generate superposition from computational basis states, e.g. CNOT, diagonal gates), classical control, computational basis measurements, and any resourceful ancillary state (of arbitrary dimension), it is not possible to implement any coherent unitary (e.g. Hadamard) exactly with non-zero probability. We also consider the approximate case by providing lower bounds for the induced trace distance between the above operations and n Hadamard gates. To demonstrate the stability of this result, this is then extended to a similar no-go result for the case of using k Hadamard gates to exactly implement $n > k$ Hadamard gates.

1 Introduction

The more peculiar aspects of quantum mechanics, such as entanglement [1] and incompatibility of measurements [2], continue to fascinate researchers and motivate a deeper understanding of this cornerstone of physics. It is also remarkable that quantum theory appears to provide a computational speed-up for certain problems over what is possible with classical physics [3]. The quest to fully understand and quantify which aspects of quantum theory are needed for useful quantum algorithms is a pressing and exciting current area of research.

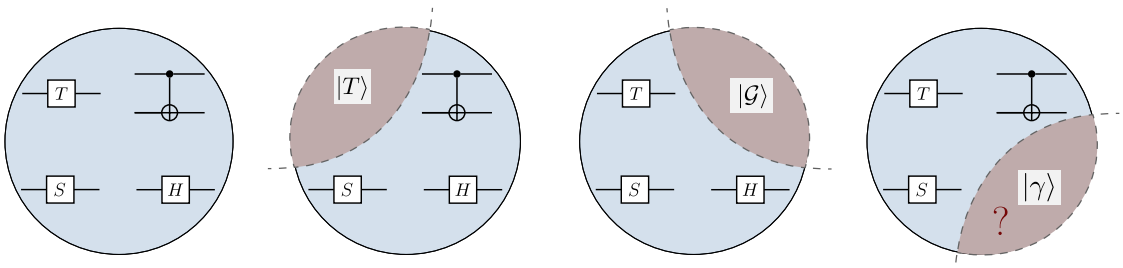
There are various ways of performing universal quantum computation: examples include the circuit model [3], measurement based approaches [4], magic state injection [5], quantum annealing [6], and continuous variable models [7]. An interesting perspective is to consider approaches involving "free" operations (i.e. easy to perform in some sense) acting on a resourceful state that is prepared independently of the computation. By focusing on this supplementary state, one could hope to gain insight into which components of quantum mechanics are responsible for the computational classical-quantum boundary.

The most widely studied universal gate set is the Clifford + T gate set; recall that the Clifford group is generated by the single qubit Hadamard (H) and phase (S) gates and the two-qubit controlled-NOT (CNOT) gate. The gate set of CNOT, T and Hadamard is also universal, and can be thought of as respectively supplying the resources of entanglement, magic (or non-stabiliserness) and coherence (or superposition). In magic state injection (MSI), one implements a T gate by performing adaptive Clifford operations on the input state and an ancillary state $|T\rangle := T|+\rangle$. Here the operations performed are free with respect to the resource of magic, and all of the magic required is contained in the pool of $|T\rangle$ states. This approach is motivated by error correction and fault tolerance schemes [5].

In contrast, measurement based quantum computation (MBQC) proceeds by adaptively performing single qubit measurements on an entangled resource state, such as a cluster state [8]. In this scenario, the resource of entanglement is present only in the state, and again the operations are free with respect to this resource. The ability to perform computational basis measurements (i.e. measure in the Z basis) and apply H, S and T gates also implies ability to measure in the X, Y and $TXT^\dagger$ bases, which is sufficient for universality [9].

From these examples, a natural question arises of where we can put the 'cut' between operations and states whilst retaining the ability to perform universal quantum computation – see Fig. 1. For example when considering the Clifford + T gate set, can one replace the Hadamard with access to some resourceful state, and still maintain universality? We provide no-go results in this direction.

In more generality one can consider whether this cut is possible for an arbitrary quantum resource theory [10]. As Hadamard is the only gate within Clifford + T capable of generating superpositions from computational basis states, the relevant resource theory here is that of coherence [11]. Our findings show that some coherence is required in the *operations* to achieve universality, providing a stark contrast with the resource theories of magic and entanglement.



(a) Universal gate set. (b) Magic state injection. (c) MBQC. (d) This work.

Figure 1: (a) A universal set of quantum gates: Hadamard (H), Phase (S), T, and controlled-NOT. (b) Each T gate can be implemented using Clifford operations and a $|T\rangle$ state. (c) If CNOT is removed from this gate set one can still perform universal quantum computation using an appropriately entangled resource state $|\mathcal{G}\rangle$, such as a cluster state. (d) We ask whether one can similarly replace the Hadamard gate with some resourceful state $|\gamma\rangle$ and still achieve universality – we show that this is not possible. In all cases we allow computational basis measurements and classical control. Also note that the case of removing S is trivial as $T^2 = S$.

1.1 Summary of Results

We provide no-go results on the possibility of performing universal quantum computation using operations unable to generate superpositions, even given access to an arbitrary state. A unitary that maps at least one computational basis state to a superposition of two or more basis states is termed *coherent*, otherwise it is *incoherent*. Our findings can be informally summarised as:

Incoherent unitaries + classical control + computational basis measurements + arbitrary ancillas

cannot implement coherent unitaries (e.g. Hadamard).

Main Conceptual Contributions

- We provide a unified framework from which to consider models of quantum computation that involve free operations acting on some fixed resourceful state.
- We give evidence that any model of quantum computation must involve the resource of coherence in the operations (exemplified by the Hadamard gate). That is, coherence cannot be siphoned off to some supplementary state, unlike in the cases of magic in magic state injection or entanglement in measurement based quantum computation.

Main Technical Contributions

Recall that the dephasing map Δ sets all off-diagonal terms of the density matrix in the computational basis to zero, and the trace distance is defined as $D(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_1$.

Lemma 15 (informal). If a channel $\mathcal{E}$ commutes with the dephasing map Δ, then for any state $|\gamma\rangle$ the induced channel $\rho \mapsto \mathcal{E}(\rho \otimes |\gamma\rangle\langle\gamma|)$ cannot implement any coherent unitary.

This generalises an observation made in an erratum to [12] that shows a similar result for qubits.

Our second main technical result is a robust extension of this to the approximate case, when specifically considering n Hadamard gates, of particular relevance in quantum computation.

Lemma 19 (informal). Let $\mathcal{E}$ be a channel that commutes with the dephasing map Δ, let H denote the Hadamard gate and D denote trace distance. Then for any state $|\gamma\rangle$ we have

$$\max_{\rho} \; D\Big(\mathcal{E}(\rho\otimes|\gamma\rangle\langle\gamma|)\;,\; H^{\otimes n}\rho H^{\otimes n}\Big) \geq 1-\frac{1}{2^n}.$$

Thirdly, we show that k Hadamards, incoherent unitaries, classical control and an arbitrary ancilla cannot be used to implement $n > k$ Hadamards exactly and deterministically.

Lemma 22 (informal). Let $U = U_k V_k \dots U_1 V_1 U_0$ be a product of unitaries, comprised of k Hadamards V_i and incoherent U_i. Then for any state $|\gamma\rangle$ we have

$$\mathrm{Tr}_2\left(U\rho\otimes|\gamma\rangle\langle\gamma|\,U^\dagger\right) = H^{\otimes n}\rho H^{\otimes n} \qquad \forall\rho, \qquad\qquad \Longrightarrow \qquad n\leq k.$$

Whilst these results stand independently in the study of coherence, we interpret them in quantum computation by showing that certain operationally motivated channels satisfy the conditions.

Supporting results include showing that quantum-controlled incoherent unitaries are incoherent (Lemma 9), placing bounds on the coherence rank of a state after k Hadamards have been applied

(Lemma 11), and proving that if the marginal of a unitary channel acting on an input state and fixed state is unitary, then the other marginal must be independent of the input state (Lemma 21).

We now provide further background and definitions, before more formally introducing our framework in the next section.

1.2 Background

The seminal result of the Gottesman-Knill theorem [3, 13–15] states that any quantum computation consisting of Clifford operations (comprised of CNOT, Hadamard and phase gates), can be simulated efficiently on a classical computer. It is known that the T gate elevates this set to universality, and the Clifford + T gate set is perhaps the most widely considered universal set of gates. Motivated by error-correction and fault-tolerance considerations [5], in place of directly applying a T gate, one can perform adaptive Clifford operations on an arbitrary input state and a so-called *magic state*, to implement the T gate deterministically. This is often referred to as a *gadget*, where one replaces all uses of a given gate with this subroutine, consuming a resourceful state in the process. See Example 1 below for further detail here.

Another example of a gadget-based approach can be found in recent work on matchgate circuits [16, 17]. Matchgates are a family of two-qubit gates, inspired by fermionic systems, that can be written as the direct sum of two single qubit gates with the same determinant, acting respectively in the even and odd parity subspaces [18]. It is known that circuits composed of matchgates acting only on nearest-neighbour qubits are classically simulable, however any family of quantum circuits can be simulated efficiently with circuits composed of matchgates acting on next-nearest-neighbour qubits [18, 19]. Hence nearest-neighbour matchgates can be augmented to universality using SWAP gates, analogously to Clifford circuits and T gates. The work of [16, 17] highlights this connection (see Figure 1 in [17]), and shows the existence of a SWAP state, which can be consumed under adaptive nearest-neighbour matchgates to implement the SWAP gate. This provides a parallel gadget based approach to the Clifford + T case, in which resourceful states are consumed to implement resourceful gates, enabling universality.

Measurement based-quantum computing (MBQC) [4] generally refers to any model of quantum computation in which the primary allowed operations are measurements. The foremost example of this is the so-called *one-way* MBQC model [20, 21], in which adaptive single qubit measurements are performed on some fixed resource state. This is usually taken to be a cluster state, a state in which qubits are laid out in a rectangular grid, initialised to $|+\rangle$ states, and controlled-Z gates are applied between neighbouring qubits. Another model is teleportation-based quantum computation, which proceeds by using Bell measurements to teleport gates [4, 22].

The above examples are all connected: they all relate to performing some perceived free operations on an apparently resourceful fixed state. In the magic state injection model, one may consider Clifford operations as free, and the resource state contains the *magic* needed for the computation. In the standard MBQC framework, local measurements are considered free (one can generalise this to consider arbitrary *local operations and classical communication* (LOCC) operations [8]), and the resource state contains all the *entanglement* needed for the computation.

The framework of *quantum resource theories* [10] aims to identify components of quantum theory that are non-classical in some sense, by defining so called *free* sets of states, and allowed channels and measurements. One can then define resource quantifiers, such as the distance a given object is away from the free set, or finding a minimal convex combination of an object and free object. This paradigm has roots motivated by thermodynamics, and the archetypal quantum resource theory is that of entanglement. Here the free states and allowed channels can respectively taken to be separable states and LOCC. The resource theory of coherence has also gathered a lot of attention in recent years [11], and is highly relevant to this work. In this context, the set of free states are those which are diagonal in some fixed basis (termed *incoherent*), however there are multiple approaches to defining the allowed class of operations, which has lead to fruitful and nuanced discussion [23] – see Appendix A for further more on this.

When considering the computational power of a set of quantum operations, there are multiple approaches one can take. One can consider *classical simulability*, namely if one can efficiently perform the same calculation on a classical computer. Here there are several subtleties: how to precisely quantify 'efficiently', and the exact simulation task considered; for example the ability

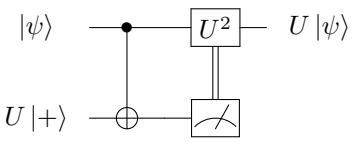
to sample from measuring the final state in the computational basis (weak simulation), or the ability to compute or bound a given output probability of the final state (strong simulation) - see e.g. [24–26]. Another angle is to consider *universality*, that is, the ability of the operations to implement any unitary or prepare any quantum state, with extensions including notions of approximate and probabilistic universality [8, 27]. These ideas are not independent: for quantum computers to be strictly more powerful than classical computers, one would expect that efficient classical simulation of a universal quantum device is not possible, however the inability to classically simulate a quantum process efficiently does in general not imply universality (for example, consider approaches to so-called 'quantum computational supremacy' [28]).

In this work, we focus on the notion of universality. We consider the resource of coherence in gadget-based approaches to quantum computation through studying the role of the Hadamard gate. Specifically, we ask whether given access to incoherent unitaries (i.e. unitaries unable to generate superpositions when acting on computational basis states), computational basis measurements, and classical control (e.g. applying unitaries conditioned on previous measurement outcomes) if there exists a quantum state (which can be completely arbitrary) such that one can implement Hadamard gates, either exactly or approximately. To phrase this in a slightly contrived fashion and give broader motivation, suppose some distant civilisation are capable of preparing and transporting some complicated resourceful state. What are the minimal operations that are necessary for the recipient in order for them to be able to perform universal quantum computation? In this work, we will provide evidence of where this resource 'cut' lies: the ability to perform coherent operations (or incompatible measurements) are all that is necessary, everything else can be moved into the resource state. Complementary results also show that the ability to perform the Hadamard gate is sufficient in this context [9], hence we draw closer to a complete answer to this question. Along the way, we show several results that may be of broader interest in quantum information, computation, and resource theories.

We will now introduce some examples that explain the above areas in more detail, providing concrete motivation and serving as a reference for the rest of the document.

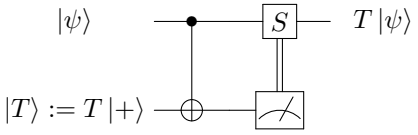
Example 1. Consider the gate set of Clifford + T, comprised of gates from $\{CNOT, H, S, T\}$, where H is the Hadamard gate and S is the phase gate. As discussed above, the T gates may be implemented by performing adaptive Clifford operations on supplementary T states. A natural question is: where else could we put the 'cut' between gates and states? Could it be possible to do universal quantum computation with only adaptive CNOT gates acting on some supplementary resourceful state?

To provide a more concrete basis for this question, consider the following circuit, valid for all diagonal gates $U = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$ and qubit input $|\psi\rangle \in \mathbb{C}^2$.



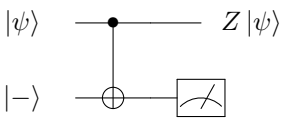
(1)

Magic state injection is the special case of this when $U = T$:



(2)

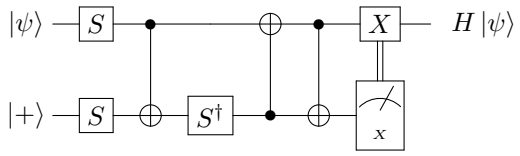
Observe that for $U = Z$, this becomes



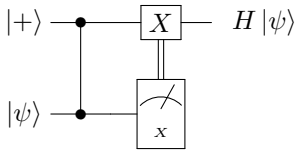
(3)

as $Z^2 = \mathbb{1}$. Hence given access to CNOTs and $|-\rangle$ states we can implement the Z gate deterministically. We can apply this as a subroutine, enabling us to implement the phase gate S using two CNOTs and the state $|-\rangle \left(\frac{|0\rangle+i|1\rangle}{\sqrt{2}}\right)$. Iterating in this way, we can reach any gate of the form $U_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$ for $k \in \mathbb{N}$ (note that $U_2 = T$). Hence for Clifford + T, we can replace the S and T gates with gadgets, and perform universal quantum computation with ability to only perform CNOTs and Hadamard on some supplementary state. However it is not clear how to restrict this gate set further when only computational basis measurements are permitted.

Example 2. So-called Hadamard gadgets are known to exist [29–31], where they play roles relating to compilation and simulation of quantum circuits. For example, the following circuits appear in [29] and [30] respectively:



(4)



(5)

However, they crucially rely on X basis measurements, that is, measurements in the coherent basis $\{|+\rangle, |-\rangle\}$. In this work, we will show that such gadgets cannot exist if one restricts to computational basis measurements.

Example 3. In [9] it is shown that measurement-based quantum computing is possible with adaptive X and Z measurements alone. This can alternatively can be viewed as the ability to only perform the Hadamard gate and measure in the computational basis. It is clear that the resource state here cannot be a graph state, as graph states are stabiliser states, and as Hadamard is a Clifford gate we could simulate the whole computation using the Gottesman-Knill theorem. Indeed the state considered in [9] is a hypergraph state [32], formed by initialising all qubits to $|+\rangle$ and performing multiply controlled Z gates for each hyperedge. In particular, one can see that as CCZ is not a Clifford operation, hypergraph states will not be stabiliser states in general.

This example shows that given the ability to only perform adaptive Hadamard gates and computational basis measurements, there exists a resourceful ancillary state such that universal quantum computation is possible.

Example 4. *Incoherent operations* (IO) are defined as channels admitting a Kraus decomposition $\mathcal{E}(\rho) = \sum_\alpha K_\alpha \rho K_\alpha^\dagger$ such that $K_\alpha \rho K_\alpha^\dagger$ is an incoherent state for each α and each incoherent state ρ. It is known that these channels supplemented with a maximally coherent state $|\Psi_d\rangle = d^{-\frac{1}{2}} \sum_{k=0}^{d-1} |k\rangle \in \mathbb{C}^d$ are able to implement any quantum channel [12].

It was originally claimed in the same paper that a similar result, namely the ability to implement any unitary given access to $|\Psi_d\rangle$, held for *strictly incoherent operations* (SIO), which are IO with the additional property that $K_\alpha^\dagger \rho K_\alpha$ is an incoherent state for each α and

each incoherent state ρ. However, it was later shown in an erratum to [12] that their proof was invalid as the operations used were not SIO. In this erratum, the authors gave a simple argument that if a qubit channel commutes with the dephasing map (which all SIO do), then even supplemented with an arbitrary ancilla one cannot implement any coherent unitary.

This example highlights an interesting distinction: IO can 'unlock' the resource in a supplementary state, whereas the slightly weaker class of SIO are unable to access any of this state resource. In this work we show that a class of operations motivated by quantum computation gadgets are also unable to harness the power in a supplementary coherent state. See Appendix A for further background on the resource theory of coherence, and how our work relates to this topic.

Example 5. In [33], it is shown that CNOT and any single qubit gate whose square is basis changing (i.e. coherent) is universal for quantum computation. The same result is also shown for the Toffoli gate and any single qubit basis changing gate. A simpler proof for the case of Toffoli + Hadamard was presented in [34]. These results are conceptually fascinating as the Toffoli gate is universal for classical computing, so by including the 'quintessentially quantum' Hadamard gate one elevates classical universality to quantum universality. As the above gates are real, one uses an additional ancilla to simulate complex numbers.

The above examples motivate the following questions:

(1) Is it possible to provide a gadget for the Hadamard gate using only incoherent unitaries, computational basis measurements, and an ancilla?

(2) Is universal quantum computation possible with only incoherent unitaries acting on some resourceful state? Or does any universal model require some coherence (e.g. Hadamard) in the operations?

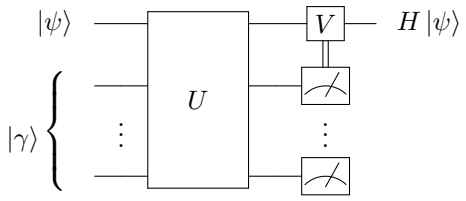
(3) Where can we put the 'cut' between states and operations for quantum computation in general?

(4) If coherence must be present in the operations, how much coherence is necessary and sufficient for universality?

(5) Is there a connection between the role of coherence in gadget-based approaches, and the role of measurements in MBQC approaches?

The purpose of this paper is to initiate this line of research, and make progress in answering some of these questions. We provide answers in the negative to points (1) and (2), whilst discussing (3) - (5) towards the end of the document and motivating them for future research.

In particular, we rule out the existence of circuits of the following general form, for U and V incoherent unitaries (e.g. products of CNOTs and T gates):

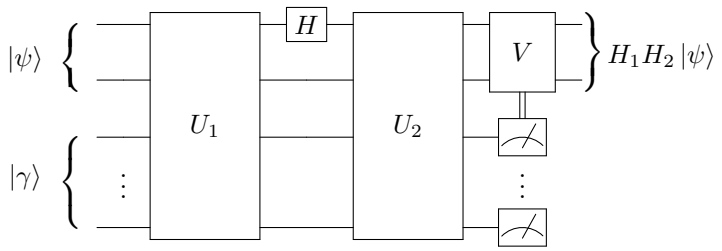


(6)

Note that we know that the above diagram is possible with $|\gamma\rangle = |+\rangle$ if we instead allow X measurements, as shown in Example 2.

At this stage, one might worry that the ancillary state $|\gamma\rangle$ cannot be useful only as the set of unitaries considered are completely resourceless. A priori, it is possible that the use of a single Hadamard gate could allow incoherent unitaries to unlock all the power from the ancillary state to implement a more coherent gate, for example, two Hadamards. Hence we also consider the natural extension of whether incoherent unitaries, computational basis measurements, an ancilla, and k

Hadamards can simulate $n > k$ Hadamards. In the case of $k = 1$ and $n = 2$, the corresponding diagram could be of the form:



(7)

where U_i and V are incoherent unitaries and H_i denotes a Hadamard gate on the i-th qubit. We are also able to rule out this case in this work. This demonstrates the importance of having the ability to generate large amounts of coherence in any model of quantum computation, directly contrasting with the magic state injection case in which all the 'non-stabiliserness' can be placed in supplementary ancillas.

The document is organised as follows. After fixing notation, we motivate a general framework for quantum computation involving some free unitaries acting on a resourceful state. We then apply this to coherence in our results section, focusing on the case of incoherent resources attempting to use a supplementary state to implement $H^{\otimes n}$ (we refer to this as the case $0 \mapsto n$), as well as the case of incoherent resources and the use of k Hadamards to implement $H^{\otimes n}$ (the case $k \mapsto n$). We consider the cases of exact, deterministic, approximate and probabilistic implementation. We conclude with a discussion of the key concepts our work relates to, and provide several novel research problems as outlook. Appendix A provides further background to resource theories and coherence.

1.3 Notation and Definitions

Let $\mathcal{L}(\mathcal{H})$ denote the set of linear maps on a Hilbert space $\mathcal{H}$. In this work all Hilbert spaces will be finite dimensional, $\mathcal{H} \cong \mathbb{C}^d$, and in particular we will focus on qubit systems. Quantum states are positive semi-definite elements of $\mathcal{L}(\mathcal{H})$ with unit trace: we denote this set by $S(\mathcal{H})$. Quantum channels are completely positive trace-preserving (CPTP) maps $\mathcal{E} : \mathcal{L}(\mathcal{H}_1) \to \mathcal{L}(\mathcal{H}_2)$. Similarly, quantum subchannels are completely positive trace non-increasing maps from $\mathcal{L}(\mathcal{H}_1)$ to $\mathcal{L}(\mathcal{H}_2)$. We may abuse notation by referring to a unitary channel $\mathcal{U}(\cdot) = U(\cdot)U^\dagger$ simply as U, and by writing $|\psi^n\rangle$ in place of $|\psi\rangle^{\otimes n}$.

The Pauli matrices are

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{8}$$

and the n-qubit Pauli group $\mathcal{P}_n$ is generated by tensor products of Pauli matrices, elements being referred to simply as 'Paulis'. The Clifford group is the normaliser of $\mathcal{P}_n$ and is generated by (tensor products of) the following gates

$$\begin{array}{lll} \underline{\text{Hadamard}} & \underline{\text{Phase}} & \underline{\text{Controlled-NOT}} \\ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, & S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, & CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \end{array} \tag{9}$$

The T gate and the T state are respectively defined as

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}, \qquad |T\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{\frac{i\pi}{4}} |1\rangle \right). \tag{10}$$

The trace distance on quantum states is defined as

$$D(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_1, \tag{11}$$

where $\|M\|_1 = \mathrm{Tr}(\sqrt{M^\dagger M})$. The trace distance has the following properties for all states ρ, σ: (i) positivity: $D(\rho,\sigma) \geq 0$ with equality $\iff$ $\rho = \sigma$ (ii) symmetry: $D(\rho,\sigma) = D(\sigma,\rho)$ (iii) triangle inequality: $D(\rho,\sigma) \leq D(\rho,\omega) + D(\omega,\sigma)$, (iv) contractivity: $D(\Lambda(\rho),\Lambda(\sigma)) \leq D(\rho,\sigma)$ for all quantum channels Λ.

The induced trace distance on channels results from maximising over possible input states:

$$\mathcal{D}(\mathcal{E},\mathcal{V}) := \max_\rho \; D\Big(\mathcal{E}(\rho),\mathcal{V}(\rho)\Big). \tag{12}$$

We say that a channel $\mathcal{E}$ *ϵ-approximates* a channel $\mathcal{V}$ if they they are at most ϵ close in this induced trace norm.

In the resource theory of coherence, one fixes a basis $\{|x\rangle\}$ of $\mathbb{C}^d$ (which we may refer to as the computational basis). A state is then *incoherent* if it can be written as

$$\rho = \sum_x p_x \, |x\rangle\langle x| \tag{13}$$

in this basis. We denote the set of incoherent states (for an implied fixed dimension) by $\mathcal{I}$ – note that it is convex and compact. A unitary U is *incoherent* relative to the basis $\{|x\rangle\}_{x=1}^d$ if it can be written as

$$U = \sum_{x=1}^{d} e^{i\theta_x} \, |\pi(x)\rangle\langle x| \tag{14}$$

for d real numbers θ_x and some permutation π on d elements. In particular, incoherent unitaries map a computational basis state to another computational basis state, possibly multiplied by some phase. They are precisely the maximal set of unitaries mapping $\mathcal{I}$ to itself. Examples of incoherent unitaries include the Pauli operators, the phase and T gates, CNOT, SWAP, and the Toffoli gate. Examples of unitaries that are coherent (i.e. not incoherent, able to generate coherence) include the Hadamard gate, the Fourier transform, and X rotations $e^{i\theta X}$ for $\theta \notin \{n\pi \; ; \; n \in \mathbb{Z}\}$. Coherent unitaries may also be called *basis changing* [33].

For a fixed basis $\{|x\rangle\}$, the *dephasing map* is defined as

$$\Delta(\rho) := \sum_x |x\rangle\langle x| \, \rho \, |x\rangle\langle x| \, . \tag{15}$$

This has the effect of removing the off-diagonal elements on a density operator, hence $\Delta(\rho) \in \mathcal{I}$ for all states ρ. We may use the symbol Δ multiple times in an expression even though they may act on quantum states of different dimensions, which can be inferred from context. We use the term *incoherent resources* informally to refer to operations arising from incoherent unitaries, classical control, computational basis measurements and preparation, and partial traces. Throughout we will use $|\gamma\rangle$ as notation for a pure ancilla, and τ as notation for a mixed state ancilla.

See Section 3.1 for more preliminaries, and Appendix A for further background on resource theories, in particular that of coherence.

2 Framework

In this section we will consider a general paradigm for quantum computation using some additional ancillary state as a resource. Consider the following:

Free operations:		
• Preparation of computational basis states. • Measurement in the computational basis. • Classical control and adaptivity. • Some set of unitaries $\mathcal{U}$.	+	an additional resourceful state $\|\gamma\rangle$.

(16)

Here 'classical control and adaptivity' refers to the ability to perform a unitary from $\mathcal{U}$ or measurement classically conditioned on the outcomes of previous measurements.

2.1 Examples

Many approaches to quantum computation fall into the above framework – see Table 1 for a list of examples. In the standard circuit model, we take the set of unitaries $\mathcal{U}$ to be a universal gate set, and do not consider a supplementary state $|\gamma\rangle$ (i.e. it is redundant here). In the magic state injection model, the set $\mathcal{U}$ is taken as Clifford gates, and the supplementary state $|\gamma\rangle$ can be taken as a tensor product of T states $|\gamma\rangle = |T\rangle^{\otimes m}$, where m would be the number of T gates in the desired circuit. For efficient quantum computation, the depth of a family of circuits should grow at most polynomially in terms of the number of qubits n, hence in practice we would require $m = O(\text{poly}(n))$. Similarly, we could also take $\mathcal{U}$ to be nearest-neighbour matchgates, and $|\gamma\rangle$ to be a polynomial number of SWAP states (as defined and discussed in [16]).

Model	Operations	State	References
Circuit	Universal gate set	–	[3]
Magic State Injection	Clifford	$\|T\rangle^{\otimes p}$	[35]
Matchgates	Nearest neighbour matchgates	$\|SWAP\rangle^{\otimes p}$	[16, 17]
1-way MBQC	LOCC	Graph state	[8, 36]
1-way MBQC	Hadamard	Hypergraph state	[9]
Teleportation MBQC	Rotated Bell unitaries Paulis	$\|\phi^+\rangle^{\otimes p}$	[4, 22]

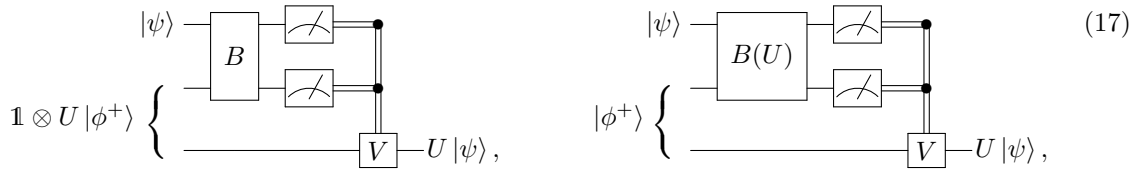
Table 1: Comparison of different models of quantum computation that fall into the framework summarised in Eq. (16), we are also allowing classical control and computational basis measurement and preparation freely. $|T\rangle$, $|SWAP\rangle$ and $\left|\phi^+\right\rangle$ respectively refer to the T state, the SWAP state [16], and the maximally entangled state. Here the tensor power p should be taken as some polynomial of the number of qubits. In place of considering measurements, we can consider the corresponding unitaries that rotate the computational basis into the appropriate basis. See also Table 1 in [9] for a more extensive summary of MBQC approaches using different measurement bases.

For measurement-based quantum computation, we take $|\gamma\rangle$ to be some entangled state, such as a graph or hypergraph state. The operations permitted here are usually taken to be local projective measurements, but we can include them in the above framework in the following way. Instead of measuring in a specific basis, we could first apply a local unitary and then measure in the computational basis. Explicitly, if we wish to measure observable $\mathcal{P} = \sum_x \alpha_x |\psi_x\rangle\langle\psi_x|$, we could instead perform the unitary $U = \sum_x |x\rangle\langle\psi_x|$ and measure in the computational basis to the same effect[1]. Hence we can incorporate measurement-based approaches here, however note that the reverse direction does not hold: the ability to perform measurements in various bases does not directly imply the ability to perform the corresponding unitaries[2]. We also remark that if the set of unitaries $\mathcal{U}$ are single qubit unitaries, then clearly we are in the measurement based scenario (as opposed to some gate injection scheme).

[1] This is effectively the Heisenberg picture.

[2] However as we have seen, there exist Hadamard gadgets if one is allowed to perform an X measurement. Hence with respect to incoherent unitaries, the Hadamard gate and X measurement are equivalent in some sense.

Let us also recall teleportation-based MBQC [4, 22]. Consider the following two circuit identities:



(17)

where $B := (H \otimes \mathbb{1})CNOT_{12}$ denotes the Bell unitary, $B(U) := (\mathbb{1} \otimes U)B$ is the rotated Bell unitary, $|\phi^+\rangle = d^{-\frac{1}{2}} \sum_{k=0}^{d-1} |kk\rangle \in \mathbb{C}^{d^2}$ is the maximally entangled state, and V is a Pauli correction term. Hence given a pool of Bell states or rotated Bell states we can achieve universality in this way. One can also teleport the CNOT gate in a similar fashion using a 4 qubit Bell state.

Pauli based computation (PBC) [37] proceeds by adaptively performing non-destructive Pauli measurements on $|T\rangle$ states as input. To incorporate this into our framework by phrasing it in the language of unitaries and computational basis measurements, we would have to find unitaries U such that $UCU^\dagger = P$, where C is a non-degenerate Hermitian operator diagonal in the computational basis, and P is a tensor product of Pauli operators. Note that measuring the operator $Z \otimes \cdots \otimes Z$ is not equivalent to measuring in the computational basis (it has 2 outcomes as opposed to 2^n).

We also remark that to consider the notion of *efficient* universal quantum computation, it is necessary to consider a family of sets of unitaries on n qubits, and the size of ancillary state $|\gamma(n)\rangle$ should scale at most polynomially with n [8, 27]. Our results allow the ancilla to be of arbitrary size, and we show the impossibility of providing a Hadamard gadget (using incoherent resources) within this framework. To extend our discussion to the MBQC framework, the scaling size of the ancillary state must be taken into account. To see this, recall that an ϵ-net is a set of states such that any state is within distance ϵ of some state in the net. One could take the tensor product all the states in such a net as the ancilla. Then for any given state, there would exist a marginal of $|\gamma\rangle$ within distance ϵ. Thus it may appear that this would lead to a universal model of quantum computation in which the only operations required are partial traces. However, such a state would not scale polynomially in the number of qubits – we elaborate on this concept in Section 4.2.

2.2 General Form of Operations

In order to make concrete statements, we now motivate an expression for a general operation within the above framework. We will first need a short definition:

Definition 6. Given some set of unitaries $\mathcal{U}$ and a preferred basis $\{|x\rangle\}$, we denote by $\mathcal{C}(\mathcal{U})$ the corresponding set of generalised controlled unitaries. In particular, on n qubits these are of the form

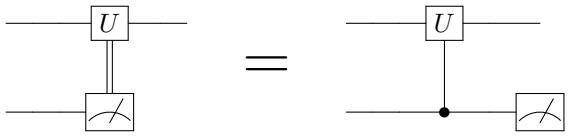
$$\sum_{x \in S} |x\rangle\langle x| \otimes U + \sum_{y \in S^c} |y\rangle\langle y| \otimes \mathbb{1}, \tag{18}$$

where $U \in \mathcal{U}$ acts on $k \leq n$ qubits, $S \subseteq \{0,1\}^{n-k}$ and S^c is the complement of S in $\{0,1\}^{n-k}$.

This definition simply describes the quantum equivalent of classically controlled operations: given a computational basis vector, a unitary is performed on a subset of the qubits only for some specific values of the remaining bits. Observe that CNOT, controlled-Z and Toffoli fall under this definition, and general controlled operations are also discussed in [3, 38] (but for the case where S contains a single bitstring). Note that this definition also encompasses the case of $\mathbb{1} \otimes U$ (here $S = \{0,1\}^{n-k}$ and S^c is the empty set), and also the case of $\mathbb{1} \otimes \mathbb{1}$; we will use the term 'controlled-U' in this broader sense.

Now consider the operations arising from Eq. (16). We can without loss of generality append all computational basis states at the beginning, and absorb them into $|\gamma\rangle\langle\gamma|$. Hence we can consider the input to be $\rho \otimes |\gamma\rangle\langle\gamma|$.

One could then apply a sequence of intermittent unitaries and computational basis measurements, which could be an adaptive process conditioned on some classical information and the outcomes of previous measurements. Note that we can delay these measurements to the end, by instead using unitaries from the controlled set $\mathcal{C}(\mathcal{U})$. That is, if a unitary U is to be applied on system A conditioned on the outcome of some previous measurement on system B, we could instead apply a unitary to system B (mapping the original measurement bases to the computational basis), and perform a controlled-U operation on system A with system B as control. We can then defer the measurement of system B until the end of the computation. This is often referred to as the *principle of deferred measurement* [3], see Fig. 2. For example in one-way MBQC, this would result in a circuit of controlled single qubit unitaries being applied to the cluster state. Finally, one could disregard some of the systems, corresponding to a partial trace. Put together, this now leads to the following observation.



(19)

Figure 2: Principle of Deferred Measurement [3].

Observation 7. The most general channel possible to implement within the above framework is given by

$$\mathcal{E}(\rho) = \mathrm{Tr}_X\Big(U(\rho\otimes\tau)U^\dagger\Big). \tag{20}$$

Here U belongs to the set of controlled unitaries $\mathcal{C}(\mathcal{U})$, Tr_X denotes a partial trace on some of the subsystems, and τ is an arbitrary fixed state.

The most general probabilistic (i.e. trace non-increasing) operation possible to implement within the above framework is given by a convex combination of operations of the form

$$\mathcal{E}^x(\rho) = \mathrm{Tr}_X\Big((\mathbb{1}\otimes|x\rangle\langle x|)\ U(\rho\otimes\tau)U^\dagger\Big), \tag{21}$$

where the projector $|x\rangle\langle x|$ denotes a measurement in the computational basis on some of the subsystems.

Note that the channel in Eq. (20) could include some final computational basis measurements, but as we consider the overall channel to be independent of the outcomes of these measurements this corresponds to a partial trace. See Remark 28 in Appendix A for a brief comment on how the channels we consider relate to the resource theory of coherence.

In the probabilistic case, we will be interested in the case where these subchannels are proportional to a unitary channel. Note that in general for a subchannel $\mathcal{E}$ to be proportional to a channel $\mathcal{V}$, i.e.

$$\frac{\mathcal{E}(\rho)}{\mathrm{Tr}(\mathcal{E}(\rho))} = \mathcal{V}(\rho), \tag{22}$$

we must have that $\mathrm{Tr}(\mathcal{E}^x(\rho))$ is independent of ρ, to ensure linearity.

Remark 8. We can take the ancilla to be pure without loss of generality, as we can always purify the state. That is, given $\tau = \sum p_n |n\rangle\langle n|$ in spectral decomposition, we can take $|\gamma\rangle = \sum_n \sqrt{n}\,|n\rangle\,|n\rangle$. This would incur a dimension increase of at most from $d \to d^2$ and involve rewriting the unitary U as $\mathbb{1}\otimes U$, but in our work we will leave the dimension on the

ancilla to be unrestricted, and consider the identity to always be included in the set of free unitaries. We may interchangeably write the channels of the form Eq. (20) as $\mathrm{Tr}_X(U(\rho\otimes\tau)U^\dagger)$ or $\mathrm{Tr}_X(U(\rho\otimes|\gamma\rangle\langle\gamma|)U^\dagger)$.

Having justified the form for channels considered in our framework, we can now use Eq. (20) and Eq. (21) as a solid foundation as we progress to our results section.

3 Results

In this section we now begin presenting in detail our results. Our first main contribution is to rule out a model of universal quantum computation that involves purely incoherent resources acting on some (possibly coherent) resourceful state. That is, we show that such an example would not exist in Table 1.

We will proceed by considering channels of the form $\mathcal{E}(\rho) = \mathrm{Tr}_X(U(\rho\otimes\tau)U^\dagger)$ as in Eq. (20), and we will compare these to the channel $\rho \mapsto H^{\otimes n}\rho H^{\otimes n}$. As per the discussion above in Section 2, the channel $\rho \mapsto \mathcal{E}(\rho)$ is a mathematical way of writing any operation that involves free unitaries and adaptive computational basis measurements acting on the input state ρ and some fixed ancilla τ.

We will consider two cases: firstly when we only allow the ability to perform incoherent unitaries (such as CNOT, S, T etc.). In this case the unitary U in $\mathcal{E}(\rho)$ will a be quantum controlled version of an incoherent unitary. Secondly, we will tackle the case of using k Hadamards to implement $n > k$ Hadamards. We consider the cases of exact, deterministic, approximate and probabilistic implementation, see Table 2 for a detailed summary of our findings.

	$0 \mapsto n$		$k \mapsto n$	
Exact & Deterministic	✗	(Theorem 18)	✗	(Theorem 23)
Exact & Probabilistic	✗	(Theorem 18)	?	
Approximate & Deterministic	$\mathcal{D} \geq 1 - \frac{1}{2^n}$	(Theorem 20)	?	
Approximate & Probabilistic	$\mathcal{D} \geq 1 - \frac{1}{2^n}$	(Theorem 20)	?	

Table 2: Summary of our results for using k Hadamards, incoherent unitaries, classical control, computational basis measurements and an arbitrary ancilla to simulate n Hadamards, where $n > k$. A cross (✗) indicates that we have proven a no-go result for this case. Here $\mathcal{D} = \max_\rho D(\mathcal{E}(\rho), H^{\otimes n}\rho H^{\otimes n})$ for D trace distance and $\mathcal{E}$ is the simulating channel using k Hadamards, as defined in Observation 7. A question mark (?) indicates that we have not considered this case in this work. The approximate bounds should also be compared with the case of using no ancilla, for which we show a lower bound of $\mathcal{D} \geq \sqrt{1 - 2^{k-n}}$ in Lemma 21.

The following subsection introduces some simple facts and supporting results.

3.1 Preliminaries

Here we discuss some basic results that will be useful to us in this section. The following lemma will prove crucial.

Lemma 9. The family of controlled unitaries $\mathcal{C}(\mathcal{U})$ are incoherent if and only if $\mathcal{U}$ are incoherent.

Proof. Recall from Definition 6 that the controlled unitaries are of the form

$$V = \sum_{x\in S} |x\rangle\langle x| \otimes U + \sum_{y\in S^c} |y\rangle\langle y| \otimes \mathbb{1} \tag{23}$$

for S some subset of bitstrings, and S^c its complement.

Now consider this operator acting on a computational basis state $|c_1\rangle |c_2\rangle$, (with the same tensor product structure as V above). First suppose that $c_1 \in S^c$. Then $V|c_1c_2\rangle = |c_1c_2\rangle$. Now consider $c_1 \in S$. For $U = \sum_z e^{i\theta_z} |\pi(z)\rangle\langle z|$ incoherent, we have

$$V|c_1c_2\rangle = \sum_{x\in S} |x\rangle\langle x| \otimes U|c_1c_2\rangle \tag{24}$$

$$= \sum_{x\in S} |x\rangle\langle x| \otimes \left(\sum_z e^{i\theta_z} |\pi(z)\rangle\langle z|\right) |c_1c_2\rangle \tag{25}$$

$$= e^{i\theta_{c_2}} |c_1\rangle |\pi(c_2)\rangle . \tag{26}$$

Hence V is of the form $V = \sum_x e^{i\theta_x} |\pi(x)\rangle\langle x|$ and is thus incoherent. For the other direction, if U is not incoherent, then it will map at least one basis vector $|c_2\rangle$ to a superposition. Then for $c_1 \in S$, V will map $|c_1c_2\rangle$ to $|c_1\rangle U|c_2\rangle$, which will also be a superposition, and so V is not incoherent. □

For our purposes, this Lemma allows us to take U to be itself incoherent in Observation 7, as by definition it belongs to the set of controlled incoherent unitaries. Note also that as SWAP is itself an incoherent unitary, in our case we can without loss of generality take the trace in Observation 7 to be on the ancillary subsystem, i.e.

$$\mathcal{E}^x(\rho) = \mathrm{Tr}_2\Big(U(\rho\otimes\tau)U^\dagger\Big). \tag{27}$$

In addition, we will consider the case of being able to perform k Hadamard gates, and seek to use incoherent resources and a supplementary state to implement $n > k$ Hadamard gates. In this case, without loss of generality the unitary U above will be of the following form

$$U = U_kV_k \dots U_1V_1U_0, \tag{28}$$

for U_i incoherent unitaries and V_i controlled-Hadamards ("controlled" in the general sense of Definition 6).

The following definition serves as a useful discrete quantifier of coherence for pure states.

Definition 10. The *coherence rank* [11, 39] of a pure state $|\psi\rangle$ is defined to be the minimum number of terms required to write the state as a linear combination of computational basis states. We denote this by $\chi(|\psi\rangle)$.

For example $\chi(|x\rangle) = 1$ for any computational basis state $|x\rangle$, and $\chi(|+\rangle^{\otimes n}) = 2^n$. We also have that $\chi(|\psi\rangle\otimes|\phi\rangle) = \chi(|\psi\rangle)\chi(|\phi\rangle)$. With this defined, we can state the following lemma.

Lemma 11. Let $U = U_kV_k \dots U_1V_1U_0$ be a product of unitaries, alternating between incoherent unitaries U_i and controlled-Hadamards V_i. Then we have for any state $|\psi\rangle$, the coherence rank satisfies

$$\frac{\chi(|\psi\rangle)}{2^k} \le \chi\left(U|\psi\rangle\right) \le 2^k\chi(|\psi\rangle). \tag{29}$$

Proof. First note that $\chi(U|\psi\rangle) = \chi(|\psi\rangle)$ for any incoherent unitary U (they can only permute and apply local phases to computational basis states). Now let V be a Hadamard or controlled-Hadamard gate (in the general sense of Definition 6), and consider the action on a computational basis state $|x\rangle$. We have that $V|x\rangle$ must have coherence rank either 1 or 2. Write $|\psi\rangle = \sum_x \alpha_x |x\rangle$, from which it becomes clear that $V|\psi\rangle = \sum_x \alpha_x V|x\rangle$ can have at most $2\chi(|\psi\rangle)$ terms (some of the terms could cancel). Hence we have $\chi(V|\psi\rangle) \le 2\chi(|\psi\rangle)$ for all $|\psi\rangle$, which also implies that $\chi(|\psi\rangle) \le 2\chi(V^\dagger|\psi\rangle) = 2\chi(V|\psi\rangle)$, as V is self-inverse. Combining these shows that

$$\frac{\chi(|\psi\rangle)}{2} \le \chi\left(V|\psi\rangle\right) \le 2\chi(|\psi\rangle). \tag{30}$$

Now we can use induction. The base case of $U = U_1 V_1$ follows immediately from the above. Now suppose that

$$\frac{\chi(|\psi\rangle)}{2^k} \leq \chi\left(U_k V_k \dots U_1 V_1 U_0 |\psi\rangle\right) \leq 2^k \chi(|\psi\rangle). \tag{31}$$

Define $|\phi\rangle = U_k V_k \dots U_1 V_1 U_0 |\psi\rangle$, and we then get

$$\frac{\chi(|\phi\rangle)}{2} \leq \chi\left(U_{k+1} V_{k+1} |\phi\rangle\right) = \chi\left(V_{k+1} |\phi\rangle\right) \leq 2\chi(|\phi\rangle). \tag{32}$$

□

We will use these upper and lower bounds on the coherence rank as a key ingredient in Theorem 23, one of our no-go results.

We can also make some simple observations about the trace distance, in particular:

Lemma 12. For the induced trace distance, it is sufficient to take the maximum over pure states, i.e. for any channels $\mathcal{E}$, $\mathcal{V}$

$$\mathcal{D}(\mathcal{E}, \mathcal{V}) := \max_{\rho} \; D\Big(\mathcal{E}(\rho), \mathcal{V}(\rho)\Big) = \max_{|\phi\rangle} \; D\Big(\mathcal{E}(|\phi\rangle\langle\phi|), \mathcal{V}(|\phi\rangle\langle\phi|)\Big). \tag{33}$$

Proof.

$$\begin{aligned}
\max_{\rho} D(\mathcal{E}(\rho), \mathcal{V}(\rho)) &= \max_{p_i, \psi_i} D\Big(\sum p_i \mathcal{E}(\psi_i), \sum p_i \mathcal{V}(\psi_i)\Big) && (34)\\
&\leq \max_{p_i, \psi_i} \sum p_i D(\mathcal{E}(\psi_i), \mathcal{V}(\psi_i)) && (35)\\
&\leq \max_{p_i, \psi_i} \sum p_i \left(\max_{\phi} D(\mathcal{E}(\phi), \mathcal{V}(\phi))\right) && (36)\\
&= \max_{\phi} D(\mathcal{E}(\phi), \mathcal{V}(\phi)) && (37)\\
&\leq \max_{\rho} D(\mathcal{E}(\rho), \mathcal{V}(\rho)) && (38)
\end{aligned}$$

where ρ denotes a mixed state, ψ_i and ϕ denote pure states, and we used linearity of the channels and joint convexity of the trace distance [3]. □

For pure states we also have that [40]

$$D\Big(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|\Big) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}. \tag{39}$$

Combining this with Lemma 12 leads to the following corollary:

Corollary 13. The induced trace distance between unitary channels is given by

$$\mathcal{D}(U, V) = \max_{|\psi\rangle} \sqrt{1 - |\langle\psi| U^\dagger V |\psi\rangle|^2}. \tag{40}$$

Let us now briefly consider the case of no-ancilla. We would expect a non-zero distance between $H^{\otimes n}$ and a unitary composed of incoherent gates and $k < n$ Hadamard gates. We have the following lower bound in this case:

Lemma 14. Let $U = U_k V_k \dots U_1 V_1 U_0$, where U_i are incoherent and V_i are controlled Hadamards, and let $n \geq k$. Then

$$\mathcal{D}(U, H^{\otimes n}) \geq \sqrt{1 - 2^{k-n}}. \tag{41}$$

Proof. Using Corollary 13 we have that

$$\mathcal{D}(U, H^{\otimes n}) = \max_{|\psi\rangle} \sqrt{1 - |\langle\psi| H^{\otimes n} U |\psi\rangle|^2} \tag{42}$$

$$\geq \sqrt{1 - |\langle 0^n| H^{\otimes n} U |0^n\rangle|^2} \tag{43}$$

$$\geq \sqrt{1 - |\langle +^n| U |0^n\rangle|^2}. \tag{44}$$

Now $U|0^n\rangle = U_k V_k \dots U_1 V_1 U_0 |0^n\rangle$ will have coherence rank at most 2^k (as each incoherent unitary preserves the coherence rank, and each controlled Hadamard can at most double the coherence rank, by Lemma 11). Thus we have $U|0^n\rangle = \sum_{x=0}^{2^k-1} \alpha_x |c_x\rangle$ where $|c_x\rangle$ are (not necessarily distinct) computational basis states. As $|+^n\rangle = 2^{\frac{-n}{2}} \sum_{x\in\{0,1\}^n} |x\rangle$, we have that

$$|\langle +^n| U |0^n\rangle|^2 = \left| \frac{\sum_{x=0}^{2^k-1} \alpha_x}{2^{\frac{n}{2}}} \right|^2 \leq \frac{2^k \sum_{x=0}^{2^k-1} |\alpha_x|^2}{2^n} = 2^{k-n}, \tag{45}$$

where the inequality follows from Cauchy-Schwarz: $\left|\sum_{x=0}^{M-1} \alpha_x\right|^2 \leq M \sum_{x=0}^{M-1} |\alpha_x|^2$ for all M, and we used $\sum_{x=0}^{2^k-1} |\alpha_x|^2 = 1$. Hence we have that

$$\mathcal{D}(U, H^{\otimes n}) \geq \sqrt{1 - |\langle +^n| U |0^n\rangle|^2} \tag{46}$$

$$\geq \sqrt{1 - 2^{k-n}}. \tag{47}$$

□

This shows that if $k \ll n$, the unitary U composed of k Hadamards cannot be close in induced trace distance to n Hadamards, as intuitively expected.

We now consider the first case of using purely incoherent unitaries (0 Hadamards) and an ancilla to implement n Hadamards, considering the exact, approximate and probabilistic cases.

3.2 Incoherent resources and an ancilla cannot implement $n > 0$ Hadamards

We first consider the question of whether incoherent resources supplemented with an arbitrary ancillary state can implement a single Hadamard gate. We show that this is not the case. Our strategy is to first show in Lemma 15 below that if a channel satisfies a certain relation with the dephasing map, then when acting jointly on an input state and fixed arbitrary ancilla the channel cannot implement any coherent unitary. Secondly, we show in Lemma 16 that channels that only use incoherent resources supplemented with an arbitrary ancilla state (see Section 2) satisfy this relation, and hence are not able to implement any coherent unitary, such as the Hadamard.

To begin, let us prove the following lemma, which is in fact a generalisation of an observation made in the erratum of [12] (see Example 4 for more context here).

Lemma 15. Let $\mathcal{E} : \mathcal{S}(\mathcal{H}_1) \otimes \mathcal{S}(\mathcal{H}_2) \to \mathcal{S}(\mathcal{H}_1)$ be any channel such that

$$\Delta \circ \mathcal{E} \circ \Delta = \Delta \circ \mathcal{E}, \tag{48}$$

where Δ is the dephasing map defined in Eq. (15). Then for any state $\tau \in \mathcal{S}(\mathcal{H}_2)$ the channel

$\mathcal{E}_\tau(\rho) := \mathcal{E}(\rho \otimes \tau)$ cannot implement any coherent unitary exactly.

Proof of Lemma 15. Suppose that $\mathcal{E}(\rho \otimes \tau) = U\rho U^\dagger$ for some unitary U. We seek to show that U must be incoherent if the condition (48) is met. This condition implies that

$$\Delta\Big(\mathcal{E}(\Delta(\rho \otimes \tau))\Big) = \Delta\Big(U\rho U^\dagger\Big), \qquad \forall \rho. \tag{49}$$

Let $U_{yx} := \langle y| U |x\rangle$, so that

$$U|x\rangle = \sum_y U_{yx}|y\rangle \qquad U^\dagger|x\rangle = \sum_y U^*_{xy}|y\rangle \tag{50}$$

$$\langle x|U = \sum_y U_{xy}\langle y| \qquad \langle x|U^\dagger = \sum_y U^*_{yx}\langle y|, \tag{51}$$

We can now use the facts that $\Delta(\rho \otimes \tau) = \Delta(\rho) \otimes \Delta(\tau)$ and $\Delta(|x\rangle\langle x|) = |x\rangle\langle x|$, and first input $\rho = |x\rangle\langle x|$ in Eq. (49) to obtain

$$\Delta\Big(\mathcal{E}(|x\rangle\langle x| \otimes \Delta(\tau))\Big) = \Delta\left(\sum_{y,z} U_{yx}U^*_{zx}|y\rangle\langle z|\right) \tag{52}$$

$$= \sum_y |U_{yx}|^2 |y\rangle\langle y| \tag{53}$$

Multiplying both sides by $|U_{zx}|^2$ and summing over x implies

$$\sum_x |U_{zx}|^2 \Delta\Big(\mathcal{E}(|x\rangle\langle x| \otimes \Delta(\tau))\Big) = \sum_{x,y} |U_{zx}|^2 |U_{yx}|^2 |y\rangle\langle y|. \tag{54}$$

Now focusing on $\rho = U^\dagger|z\rangle\langle z|U = \sum_{x,w} U_{zw}U^*_{zx}|x\rangle\langle w|$, we have $\Delta(\rho) = \sum_x |U_{zx}|^2 |x\rangle\langle x|$. Eq. (49) then implies that

$$\sum_x |U_{zx}|^2 \Delta \circ \mathcal{E}\Big(|x\rangle\langle x| \otimes \Delta(\tau)\Big) = |z\rangle\langle z|. \tag{55}$$

Comparing (54) with (55), as the left-hand sides are equal we see that

$$\sum_{x,y} |U_{zx}|^2 |U_{yx}|^2 |y\rangle\langle y| = |z\rangle\langle z|. \tag{56}$$

This can only be true if

$$\sum_x |U_{zx}|^2 |U_{yx}|^2 = 0 \quad \text{for } y \neq z. \tag{57}$$

However as all terms are non-negative, we have the stronger implication that

$$|U_{zx}||U_{yx}| = 0 \quad \text{for } y \neq z, \forall x. \tag{58}$$

This final equation implies that for all x, there can be at most one value of y such that $U_{yx} \neq 0$. As U is unitary, this implies that in each column there is exactly one non-zero entry, so U must be incoherent. In particular,

$$U|x\rangle = \sum_y U_{yx}|y\rangle = U_{y'x}|y'\rangle, \tag{59}$$

for some y' (depending on x). Thus in summary, Eq. (49) implies that if the channel $\mathcal{E}_\tau$ is unitary then it must be incoherent, independent of τ. □

To put this technical result into context, we now show that the channels proposed in Observation 7 satisfy the condition in Lemma 15, and thus an arbitrary ancilla is not sufficient to elevate incoherent resources to computational universality.

Lemma 16. For any incoherent unitary U, the map $\rho \mapsto \mathrm{Tr}_2\left(U\rho U^\dagger\right)$ commutes with the dephasing map Δ.

See Eq. (116) for the definition of incoherent unitaries, and Eq. (15) for the definition of the dephasing map.

Proof. First let us see that the dephasing map commutes with the action of any incoherent unitary, recall that these are of the form $U = \sum_{x=1}^{d} e^{i\theta_x} |\pi(x)\rangle\langle x|$ for some permutation π (Eq. (116)).

Then for any state ρ we have

$$U\Delta(\rho)U^\dagger = \left(\sum_y e^{i\theta_y} |\pi(y)\rangle\langle y|\right) \sum_x |x\rangle\langle x|\,\rho\,|x\rangle\langle x| \left(\sum_z e^{-i\theta_z} |z\rangle\langle\pi(z)|\right) \tag{60}$$

$$= \sum_{x,y,z} e^{i\theta_y} e^{-i\theta_z} \; |\pi(y)\rangle\langle y|x\rangle\langle x|\,\rho\,|x\rangle\langle x|z\rangle\langle\pi(z)| \tag{61}$$

$$= \sum_x |\pi(x)\rangle\langle x|\,\rho\,|x\rangle\langle\pi(x)|\,. \tag{62}$$

Noting that we can also write the dephasing map as $\Delta(\rho) = \sum_x |\pi(x)\rangle\langle\pi(x)|\,\rho\,|\pi(x)\rangle\langle\pi(x)|$ for any permutation π leads to

$$\Delta(U\rho U^\dagger) = \sum_x |\pi(x)\rangle\langle\pi(x)| \left(\sum_y e^{i\theta_y} |\pi(y)\rangle\langle y|\,\rho \sum_z e^{-i\theta_z} |z\rangle\langle\pi(z)|\right) |\pi(x)\rangle\langle\pi(x)| \tag{63}$$

$$= \sum_{x,y,z} e^{i\theta_y} e^{-i\theta_z} \, |\pi(x)\rangle\langle\pi(x)|\pi(y)\rangle\langle y|\,\rho\,|z\rangle\langle\pi(z)|\pi(x)\rangle\langle\pi(x)| \tag{64}$$

$$= \sum_x |\pi(x)\rangle\langle x|\,\rho\,|x\rangle\langle\pi(x)|\,. \tag{65}$$

Hence the equality of Eq. (62) and Eq. (65) (and as ρ was arbitrary) show that $\Delta \circ U = U \circ \Delta$ for any incoherent U. It is also clear that the dephasing map commutes with the partial trace, from which the result follows. □

Since $\Delta^2 = \Delta$, we have that $\mathcal{E} \circ \Delta = \Delta \circ \mathcal{E} \implies \Delta \circ \mathcal{E} \circ \Delta = \Delta \circ \mathcal{E}$ for any channel $\mathcal{E}$, that is, commutation of $\mathcal{E}$ with Δ implies the condition imposed in Lemma 15.

Hence Lemma 16 and Lemma 15 together show that given incoherent unitaries and classical control, encapsulated by the channel $\rho \mapsto \mathcal{E}(\rho \otimes \tau)$ (see the discussion in Section 2), cannot exactly implement any coherent unitary, even when supplemented with an arbitrary ancilla. This is in direct contrast to other situations, such as magic state injection.

This result is about exactly implementing a coherent unitary. It is natural to question whether this no-go result arises from demanding too much. One possible relaxation is to consider implementation of a coherent unitary with some non-zero probability: surprisingly we can still show that this is impossible.

We can also show the same result for probablistic implementations. Recall from Observation 7 (and surrounding text) that we represent these by convex combinations of normalised sub-channels

$$\mathcal{E}^x(\rho) = \alpha \mathrm{Tr}_X\left(\mathbb{1} \otimes |x\rangle\langle x|\, U\rho \otimes \tau U^\dagger\right). \tag{66}$$

where the normalisation factor α does not depend on the input ρ.

Lemma 17. For incoherent U, the normalised sub-channel $\rho \mapsto \mathcal{E}^x(\rho)$ commutes with the dephasing map Δ.

The working is very similar to that of Lemma 16, and we give a more concise proof as follows.

Proof.

$$(\Delta \circ \mathcal{E}^x)(\rho) = \sum_i |i\rangle\langle i| \operatorname{Tr}_X \left(\mathbb{1} \otimes |x\rangle\langle x| \, U\rho U^\dagger \right) |i\rangle\langle i| \tag{67}$$

$$= \sum_j \operatorname{Tr}_X \left(|j\rangle\langle j| \, \mathbb{1} \otimes |x\rangle\langle x| \, U\rho U^\dagger \, |j\rangle\langle j| \right) \tag{68}$$

$$= \operatorname{Tr}_X \left(\mathbb{1} \otimes |x\rangle\langle x| \sum_j |j\rangle\langle j| \, U\rho U^\dagger \, |j\rangle\langle j| \right) \tag{69}$$

$$= \operatorname{Tr}_X \left(\mathbb{1} \otimes |x\rangle\langle x| \, U \sum_j |j\rangle\langle j| \, \rho \, |j\rangle\langle j| \, U^\dagger \right) \tag{70}$$

$$= (\mathcal{E}^x \circ \Delta)(\rho) \tag{71}$$

□

As any convex combination of such channels will also commute with the dephasing map, by Lemma 15 we can see that any attempt to even probabilistically implement a coherent unitary exactly will fail. We can summarise the preceding with our first main result:

Theorem 18. Given the ability to perform incoherent unitaries, computational basis measurements and classical control, it is impossible to implement any coherent unitary (e.g. Hadamard) exactly with any non-zero probability, even when supplemented with an arbitrary ancilla.

Proof. As discussed in Section 2, the ability to perform incoherent unitaries, computational basis measurements and classical control is encapsulated by channels of the form $\rho \mapsto \operatorname{Tr}_2(U\rho U^\dagger)$ for U incoherent, or in the probabilistic case by convex combinations of subchannels $\rho \mapsto \operatorname{Tr}_2(\mathbb{1} \otimes |x\rangle\langle x| \; U\rho U^\dagger)$. By Lemma 16 and Lemma 17, these maps commute with the dephasing map Δ. Hence we can apply Lemma 15 to see that given access to the above operations, one can never implement any coherent unitary exactly. □

Approximate Implementation

Having considered the exact and probabilistic cases, we now turn our attention to the approximate case, focusing on tensor products of Hadamard gates (as opposed to arbitrary coherent unitaries). Specifically, we seek lower bounds on the induced trace distance between the channels introduced in Observation 7 and n Hadamard gates. Our second main technical result achieves this goal as follows.

Lemma 19. Let $\mathcal{E} : \mathcal{S}(\mathcal{H}_1) \otimes \mathcal{S}(\mathcal{H}_2) \to \mathcal{S}(\mathcal{H}_1)$ be any channel that commutes with the dephasing map, i.e.

$$\mathcal{E} \circ \Delta = \Delta \circ \mathcal{E}, \tag{72}$$

where Δ is the dephasing map defined in Eq. (15). Define the channel $\mathcal{E}_\tau(\rho) := \mathcal{E}(\rho \otimes \tau)$ for an arbitrary state $\tau \in \mathcal{S}(\mathcal{H}_2)$. Let $\mathcal{D}$ denote the induced trace distance on quantum channels. Then for all states τ, we have

$$\mathcal{D}\left(\mathcal{E}_\tau \; , \; H^{\otimes n} \right) \geq 1 - \frac{1}{2^n}. \tag{73}$$

Proof of Lemma 19. Let $C_n = \{|x\rangle \; : \; x \in \{0,1\}^n\}$ denote the set of computational basis states, and $B_n = \{|x\rangle \; : \; x \in \{+,-\}^n\}$ denote the set of conjugate basis states. Note that $H^{\otimes n}$ maps bijectively between C_n and B_n. We then have

$$\mathcal{D}\Big(\mathcal{E}_\tau\ ,\ H^{\otimes n}\Big) := \max_\rho D\Big(\mathcal{E}(\rho\otimes\tau)\ ,\ H^{\otimes n}\rho H^{\otimes n}\Big) \tag{74}$$

$$\geq \max_\rho D\Big(\Delta\circ\mathcal{E}(\rho\otimes\tau)\ ,\ \Delta(H^{\otimes n}\rho H^{\otimes n})\Big) \tag{75}$$

$$= \max_\rho D\Big(\mathcal{E}(\Delta(\rho)\otimes\Delta(\tau))\ ,\ \Delta(H^{\otimes n}\rho H^{\otimes n})\Big) \tag{76}$$

$$\geq \max_{|\phi\rangle\in B_n} D\Big(\mathcal{E}(\Delta(|\phi\rangle\langle\phi|)\otimes\Delta(\tau))\ ,\ \Delta(H^{\otimes n}\,|\phi\rangle\langle\phi|\,H^{\otimes n})\Big) \tag{77}$$

$$= \max_{|\psi\rangle\in C_n} D\Big(\mathcal{E}(\frac{\mathbb{1}}{2^n}\otimes\Delta(\tau))\ ,\ |\psi\rangle\langle\psi|)\Big), \tag{78}$$

where we used the contractivity of the trace distance under quantum channels, and the condition on $\mathcal{E}$ commuting with the dephasing map from the theorem statement.

Now define $\sigma := \mathcal{E}(\frac{\mathbb{1}}{2^n}\otimes\Delta(\tau))$, and note that $\Delta(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$ for all $|\psi\rangle\in C_n$. Again using contractivity of the trace distance we can then write

$$\mathcal{D}\Big(\mathcal{E}_\tau\ ,\ H^{\otimes n}\Big) \geq \max_{|\psi\rangle\in C_n} D\Big(\sigma\ ,\ |\psi\rangle\langle\psi|)\Big) \tag{79}$$

$$\geq \max_{|\psi\rangle\in C_n} D\Big(\Delta(\sigma)\ ,\ \Delta(|\psi\rangle\langle\psi|))\Big) \tag{80}$$

$$= \max_{|\psi\rangle\in C_n} D\Big(\Delta(\sigma)\ ,\ |\psi\rangle\langle\psi|)\Big) \tag{81}$$

$$\geq \max_{|\psi\rangle\in C_n} \Big(1-\langle\psi|\,\Delta(\sigma)\,|\psi\rangle\Big) \tag{82}$$

$$\geq 1-\frac{1}{2^n} \tag{83}$$

The last line can be seen by observing that for any incoherent state, the maximum diagonal entry must be at least $\frac{1}{2^n}$.

□

This bound is displayed in Table 2, and for the case of a single Hadamard the bound becomes $\mathcal{D}(\mathcal{E}_\tau, H)\geq\frac{1}{2}$. Operationally, this means that using an optimal (unentangled) input to the channels, we can distinguish them with high probability given multiple uses. Note also that as the induced trace distance is a lower bound on the diamond distance [41], we also have the same lower bound on the diamond distance between the above channels. We can also see that this bound is tight, as for example taking the channel $\mathcal{E}$ to be the map that always outputs the maximally mixed state (which commutes with Δ), we have that $\mathcal{D}(\mathcal{E}_\tau, H^{\otimes n}) = 1-\frac{1}{2^n}$ which matches the bound.

Furthermore, we can observe that the above analysis also applies to the probabilistic case: using the fact that the corresponding normalised subchannel (21) commutes with Δ (Lemma 17) we see that Lemma 19 also applies. The conclusion is that even approximate, probabilistic implementation of Hadamards is not possible, which is our second main result. Recall (from Section 1.3) that we say we can implement a channel $\mathcal{E}$ *ϵ-approximately* if we can implement a channel $\mathcal{V}$ with induced trace distance $\mathcal{D}(\mathcal{E},\mathcal{V})\leq\epsilon$.

Theorem 20. Given the ability to perform incoherent unitaries, computational basis measurements and classical control, it is impossible to implement n Hadamards ϵ-approximately with non-zero probability, for $0\leq\epsilon<1-2^{-n}$. In particular, it is impossible to implement a single Hadamard ϵ-approximately with non-zero probability, for $0\leq\epsilon<\frac{1}{2}$.

Proof. The proof follows a similar structure to that of Theorem 18. We can describe channels arising from the stated operations by channels of the form $\rho\mapsto \mathrm{Tr}_2(U\rho U^\dagger)$ for U incoherent, or

in the probabilistic case by convex combinations of subchannels $\rho \mapsto \mathrm{Tr}_2(\mathbb{1} \otimes |x\rangle\langle x|\ U\rho U^\dagger)$ (see Section 2). These maps commute with the dephasing map Δ by Lemma 16 and Lemma 17. Then Lemma 19 implies that given access to the above operations, one can never implement a channel that has induced trace distance with $H^{\otimes n}$ of strictly less than $1 - 2^{-n}$. □

3.3 Incoherent resources, k Hadamards and an ancilla cannot implement $n > k$ Hadamards

The above showed that incoherent resources supplemented with an arbitrary state is not sufficient to implement even a single Hadamard gate, even approximately and probabilistically. A further generalisation is to consider the case of having the ability to perform up to k Hadamard gates, incoherent unitaries, classical control and access to an ancillary state. Could it be possible here to implement n Hadamard gates, with n strictly greater than k? It would be very striking if this were the case, as then by repeating this process (and having many copies of the ancilla) one could implement an arbitrarily high number of Hadamard gates when originally only given the ability to perform a fixed number of them. We will show that this is indeed not the case, which demonstrates the robustness of our previous results in this direction. Our result holds when also considering general controlled Hadamard gates, which is stronger than considering single qubit Hadamard gates as these are a special case of our generalised controlled operations in Definition 6. Note also that the previous section is a special case of the scenario here (with $k = 0$), however the approach and proof technique here differs substantially.

Let us first see a simple example of the case $1 \mapsto 2$ to illustrate the general argument to follow. For example, one could ask about the existence of circuits of the form as in Fig. 3, for all two-qubit inputs $|\psi\rangle$, fixed ancilla $|\gamma\rangle$, incoherent unitaries U, V and W, and where H_i denotes a Hadamard on the i-th qubit.

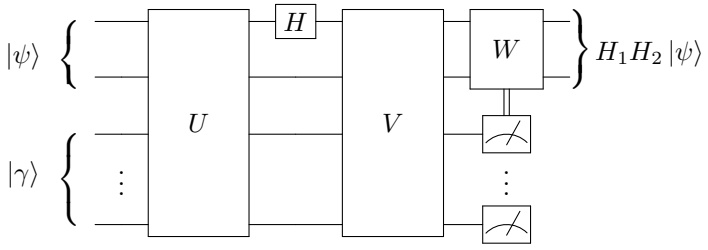


Figure 3: A possible circuit for using a single Hadamard gate and incoherent unitaries U, V and W to implement two Hadamard gates. We rule out the existence of such a circuit in this work.

Let us now be more precise, and argue by contradiction. Suppose that the above task was possible. This would mean that the following equation would hold:

$$H_1H_2\,|\psi\rangle\,|\gamma_\psi\rangle = VH_1U\,|\psi\rangle\,|\gamma\rangle\,, \tag{84}$$

for some state $|\gamma\rangle$, a set of states $|\gamma_\psi\rangle$ that could depend on $|\psi\rangle$, incoherent unitaries U and V, and where H_i denotes a Hadamard on the i-th qubit. To see how the above diagram can be written in this form, recall from Section 2 that we can replace the last gate W by its quantum controlled version (which will be incoherent by Lemma 9) and absorb it into V.

Now expanding $|\psi\rangle$ in a basis allows us to see that $|\gamma_\psi\rangle$ must actually be independent of $|\psi\rangle$. One may already expect this, as the first register contains all the information of the pure state $|\psi\rangle$, for the ancilla system to contain some information of $|\psi\rangle$ would seem to imply a form of cloning. Indeed for $|\psi\rangle = \sum_x \alpha_x\,|x\rangle$ we have

$$H_1H_2\,|\psi\rangle\,|\gamma_\psi\rangle = \sum_x \alpha_x VH_1U\,|x\rangle\,|\gamma\rangle = \sum_x \alpha_x H_1H_2\,|x\rangle\,|\gamma_x\rangle\,. \tag{85}$$

Tracing out the first register then gives

$$|\gamma_\psi\rangle\langle\gamma_\psi| = \sum_x |\alpha_x|^2\,|\gamma_x\rangle\langle\gamma_x|\,, \tag{86}$$

from which the independence on $|\psi\rangle$ follows: a sum of rank 1 operators with non-negative coefficients can only be equal to a rank 1 operator if all the operators are proportional. We can now write

$$VH_1U\,|\psi\rangle\,|\gamma\rangle = H_1H_2\,|\psi\rangle\,|\gamma'\rangle \tag{87}$$

for some state $|\gamma'\rangle$. Let the coherence rank of $|\gamma\rangle$ and $|\gamma'\rangle$ be r and r' respectively. Then taking $|\psi\rangle$ to be $|00\rangle$ and $|{+}{+}\rangle$, Eq. (87) implies the following two equations

$$VH_1U\,|00\rangle\,|\gamma\rangle = |{+}{+}\rangle\,|\gamma'\rangle \tag{88}$$

$$VH_1U\,|{+}{+}\rangle\,|\gamma\rangle = |00\rangle\,|\gamma'\rangle\,. \tag{89}$$

By recalling that incoherent unitaries cannot change the coherence rank, and a single Hadamard can at most double and at least halve the coherence rank, these equations respectively imply that

$$4r' \in [\frac{r}{2}, 2r] \tag{90}$$

$$r' \in [2r, 8r] \quad \implies 4r' \in [8r, 32r], \tag{91}$$

which is a contradiction. We thus see that it must be impossible for a single Hadamard gate, incoherent unitaries and classical control to implement two Hadamard gates, even given access to the arbitrary state $|\gamma\rangle$.

We can generalise and formalise this argument to show the impossibility of k Hadamards and incoherent resources implementing $n > k$ Hadamards. The argument will proceed in the same two steps as above: first showing that the ancillary register must be left in a state that is independent of the input ρ, and secondly use the resource content of these states (coherence rank) to derive a contradiction.

Lemma 21. Suppose that there exists some bipartite unitary U, local unitary V, and state $|\gamma\rangle$ such that for all ρ we have

$$\mathrm{Tr}_2\left(U\rho\otimes|\gamma\rangle\langle\gamma|\,U^\dagger\right) = V\rho V^\dagger. \tag{92}$$

Then

$$\mathrm{Tr}_1\left(U\rho\otimes|\gamma\rangle\langle\gamma|\,U^\dagger\right) = |\gamma'\rangle\langle\gamma'| \tag{93}$$

for some fixed pure state $|\gamma'\rangle$ that is independent of ρ.

Proof. In particular, for $\rho = |\psi\rangle\langle\psi|$ a pure state, Eq. (92) becomes

$$\mathrm{Tr}_2\left(U\,|\psi\rangle\langle\psi|\otimes|\gamma\rangle\langle\gamma|\,U^\dagger\right) = V\,|\psi\rangle\langle\psi|\,V^\dagger. \tag{94}$$

Since tracing out the second system of $U\,|\psi\rangle\,|\gamma\rangle$ results in a pure state for all $|\psi\rangle$, the total state $U\,|\psi\rangle\,|\gamma\rangle$ must be a pure product state. So in summary we must have

$$U\Big(\,|\psi\rangle\,|\gamma\rangle\,\Big) = V\otimes\mathbb{1}\Big(\,|\psi\rangle\,|\gamma_\psi\rangle\,\Big) \tag{95}$$

for some pure state $|\gamma_\psi\rangle$ that a priori could depend on $|\psi\rangle$.

Now as before, write $|\psi\rangle = \sum_x \alpha_x\,|x\rangle$. Then we have

$$V\otimes\mathbb{1}\,|\psi\rangle\,|\gamma_\psi\rangle = \sum_x \alpha_x\; U\,|x\rangle\,|\gamma\rangle = \sum_x \alpha_x\; V\otimes\mathbb{1}\,|x\rangle\,|\gamma_x\rangle \tag{96}$$

Multiplying by $V^\dagger\otimes\mathbb{1}$ now implies that

$$\sum_x \alpha_x\,|x\rangle\,|\gamma_\psi\rangle = \sum_x \alpha_x\;\;|x\rangle\,|\gamma_x\rangle\,. \tag{97}$$

Tracing out the first system gives

$$|\gamma_\psi\rangle\langle\gamma_\psi| = \sum_x |\alpha_x|^2 |\gamma_x\rangle\langle\gamma_x|, \tag{98}$$

which in turn implies

$$|\gamma_\psi\rangle\langle\gamma_\psi| = |\gamma_x\rangle\langle\gamma_x| = |\gamma_{x'}\rangle\langle\gamma_{x'}| \qquad \forall x, x', \psi \tag{99}$$

and so $|\gamma_\psi\rangle$ must be independent of $|\psi\rangle$.

Hence we have shown that for all pure states $|\psi\rangle$

$$\mathrm{Tr}_1\left(U|\psi\rangle\langle\psi| \otimes |\gamma\rangle\langle\gamma| U^\dagger\right) = |\gamma'\rangle\langle\gamma'| \tag{100}$$

for some state $|\gamma'\rangle$ independent of $|\psi\rangle$. To complete the proof, write an arbitrary mixed state as $\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$ with $\sum_k p_k = 1$, and observe that

$$\mathrm{Tr}_1\left(U\rho \otimes |\gamma\rangle\langle\gamma| U^\dagger\right) = \sum_k p_k \mathrm{Tr}_1\left(U|\psi_k\rangle\langle\psi_k| \otimes |\gamma\rangle\langle\gamma| U^\dagger\right) \tag{101}$$

$$= \sum_k p_k |\gamma'\rangle\langle\gamma'| \tag{102}$$

$$= |\gamma'\rangle\langle\gamma'| \tag{103}$$

□

We can use this lemma to explicitly rule out the possibility of k Hadamards and incoherent resources exactly implementing n Hadamards. To do this, we will consider unitaries of the following form:

$$U = U_k V_k \dots U_1 V_1 U_0, \tag{104}$$

where U_i are incoherent unitaries and V_i are Hadamards or controlled Hadamards (in the general sense of Definition 6). As discussed in Section 2, this describes any operation involving incoherent unitaries, classical control and k Hadamard gates – see Eq. (28) and surrounding text. We can now state our next result.

Lemma 22. Let $U = U_k V_k \dots U_1 V_1 U_0$ be a product of unitaries, alternating between incoherent unitaries U_i and controlled-Hadamards V_i. If we have that

$$\mathrm{Tr}_2\left(U\rho \otimes |\gamma\rangle\langle\gamma| U^\dagger\right) = H^{\otimes n}\rho H^{\otimes n} \qquad \forall \rho, \tag{105}$$

then we must have that $n \leq k$.

Proof. Consider the case where $\rho = |\psi\rangle\langle\psi|$ is a pure state. Using Lemma 21, we can then write Eq. (105) as

$$U|\psi\rangle|\gamma\rangle = H^{\otimes n} \otimes \mathbb{1}\,|\psi\rangle \otimes |\gamma'\rangle \tag{106}$$

for some fixed state $|\gamma'\rangle$.

Let $|\gamma\rangle$ and $|\gamma'\rangle$ have coherence ranks r and r' respectively (recall Definition 10 for the definition of the coherence rank χ), and consider the cases of $|\psi\rangle$ being equal to $|0^n\rangle$ and $|+^n\rangle$:

$$U|0^n\rangle|\gamma\rangle = |+^n\rangle|\gamma'\rangle \tag{107}$$

$$U|+^n\rangle|\gamma\rangle = |0^n\rangle|\gamma'\rangle. \tag{108}$$

By comparing the coherence ranks of both sides of the above equations, we find that $\chi(U|0^n\rangle|\gamma\rangle) = 2^n r'$ and $\chi(U|+^n\rangle|\gamma\rangle) = r'$. Hence

$$\frac{\chi(U|0^n\rangle|\gamma\rangle)}{2^n} = \chi(U|+^n\rangle|\gamma\rangle). \tag{109}$$

We now directly apply Lemma 11, which provides lower and upper bounds on the coherence rank of a state after applying a sequence of incoherent unitaries and controlled Hadamards. We obtain

$$\chi(U\left|0^n\right\rangle\left|\gamma\right\rangle) \leq 2^k \chi(\left|0^n\right\rangle\left|\gamma\right\rangle) = 2^k r \tag{110}$$

$$\chi(U\left|+^n\right\rangle\left|\gamma\right\rangle) \geq 2^{-k} \chi(\left|+^n\right\rangle\left|\gamma\right\rangle) = 2^{n-k} r. \tag{111}$$

Combining these with Eq. (109) leads to

$$2^{n-k} r \leq 2^{k-n} r, \tag{112}$$

which as the coherence rank $r > 0$ implies that

$$n \leq k \tag{113}$$

as claimed. □

We summarise the implication of the preceding technical result to place it in context with the rest of the paper.

Theorem 23. Given the ability to perform incoherent unitaries and k Hadamards, computational basis measurements and classical control, then even with access to an abritray ancillary state, it is impossible to implement n Hadamards exactly, for $n > k$.

Proof. As discussed above and in Section 2, any operation involving incoherent incoherent unitaries, k Hadamards, computational basis measurements, classical control and access to some ancillary state $\left|\gamma\right\rangle$ can be written as $\rho \mapsto \mathrm{Tr}_2(U\rho \otimes \left|\gamma\right\rangle\!\left\langle\gamma\right| U^\dagger)$, where $U = U_k V_k \dots U_1 V_1 U_0$ alternates between incoherent unitaries U_i and controlled Hadamards V_i (controlled in the general sense of Definition 6). Lemma 22 then directly yields the result. □

4 Discussion and Open Questions

We have introduced a unifying framework for approaches to quantum computation involving operations on some fixed, resourceful state. After studying the role of coherence in this context, we showed that some coherence must be present in the operations. By motivating a general form of the possible channels, we have been able to provide a series of no-go results for incoherent resources being able to implement a unitary channel with increased cohering power, even given an arbitrary ancillary state. This shows that unlike e.g. magic, this resource cannot be placed inside a resourceful state and retrieved; it really has to be in the operations, showing a marked difference to other resources for quantum computation. We now detail some avenues for future work.

4.1 Extending Our Results

Firstly, it would be of value to extend and sharpen our specific results. For example, we did not include the case of using k Hadamards, incoherent resources and an arbitrary ancilla to implement $n > k$ Hadamards *approximately* or *probabilistically*, which involves considering subchannels as in Eq. (21). We leave these questions to ongoing and future work, in order to complete the picture as presented in Table 2.

In the case of using incoherent resources to simulate n Hadamards, we were content to show that approximate implementation is not possible, and we have left the optimality of our bound open. Specifically, we were able to exploit the fact that the corresponding channels commuted with the dephasing map. For channels that use a non-zero amount of coherence (e.g. using $k < n$ Hadamards), one possibility would be to find a similar characterisation, for example, commutation with some channel that only allows a small amount of coherence through.

It would also be interesting to understand if there is any advantage at all to using an ancillary state. We proved a much weaker lower bound (Lemma 19) compared to not using an ancilla at all (Lemma 21), perhaps there is still some advantage to be had here. In this work, we were primarily

concerned with providing lower bounds in order to show no-go results, but do there exist interesting upper bounds? That is, perhaps one could show that using an ancillary state allows for a strictly better approximation to a coherent unitary, compared to the case of no ancilla.

Problem 1. *Improve or show optimality of the bounds presented in this work, and find lower bounds on implementing n Hadamards using k Hadamards, incoherent unitaries, classical control, computational basis measurements, and an arbitrary ancilla.*

4.2 Links with MBQC

Our results concern the circuit model, so it would also be interesting to extend our results to the measurement based scenario. Let us first review some previous works, before commenting on how one could formulate and engage with analogous questions here.

The universality of states for one-way MBQC has been studied in [8, 27], taking LOCC as the free operations. In particular, in [8] they distinguish between four types of universality depending upon whether the input and output considered are classical (**C**) or quantum (**Q**). In this language, a device is considered to be **QQ**-universal if it can implement any unitary operation U, and **CQ**-universal if it can prepare any pure quantum state $|\psi\rangle$. This scenarios are natural when respectively considering the circuit model and the measurement based model (for which the local operations exclude the notion of a quantum input). The authors also discuss the subtleties of efficiency, and of approximate and probabilistic universality in [27].

As **QQ**-universality (quantum inputs and outputs) is concerned with simulation of a unitary channel, it possess a parallel with the gadget-based approach considered in this work. On the other hand, as **CQ**-universality is the appropriate notion for MBQC, there are some intricacies involved, for example one must take into account the dimension of the ancillary state for any meaningful definition. To see this, recall that a ϵ-net is a set of pure quantum states such that *any* pure quantum state is within distance ϵ of some state in the net. Hence, one could encode such an ϵ-net into an ancilla (i.e. take the tensor product of all states in the net). Then by simply tracing out all but one of the subsystems, one could prepare any pure state to within ϵ distance. However the size of any ϵ-net increases rapidly with the dimension of the systems [42, 43], hence this approach is highly impractical and more refined ideas would be needed.

One could extend the definitions in [8, 27] to more general free operations by posing the following question: given some set of allowed operations (e.g. LOCC) does there exists a family of resourceful ancillary states that yield **CQ**-universality? We provide an example of such a definition here, inspired by the aformentioned works.

Definition 24. A family of sets of operations $\{\mathcal{V}_n\}$ is *ϵ-approximate, efficiently* **CQ**-universal, with respect to a distance measure D if:

there exists:	a family of states $\{\|\gamma(n)\rangle\}$, where each $\|\gamma(n)\rangle$ is on at most poly(n) qubits
such that:	for every family of states $\{\|\psi_n\rangle \in (\mathbb{C}^2)^{\otimes n}\}$ obtainable by a uniform family of quantum circuits of depth at most poly(n)
there exist:	maps $\mathcal{E}_n \in \mathcal{V}_n$
such that:	$D\Big(\mathcal{E}_n(\|\gamma(n)\rangle\langle\gamma(n)\|), \|\psi_n\rangle\langle\psi_n\|\Big) \leq \epsilon \quad \forall n.$

One could also consider the probabilistic case, see [27]. For example, the operations LOCC are universal under this definition, as the cluster states serve as the resource state. Similarly, due to the results in [9], the ability to only perform local Hadamard gates (with adaptivity and computational basis measurements) are universal using hypergraph states.

Hence a natural extension of our work to the MBQC framework could be to consider if for *incoherent* LOCC operations there exists a family of resourceful states such that the pair is approximately, efficiently universal. More specifically, one could ask if there exists a family of resource states such that one can achieve efficient, universal quantum computation using only computational

basis measurements (at least two measurement bases may at first seem to be necessary [9], however note that some adaptivity is still possible in the order of systems measured). Furthermore, what would the analogous version of the $k \mapsto n$ question be? Given the ability to perform only k Hadamards (or k X measurements), can one perform universal quantum computation? Again this may translate to the existence of some fixed resourceful state, from which any state could be prepared.

Problem 2. *Is efficient, universal measurement based quantum computation possible with only incoherent resources (for example, using only Z measurements)?*

The above points also raise interesting questions about the relationship between coherence and quantum incompatibility [2, 44]. The latter refers to the fact that not all measurements can be simultaneously performed in quantum theory. For projective measurements, the natural condition is whether the corresponding observables commute (as then a common eigenbasis exists to measure in). For more general POVM measurements, the prevailing notion is to ask for the existence of a so-called *parent* measurement, from which the outcomes of all other measurements can be post-processed[3] [2].

Within our framework, we related the ability to perform in different measurement bases to the unitary that maps between the bases (i.e. in the Heisenberg picture). This could indicate that these resources are equivalent in some way, and perhaps that for any model of universal quantum computation *either* coherence must be present in the operations, or some form of incompatibility must be present in the measurements.

Problem 3. *Are coherence and measurement incompatibility computationally related?*

We also remark that due to existing Hadamard gadgets [15, 29, 30], the ability to measure in the X basis is equivalent to the ability to implement the Hadamard, given the ability to perform incoherent unitaries freely and access to ancillas.

4.3 Resource Theories

Finally, our analysis raises some interesting questions for general resource theories [10], see Appendix A for some background.

For example, [45] studies using maximally incoherent operations (MIOs) to implement arbitrary channels, in terms of the resourcefulness (e.g. coherence rank) of supplementary ancillas. MIOs are exactly the channels that map the set of incoherent states to themselves. It would be interesting to study if this could give rise to a novel model of quantum computation, using MIOs acting on resourceful coherent states. It was also shown in [46] that the coherence distillation capabilities of strictly incoherent operations (SIO) and physically incoherent operations (PIO) are very limited.

Problem 4. *Where else can the "cut" be placed? Are there interesting new models of computation?*

Furthermore, one way of seeing how our result went through is that for the resource theory of coherence, the quantum controlled free unitaries are also free. This is not the case for e.g. magic, as an S gate is Clifford, but a controlled S gate is not Clifford, or for LOCC (e.g. CNOT). This leads to a natural question:

Problem 5. *Are there other resource theories for which taking quantum control of the free operations remains free?*

Our results also hint at a general trade-off between resource generating power and unitarity. Consider a free set of states $\mathcal{F}$ and a resource quantifier Q, and define the resource generating power of a channel $\mathcal{V}$ as $\max_{\rho\in\mathcal{F}} Q(\mathcal{V}(\rho))$. Suppose a channel is of the form

$$\mathcal{E}(\rho) = \mathrm{Tr}_2\left(U\rho \otimes \tau U^\dagger\right) \tag{114}$$

and U has resource generating power α. If the channel $\mathcal{E}$ has resource generating power strictly greater than α, intuitively this might suggest that U is swapping in some of the resource contained

[3] Equivalently, one can consider the commutativity of the Naimark dilation of the measurements.

in τ, and hence $\mathcal{E}$ must be compromising on being unitary. Clearly the total resource content of $\mathcal{E}$ should be somehow upper bounded by the sum of that of U and the state τ. But in order for $\mathcal{E}$ to be unitary, perhaps it cannot use any of the resource contained in τ. See [47] for related work in this direction. The authors provide quantitative relations between resource content, implementation accuracy, and the dimension of the ancillary system, which they show diverges as the implementation accuracy goes to zero.

A similar setup is also considered in [48]. In particular, the authors consider a channel involving free unitaries acting on a resourceful state in order to implement a resourceful channel. They prove a lower bound on the resource content of the ancillary state as a function of the resource content of the target channel, and also apply this result in the context of coherence.

Problem 6. *Are there trade-offs between unitarity and resource generating power?*

In light of this, we note that the style of channels considered in this work seems to hint at a potential new class of resourceful operations. We essentially consider resourceless channels with access to an arbitrarily resourceful state, which does not neatly fit into existing resource theoretic frameworks (see Remark 28 in Appendix A).

4.4 Concluding Remarks

Whist progress has been made in understanding the components required to achieve a super-classical speedup, such as entanglement and magic, there are many exciting research avenues open to explore. The subfield of quantum resource theories has had relatively little intersection with topics in quantum computation, and there may be much to be gain from approaches that attempt to unify the different models of computation, such as gadget or measurement based. It is our hope that through studying characteristic features of quantum theory (such as coherence) on the level of states, channels and measurements, one may hope to gain a more complete understanding of the power of quantum computation.

Data Access Statement

There was no data generated as part of this research.

Acknowledgements

We are extremely grateful to Andreas Winter for pointing out that the previous Lemma 19 could be significantly improved, and for kindly letting us use the new version of the Lemma and his proof.

We also thank members of the Bristol Quantum Information Theory group for helpful discussions. BDMJ acknowledges support from UK EPSRC (EP/S023607/1) . PS is a CIFAR Azrieli Global Scholar in the Quantum Information Science Program, and also acknowledges support from a Royal Society University Research Fellowship (UHQT/NFQI). NL gratefully acknowledges support from the UK Engineering and Physical Sciences Research Council through Grants No. EP/R043957/1, No. EP/S005021/1, and No. EP/T001062/1.

References

[1] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865, 2009. DOI: 10.1103/RevModPhys.81.865.

[2] Otfried Gühne, Erkka Haapasalo, Tristan Kraft, Juha-Pekka Pellonpää, and Roope Uola. Colloquium: Incompatible measurements in quantum information science. *Reviews of Modern Physics*, 95:011003, Feb 2023. DOI: 10.1103/RevModPhys.95.011003.

[3] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[4] Richard Jozsa. An introduction to measurement based quantum computation. *NATO Science Series, III: Computer and Systems Sciences. Quantum Information Processing-From Theory to Experiment*, 199:137–158, 2006. DOI: 10.48550/arXiv.quant-ph/0508124.

[5] Earl T Campbell, Barbara M Terhal, and Christophe Vuillot. Roads towards fault-tolerant universal quantum computation. *Nature*, 549(7671):172–179, 2017. DOI: 10.1038/nature23460.
[6] Tameem Albash and Daniel A Lidar. Adiabatic quantum computation. *Reviews of Modern Physics*, 90(1):015002, 2018. DOI: 10.1103/RevModPhys.90.015002.
[7] Samuel L Braunstein and Peter Van Loock. Quantum information with continuous variables. *Reviews of Modern Physics*, 77(2):513, 2005. DOI: 10.1103/RevModPhys.77.513.
[8] M Van den Nest, W Dür, A Miyake, and HJ Briegel. Fundamentals of universality in one-way quantum computation. *New Journal of Physics*, 9(6):204, 2007. DOI: 10.1088/1367-2630/9/6/204.
[9] Yuki Takeuchi, Tomoyuki Morimae, and Masahito Hayashi. Quantum computational universality of hypergraph states with pauli-x and z basis measurements. *Scientific reports*, 9(1): 1–14, 2019. DOI: 10.1038/s41598-019-49968-3.
[10] Eric Chitambar and Gilad Gour. Quantum resource theories. *Reviews of Modern Physics*, 91 (2):025001, 2019. DOI: 10.1103/RevModPhys.91.025001.
[11] Alexander Streltsov, Gerardo Adesso, and Martin B Plenio. Colloquium: Quantum coherence as a resource. *Reviews of Modern Physics*, 89(4):041003, 2017. DOI: 10.1103/RevModPhys.89.041003.
[12] Khaled Ben Dana, María García Díaz, Mohamed Mejatty, and Andreas Winter. Resource theory of coherence: Beyond states. *Physical Review A*, 95(6):062327, 2017. DOI: 10.1103/PhysRevA.95.062327.
[13] Daniel Gottesman. *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997. DOI: 10.48550/arXiv.quant-ph/9705052.
[14] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5):052328, 2004. DOI: 10.1103/PhysRevA.70.052328.
[15] Richard Jozsa and Marten Van Den Nest. Classical Simulation Complexity of Extended Clifford Circuits. *Quantum Info. Comput.*, 14:633–648, may 2014. ISSN 1533-7146. DOI: 10.26421/QIC14.7-8-7.
[16] Martin Hebenstreit, Richard Jozsa, Barbara Kraus, Sergii Strelchuk, and Mithuna Yoganathan. All pure fermionic non-Gaussian states are magic states for matchgate computations. *Physical Review Letters*, 123(8):080503, 2019. DOI: 10.1103/PhysRevLett.123.080503.
[17] Martin Hebenstreit, Richard Jozsa, Barbara Kraus, and Sergii Strelchuk. Computational power of matchgates with supplementary resources. *Physical Review A*, 102(5):052604, 2020. DOI: 10.1103/PhysRevA.102.052604.
[18] Richard Jozsa and Akimasa Miyake. Matchgates and classical simulation of quantum circuits. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 464 (2100):3089–3106, 2008. DOI: 10.1098/rspa.2008.0189.
[19] Barbara M Terhal and David P DiVincenzo. Classical simulation of noninteracting-fermion quantum circuits. *Physical Review A*, 65(3):032325, 2002. DOI: 10.1103/PhysRevA.65.032325.
[20] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001. DOI: 10.1103/PhysRevLett.86.5188.
[21] Michael A Nielsen. Cluster-state quantum computation. *Reports on Mathematical Physics*, 57(1):147–161, 2006. DOI: 10.1016/S0034-4877(06)80014-5.
[22] Daniel Gottesman and Isaac L Chuang. Quantum teleportation is a universal computational primitive. *arXiv preprint quant-ph/9908010*, 1999. DOI: 10.1038/46503.
[23] Eric Chitambar and Gilad Gour. Critical Examination of Incoherent Operations and a Physically Consistent Resource Theory of Quantum Coherence. *Physical Review Letters*, 117: 030401, Jul 2016. DOI: 10.1103/PhysRevLett.117.030401.
[24] Maarten Van den Nest, Wolfgang Dür, Guifré Vidal, and Hans J Briegel. Classical simulation versus universality in measurement-based quantum computation. *Physical Review A*, 75(1): 012337, 2007. DOI: 10.1103/PhysRevA.75.012337.
[25] M Nest. Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond. *arXiv preprint arXiv:0811.0898*, 2008. DOI: 10.26421/QIC10.3-4-6.
[26] Xiaosi Xu, Simon Benjamin, Jinzhao Sun, Xiao Yuan, and Pan Zhang. A Herculean task: Classical simulation of quantum computers. *arXiv preprint arXiv:2302.08880*, 2023. DOI: 10.48550/arXiv.2302.08880.

[27] Caterina E Mora, Marco Piani, Akimasa Miyake, Maarten Van den Nest, Wolfgang Dür, and Hans J Briegel. Universal resources for approximate and stochastic measurement-based quantum computation. *Physical Review A*, 81(4):042315, 2010. DOI: 10.1103/PhysRevA.81.042315.

[28] Aram W Harrow and Ashley Montanaro. Quantum computational supremacy. *Nature*, 549 (7671):203–209, 2017. DOI: 10.1038/nature23458.

[29] Luke E Heyfron and Earl T Campbell. An efficient quantum compiler that reduces t count. *Quantum Science and Technology*, 4(1):015004, 2018. DOI: 10.1088/2058-9565/aad604.

[30] J. Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang. Fast and Effective Techniques for T-Count Reduction via Spider Nest Identities. In *Theory of Quantum Computation, Communication, and Cryptography*, 2020. DOI: 10.4230/LIPIcs.TQC.2020.11.

[31] Michael J Bremner, Richard Jozsa, and Dan J Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467(2126):459–472, 2011. DOI: 10.1098/rspa.2010.0301.

[32] Matteo Rossi, Marcus Huber, Dagmar Bruß, and Chiara Macchiavello. Quantum hypergraph states. *New Journal of Physics*, 15(11):113022, 2013. DOI: 10.1088/1367-2630/15/11/113022.

[33] Yaoyun Shi. Both Toffoli and Controlled-NOT Need Little Help to Do Universal Quantum Computing. 3(1):84–92, 2003. ISSN 1533-7146. DOI: 10.5555/2011508.2011515.

[34] Dorit Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. *arXiv preprint quant-ph/0301040*, 2003. DOI: 10.48550/arXiv.quant-ph/0301040.

[35] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Physical Review A*, 71(2):022316, 2005. DOI: 10.1103/PhysRevA.71.022316.

[36] Hans J Briegel, David E Browne, Wolfgang Dür, Robert Raussendorf, and Maarten Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, 2009. DOI: 10.1038/nphys1157.

[37] Sergey Bravyi, Graeme Smith, and John A Smolin. Trading classical and quantum computational resources. *Physical Review X*, 6(2):021043, 2016. DOI: 10.1103/PhysRevX.6.021043.

[38] Adriano Barenco, Charles H Bennett, Richard Cleve, David P DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical review A*, 52(5):3457, 1995. DOI: 10.1103/PhysRevA.52.3457.

[39] Nathan Killoran, Frank ES Steinhoff, and Martin B Plenio. Converting nonclassicality into entanglement. *Physical Review Letters*, 116(8):080402, 2016. DOI: 10.1103/PhysRevLett.116.080402.

[40] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013. DOI: 10.1017/9781316809976.

[41] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. DOI: 10.1017/9781316848142.

[42] Patrick Hayden, Debbie Leung, Peter W Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250:371–391, 2004. DOI: 10.1007/s00220-004-1087-6.

[43] Ashley Montanaro. Quantum states cannot be transmitted efficiently classically. *Quantum*, 3:154, 2019. DOI: 10.22331/q-2019-06-28-154.

[44] Teiko Heinosaari, Takayuki Miyadera, and Mário Ziman. An invitation to quantum incompatibility. *Journal of Physics A: Mathematical and Theoretical*, 49(12):123001, 2016. DOI: 10.1088/1751-8113/49/12/123001.

[45] María García Díaz, Kun Fang, Xin Wang, Matteo Rosati, Michalis Skotiniotis, John Calsamiglia, and Andreas Winter. Using and reusing coherence to realize quantum processes. *Quantum*, 2:100, 2018. DOI: 10.22331/q-2018-10-19-100.

[46] Ludovico Lami, Bartosz Regula, and Gerardo Adesso. Generic bound coherence under strictly incoherent operations. *Physical review letters*, 122(15):150402, 2019. DOI: 10.1103/PhysRevLett.122.150402.

[47] Ryuji Takagi and Hiroyasu Tajima. Universal limitations on implementing resourceful unitary evolutions. *Physical Review A*, 101(2):022315, 2020. DOI: 10.1103/PhysRevA.101.022315.

[48] Giulio Chiribella, Yuxiang Yang, and Renato Renner. Fundamental energy requirement of reversible quantum operations. *Physical Review X*, 11(2):021014, 2021. DOI: 10.1103/PhysRevX.11.021014.

[49] Mark Howard and Earl Campbell. Application of a resource theory for magic states to fault-tolerant quantum computing. *Physical Review Letters*, 118(9):090501, 2017. DOI: 10.1103/PhysRevLett.118.090501.
[50] James R Seddon and Earl T Campbell. Quantifying magic for multi-qubit operations. *Proceedings of the Royal Society A*, 475(2227):20190251, 2019. DOI: 10.1098/rspa.2019.0251.
[51] Eric Chitambar and Gilad Gour. Comparison of incoherent operations and measures of coherence. *Physical Review A*, 94(5):052336, 2016. DOI: 10.1103/PhysRevA.94.052336.

A Resource Theories and Coherence

Quantum resource theories [10] are flourishing as an active area of research. The primary goal is to consider unifying principles across different aspects of quantum mechanics that are quintessentially 'quantum'. Specific examples include entanglement [1], coherence [11], magic [49, 50], and incompatibility [2]. There are multiple axiomatic approaches: one can either start with some well-motivated free set of states and define the free channels as those preserving this set, or start with operationally motivated free operations (e.g. LOCC) and define the free states as those which can be generated using free operations alone.

For coherence, the starting point is to fix some particular basis $\{|x\rangle\}$ as "free", and refer to this basis as *incoherent*. These basis states can be thought of as easy to prepare, and in our work we consider them as computational basis states. An incoherent pure state is then equal to a single one of these basis states, and superpositions or coherent states are considered resourceful.

Formally, an arbitrary mixed state ρ is called *incoherent* with respect to the basis $\{|x\rangle\}$ if it can be written as

$$\rho = \sum_x p_x \, |x\rangle\langle x| \,, \tag{115}$$

for some probabilities p_x, i.e. it is diagonal in this basis. Conceptually this consists of all the states that can be written as probabilistic mixtures of computational basis states, with no superposition present. Note that the maximally mixed state $\frac{\mathbb{1}}{d}$ is an example of such an incoherent state (with $p_x = \frac{1}{d} \quad \forall\, x$). We refer to the set of incoherent states as $\mathcal{I}$.

A unitary U is *incoherent* relative to the basis $\{|x\rangle\}_{x=1}^{d}$ if it can be written as

$$U = \sum_{x=1}^{d} e^{i\theta_x} \, |\pi(x)\rangle\langle x| \tag{116}$$

for some string of d real numbers θ_x and some permutation π on d elements. In particular, incoherent unitaries map a computational basis state to another computational basis state, possibly multiplied by some phase. This definition also implies that $U\rho U^\dagger \in \mathcal{I}$ if $\rho \in \mathcal{I}$.

Example 25. Examples of incoherent unitaries include the Pauli matrices, the phase and T gates, CNOT, SWAP, and the Toffoli gate. Examples of unitaries that are coherent (i.e. not incoherent, able to generate coherence) include the Hadamard gate, the Fourier transform, and X rotations $e^{i\theta X}$ for $\theta \notin \{n\pi \;;\; n \in \mathbb{Z}\}$.

Remark 26. Note that if a unitary cannot create any superpositions, then it must be of the form

$$U = \sum_x \alpha_x \, |\pi(x)\rangle\langle x| \tag{117}$$

for some complex numbers α_x. However for this to be unitary, we must have that $|\alpha_x| = 1$ for all x. Hence if a unitary is not of the form Eq. (116), then it must necessarily map at least one computational basis state to a superposition (linear combination) of at least two

computational basis states (i.e. it cannot change the magnitude of a computational basis state).

For a fixed basis $|x\rangle$, the dephasing map is defined as

$$\Delta(\rho) := \sum_x |x\rangle\langle x| \, \rho \, |x\rangle\langle x| \tag{118}$$

this has the effect of removing the off-diagonal elements on a density matrix, and is a valid quantum channel (it is trace-preserving and completely positive).

There are many different approaches to defining a free set of operations in this resource theory, see [11, 51] for summaries. We review several of them here. *Maximally Incoherent Operations* (MIO) map incoherent states to other incoherent states, namely $\mathcal{E}$ is a MIO if $\mathcal{E}(\mathcal{I}) \subseteq \mathcal{I}$.

Lemma 27. A channel Ω maps incoherent states to incoherent states (i.e. is MIO) if and only if $\Delta \circ \Omega \circ \Delta = \Omega \circ \Delta$.

Proof. Note that for all $\rho \in \mathcal{I}$ we have $\Delta(\rho) = \rho$. If Ω maps incoherent states to incoherent states, then we must have $\Omega(\Delta(\rho)) = \Delta(\Omega(\Delta(\rho)))$ for all ρ, which implies $\Delta \circ \Omega \circ \Delta = \Omega \circ \Delta$.

To show the other direction, assume that $\Delta \circ \Omega \circ \Delta = \Omega \circ \Delta$. Then for ρ incoherent, we have $\Omega(\rho) = \Omega(\Delta(\rho)) = \Delta(\Omega(\Delta(\rho)))$, which is incoherent. □

The set of *incoherent operations* (IO) is defined as the set of quantum channels $\mathcal{E}$ which admit a Kraus decomposition $\mathcal{E}(\rho) = \sum_\lambda K_\lambda \; \rho \; K_\lambda^\dagger$ such that $\frac{K_\lambda \rho K_\lambda^\dagger}{\mathrm{Tr}(K_\lambda \rho K_\lambda^\dagger)} \in \mathcal{I}$ for all $\rho \in \mathcal{I}$. This definition means that it is not possible to generate coherence even probabilistically given access to the quantum instrument defined by $\{K_\lambda\}$. This definition is equivalent to being able to write each K_λ in the form $\sum_x \alpha_x \, |\pi(x)\rangle\langle x|$ where the coefficients α_x can be arbitrary complex numbers. If each $K_\lambda^\dagger$ can also be written this way, the corresponding operations are referred to as *strictly incoherent operations* (SIO). We also mention *physically incoherent operations* (PIO), which are channels that can be realised via performing a global incoherent unitary on the input state and some incoherent ancilla, followed by an incoherent measurement and classical processing [23]. Finally, *dephasing-covariant incoherent operations* (DIO) are channels $\mathcal{E}$ which commute with the dephasing map: $\mathcal{E} \circ \Delta = \Delta \circ \mathcal{E}$. We have the following inclusions [23]

$$PIO \subseteq SIO \subseteq DIO \subseteq MIO. \tag{119}$$

Remark 28. We are considering channels of the following form, for U incoherent,

$$\mathcal{E}^x(\rho) = \mathrm{Tr}_X \Big(\mathbb{1} \otimes |x\rangle\langle x| \, U \rho U^\dagger \Big). \tag{120}$$

These fall within the class PIO, but note that channels such as $\rho \mapsto \mathcal{E}^x(\rho \otimes \tau)$ do not, as we can SWAP in the ancillary system (which in our framework could be arbitrarily resourceful).