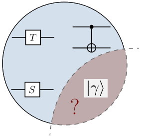
The Hadamard gate cannot be replaced by a resource state in universal quantum computation

Benjamin Jones[1], Paul Skrzypczyk[1] and Noah Linden[1]

[1]University of Bristol, UK.

Quantum Resources, December 2023, Singapore.

arXiv:2312.03515



Overview and Main Contributions

- We consider a general paradigm of quantum computation using resourceful ancillary states.

Overview and Main Contributions

- We consider a general paradigm of quantum computation using resourceful ancillary states.

- We give no-go results on the possibility of implementing Hadamard gates using incoherent unitaries, classical control, Z measurements, and an arbitrary ancilla.

Overview and Main Contributions

- We consider a general paradigm of quantum computation using resourceful ancillary states.

- We give no-go results on the possibility of implementing Hadamard gates using incoherent unitaries, classical control, Z measurements, and an arbitrary ancilla.

- We give evidence that whilst you can siphon off the resource of magic and entanglement in a supplementary state, this does not hold for coherence: i.e. some coherence must be present in the operations.

Overview and Main Contributions

- We consider a general paradigm of quantum computation using resourceful ancillary states.
- We give no-go results on the possibility of implementing Hadamard gates using incoherent unitaries, classical control, Z measurements, and an arbitrary ancilla.
- We give evidence that whilst you can siphon off the resource of magic and entanglement in a supplementary state, this does not hold for coherence: i.e. some coherence must be present in the operations.
- Our technical results relate to the resource theory of coherence.

Overview

1. Motivation
2. Results
3. Outlook

Table of Contents

Clifford + T

- Clifford + T gate set.

Clifford + T

- Clifford + T gate set.

Hadamard

Controlled-NOT

Phase

T

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$$

Clifford + T

- Clifford + T gate set.

Hadamard

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},$$

Controlled-NOT

$$CNOT = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$$

Phase

$$S = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix},$$

T

$$T = \begin{pmatrix}1 & 0\\ 0 & e^{\frac{i\pi}{4}}\end{pmatrix}$$

- Cliffords are classically simulable (Gottesman-Knill theorem).

Clifford + T

- Clifford + T gate set.

Hadamard

Controlled-NOT

Phase

T

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \qquad CNOT = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \qquad S = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}, \qquad T = \begin{pmatrix}1 & 0\\ 0 & e^{\frac{i\pi}{4}}\end{pmatrix}$$

- Cliffords are classically simulable (Gottesman-Knill theorem).
- Anything non-Clifford (e.g. T) is called *magic*.

Clifford + T

- Clifford + T gate set.

Hadamard

Controlled-NOT

Phase

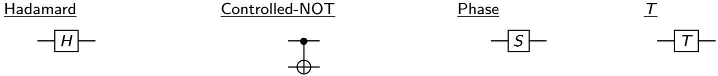
T

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$$

- Cliffords are classically simulable (Gottesman-Knill theorem).
- Anything non-Clifford (e.g. T) is called *magic*.
- $T^2 = S$.

Clifford + T

- Clifford + T gate set.



$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \qquad CNOT = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \qquad S = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}, \qquad T = \begin{pmatrix}1 & 0\\ 0 & e^{\frac{i\pi}{4}}\end{pmatrix}$$

- Cliffords are classically simulable (Gottesman-Knill theorem).
- Anything non-Clifford (e.g. T) is called *magic*.
- $T^2 = S$.
- H, $CNOT$, T respectively provide coherence, entanglement, magic.

Magic State Injection

- Leading error-correction approaches enable fault-tolerant Clifford gates, but not magic gates (e.g. T).

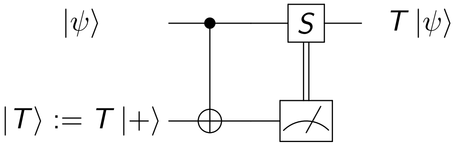
Magic State Injection

- Leading error-correction approaches enable fault-tolerant Clifford gates, but not magic gates (e.g. T).
- Clifford gates and classical control can implement a T gate [1]:

Magic State Injection

- Leading error-correction approaches enable fault-tolerant Clifford gates, but not magic gates (e.g. T).

- Clifford gates and classical control can implement a T gate [1]:

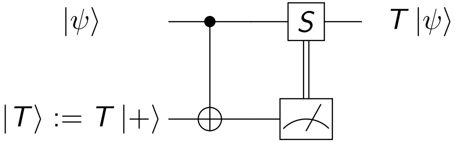


(1)

Magic State Injection

- Leading error-correction approaches enable fault-tolerant Clifford gates, but not magic gates (e.g. T).

- Clifford gates and classical control can implement a T gate [1]:



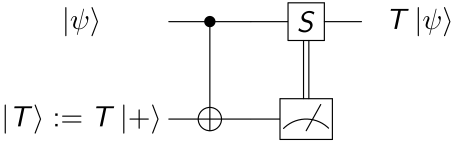
(1)

Hence we can replace each T gate with a T state and the above ‘gadget’.

Magic State Injection

- Leading error-correction approaches enable fault-tolerant Clifford gates, but not magic gates (e.g. T).

- Clifford gates and classical control can implement a T gate [1]:



(1)

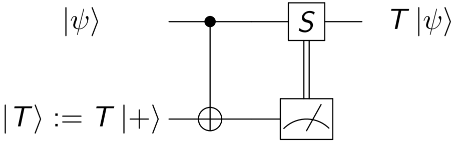
Hence we can replace each T gate with a T state and the above 'gadget'.

Free operations acting on resourceful state.

Magic State Injection

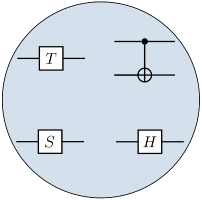
- Leading error-correction approaches enable fault-tolerant Clifford gates, but not magic gates (e.g. T).

- Clifford gates and classical control can implement a T gate [1]:



(1)

Hence we can replace each T gate with a T state and the above 'gadget'.

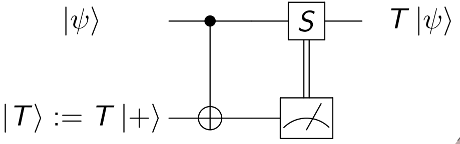


Free operations acting on resourceful state.

Magic State Injection

- Leading error-correction approaches enable fault-tolerant Clifford gates, but not magic gates (e.g. T).

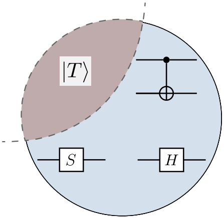
- Clifford gates and classical control can implement a T gate [1]:



(1)

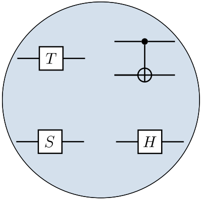
Hence we can replace each T gate with a T state and the above 'gadget'.

Free operations acting on resourceful state.



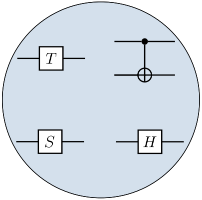
Measurement Based Quantum Computation

What about removing CNOT from Clifford + T?



Measurement Based Quantum Computation

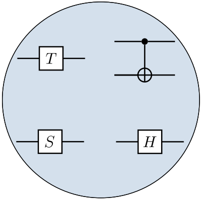
What about removing CNOT from Clifford + T?
- This naturally leads to MBQC.



Measurement Based Quantum Computation

What about removing CNOT from Clifford + T?
- This naturally leads to MBQC.

- MBQC involves performing adaptive local measurements on an entangled resourceful state, e.g a cluster state.

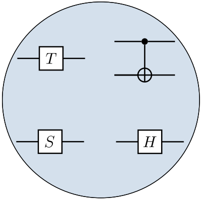


Measurement Based Quantum Computation

What about removing CNOT from Clifford + T?
- This naturally leads to MBQC.

- MBQC involves performing adaptive local measurements on an entangled resourceful state, e.g a cluster state.

- The ability to perform Z measurements and apply H, S and T gates implies ability to measure in the X, Y and $TXT^\dagger$ bases, which is sufficient for universality.



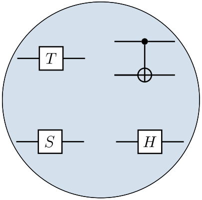
Measurement Based Quantum Computation

What about removing CNOT from Clifford + T?
- This naturally leads to MBQC.

- MBQC involves performing adaptive local measurements on an entangled resourceful state, e.g a cluster state.

- The ability to perform Z measurements and apply H, S and T gates implies ability to measure in the X, Y and $TXT^{\dagger}$ bases, which is sufficient for universality.

- It is also known that MBQC is possible with Z and X measurements on *hypergraph* states [2], one can achieve this with computational basis measurements and Hadamard.



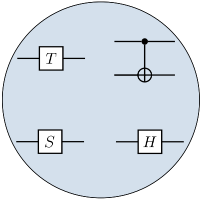
Measurement Based Quantum Computation

What about removing CNOT from Clifford + T?
- This naturally leads to MBQC.

- MBQC involves performing adaptive local measurements on an entangled resourceful state, e.g a cluster state.

- The ability to perform Z measurements and apply H, S and T gates implies ability to measure in the X, Y and $TXT^\dagger$ bases, which is sufficient for universality.

- It is also known that MBQC is possible with Z and X measurements on *hypergraph* states [2], one can achieve this with computational basis measurements and Hadamard.

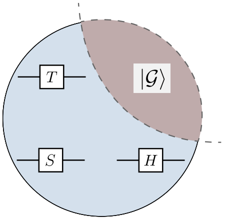


Free operations acting on resourceful state.

Measurement Based Quantum Computation

What about removing CNOT from Clifford + T?
- This naturally leads to MBQC.

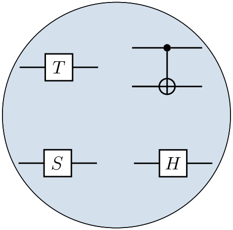
- MBQC involves performing adaptive local measurements on an entangled resourceful state, e.g a cluster state.
- The ability to perform Z measurements and apply H, S and T gates implies ability to measure in the X, Y and $TXT^\dagger$ bases, which is sufficient for universality.
- It is also known that MBQC is possible with Z and X measurements on *hypergraph* states [2], one can achieve this with computational basis measurements and Hadamard.



Free operations acting on resourceful state.

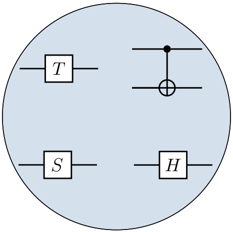
Where can we put the cut?

(a) Universal gate set.

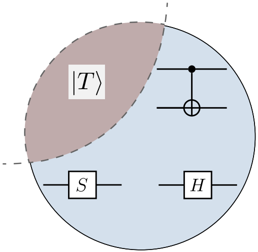


Where can we put the cut?

(a) Universal gate set.

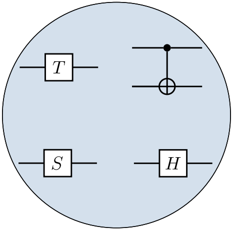


(b) MSI.

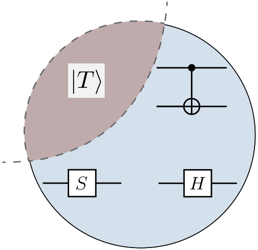


Where can we put the cut?

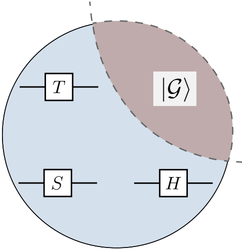
(a) Universal gate set.



(b) MSI.

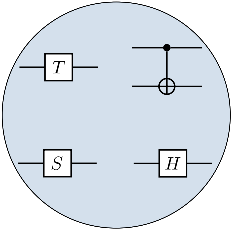


(c) MBQC.

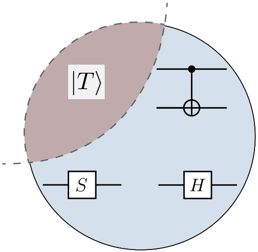


Where can we put the cut?

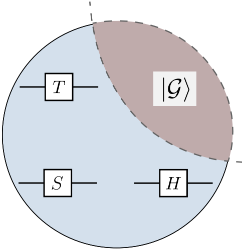
(a) Universal gate set.

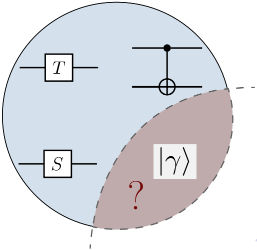


(b) MSI.



(c) MBQC.





(d) This work.

Motivating Questions

- Can we find a unified framework for quantum computation using free operations on resourceful states?

Motivating Questions

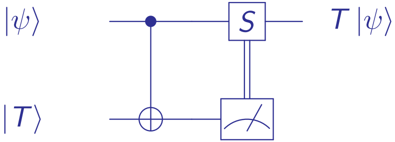
- Can we find a unified framework for quantum computation using free operations on resourceful states?
- Is there an implementation of the Hadamard gate using only CNOT, S and T gates, classical control, computational basis measurements and an ancillary state?

Motivating Questions

- Can we find a unified framework for quantum computation using free operations on resourceful states?
- Is there an implementation of the Hadamard gate using only CNOT, S and T gates, classical control, computational basis measurements and an ancillary state?
- More generally, where can we put the 'cut' between gates and states and still achieve universal quantum computation? We can put all the magic and entanglement in a supplementary state, but what about coherence?

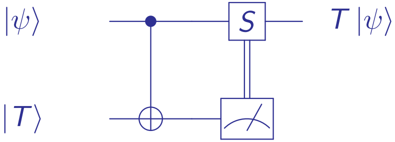
Table of Contents

First ideas: a Hadamard gadget?

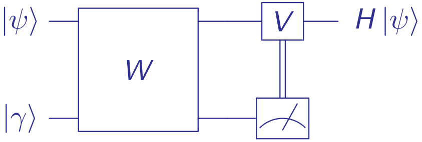


(2)

First ideas: a Hadamard gadget?



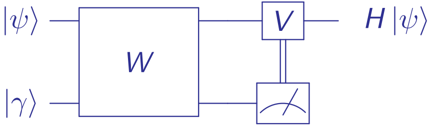
(2)



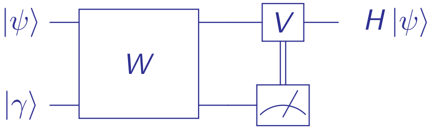
?

(3)

First ideas

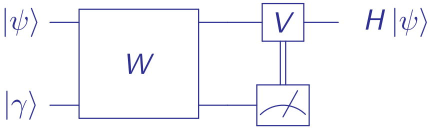


First ideas

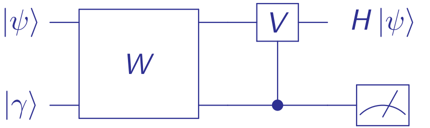


We can replace classical control with quantum control:

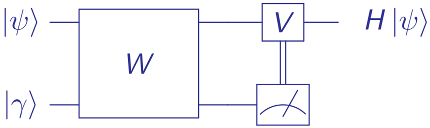
First ideas



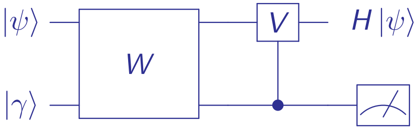
We can replace classical control with quantum control:



First ideas

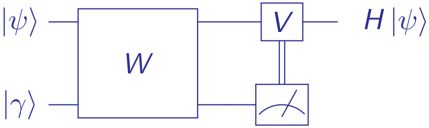


We can replace classical control with quantum control:

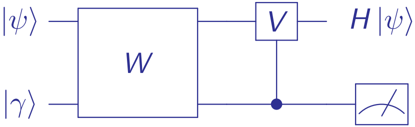


Deterministic implementation corresponds to partial trace:

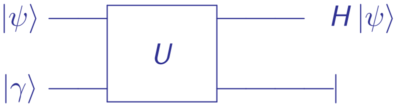
First ideas



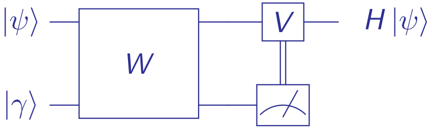
We can replace classical control with quantum control:



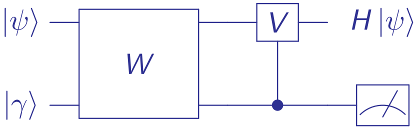
Deterministic implementation corresponds to partial trace:



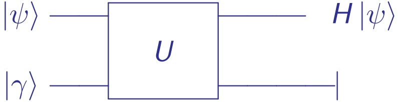
First ideas



We can replace classical control with quantum control:

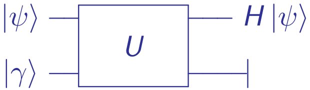


Deterministic implementation corresponds to partial trace:



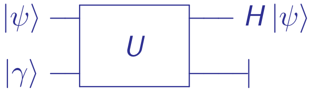
Does there exist a product of (possibly controlled) gates of $CNOT$, T, S for U?

First ideas



(4)

First ideas

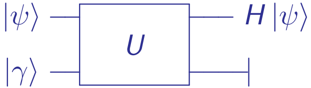


(4)

- CNOT, S and T are all instances of *incoherent unitaries*, i.e. are of the following form for some permutation π and real numbers θ_x.

$$U = \sum_{x=1}^{d} e^{i\theta_x} |\pi(x)\rangle\langle x| \tag{5}$$

First ideas



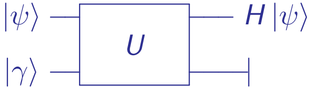
(4)

- CNOT, S and T are all instances of *incoherent unitaries*, i.e. are of the following form for some permutation π and real numbers θ_x.

$$U = \sum_{x=1}^{d} e^{i\theta_x} |\pi(x)\rangle\langle x| \tag{5}$$

- E.g. CNOT, S, T, Toffoli, SWAP, Paulis are all incoherent, but Hadamard, quantum fourier transform are coherent.

First ideas



(4)

- CNOT, S and T are all instances of *incoherent unitaries*, i.e. are of the following form for some permutation π and real numbers θ_x.

$$U = \sum_{x=1}^{d} e^{i\theta_x} |\pi(x)\rangle\langle x| \tag{5}$$

- E.g. CNOT, S, T, Toffoli, SWAP, Paulis are all incoherent, but Hadamard, quantum fourier transform are coherent.

We ask generally if there exists a (controlled) incoherent U and arbitrary state $|\gamma\rangle$ s.t.

$$\mathcal{E}(\rho) = \text{Tr}_2 \left(U\rho \otimes |\gamma\rangle\langle\gamma| \, U^\dagger \right) = H\rho H^\dagger \qquad \forall \rho. \tag{6}$$

Some Preliminaries

Some Preliminaries

- 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:

$$\sum_{x\in S} |x\rangle\langle x| \otimes U + \sum_{y\in S^c} |y\rangle\langle y| \otimes \mathbb{1}, \tag{7}$$

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 $\{0,1\}^{n-k}$.

Some Preliminaries

- 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:

$$\sum_{x\in S} |x\rangle\langle x| \otimes U + \sum_{y\in S^c} |y\rangle\langle y| \otimes \mathbb{1}, \tag{7}$$

  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 $\{0,1\}^{n-k}$.

- Lemma: controlled incoherent unitaries are incoherent.

Some Preliminaries

- 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:

$$\sum_{x\in S} |x\rangle\langle x| \otimes U + \sum_{y\in S^c} |y\rangle\langle y| \otimes \mathbb{1}, \tag{7}$$

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 $\{0,1\}^{n-k}$.

- Lemma: controlled incoherent unitaries are incoherent.

- Incoherent states are $\rho = \sum_x p_x |x\rangle\langle x|$.

Some Preliminaries

- 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:

$$\sum_{x\in S} |x\rangle\langle x| \otimes U + \sum_{y\in S^c} |y\rangle\langle y| \otimes \mathbb{1}, \tag{7}$$

  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 $\{0,1\}^{n-k}$.

- Lemma: controlled incoherent unitaries are incoherent.

- Incoherent states are $\rho = \sum_x p_x |x\rangle\langle x|$.

- The dephasing map is defined as $\Delta(\rho) := \sum_x |x\rangle\langle x| \rho |x\rangle\langle x|$.

A unifying framework

Free operations:

A unifying framework

Free operations:

- Preparation of computational basis states.
- Measurement in the computational basis.
- Classical control and adaptivity.
- Some set of unitaries $\mathcal{U}$.

A unifying framework

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 $|\gamma\rangle$.

A unifying framework

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 $|\gamma\rangle$.

Observation

Most general channel possible to implement deterministically can be written as

$$\mathcal{E}(\rho) = Tr_X\Big(U\ \rho \otimes |\gamma\rangle\langle\gamma|\ U^\dagger\Big). \quad (8)$$

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 $|\gamma\rangle$ is an arbitrary fixed state.

A unifying framework

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 $|\gamma\rangle$.

Observation

Most general channel possible to implement deterministically can be written as

$$\mathcal{E}(\rho) = Tr_X\Big(U \ \rho \otimes |\gamma\rangle\langle\gamma| \ \ U^\dagger \Big). \tag{8}$$

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 $|\gamma\rangle$ is an arbitrary fixed state.

This incorporates lots of examples: MSI, MBQC, matchgates, Pauli-based QC ...

A unifying framework

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 $|\gamma\rangle$.

Observation

Most general channel possible to implement deterministically can be written as

$$\mathcal{E}(\rho) = Tr_X\Big(U\ \rho \otimes |\gamma\rangle\langle\gamma|\ \ U^\dagger\Big). \tag{8}$$

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 $|\gamma\rangle$ is an arbitrary fixed state.

This incorporates lots of examples: MSI, MBQC, matchgates, Pauli-based QC ...
In our case, $\mathcal{U}$ are incoherent unitaries, so $\mathcal{C}(\mathcal{U})$ are also incoherent, and as SWAP is incoherent we can WLOG take the trace over the second system.

Result 1

$$\mathcal{E}(\rho) = \mathrm{Tr}_2\left(U\rho \otimes |\gamma\rangle\langle\gamma|\, U^\dagger\right) \stackrel{?}{=} H\rho H^\dagger \qquad \forall\rho \tag{9}$$

Result 1

$$\mathcal{E}(\rho) = \mathrm{Tr}_2\left(U\rho \otimes |\gamma\rangle\langle\gamma|\, U^\dagger\right) \stackrel{?}{=} H\rho H^\dagger \qquad \forall\rho \tag{9}$$

Lemma (See erratum of [3])

Erratum: Resource theory of coherence: Beyond states [Phys. Rev. A **95**, 062327 (2017)]

Khaled Ben Dana, María García Díaz, Mohamed Mejatty, and Andreas Winter
Phys. Rev. A **96**, 059903 – Published 9 November 2017

Result 1

$$\mathcal{E}(\rho) = \mathrm{Tr}_2\left(U\rho \otimes |\gamma\rangle\langle\gamma|\, U^\dagger\right) \stackrel{?}{=} H\rho H^\dagger \qquad \forall\rho \tag{9}$$

Lemma (See erratum of [3])

Erratum: Resource theory of coherence: Beyond states [Phys. Rev. A **95**, 062327 (2017)]
Khaled Ben Dana, María García Díaz, Mohamed Mejatty, and Andreas Winter
Phys. Rev. A **96**, 059903 – Published 9 November 2017

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 $\Delta \circ \mathcal{E} \circ \Delta = \Delta \circ \mathcal{E}$. 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.

Result 1

$$\mathcal{E}(\rho) = \mathrm{Tr}_2\left(U\rho\otimes|\gamma\rangle\langle\gamma|\,U^\dagger\right) \overset{?}{=} H\rho H^\dagger \qquad \forall\rho \tag{9}$$

Lemma (See erratum of [3])

Erratum: Resource theory of coherence: Beyond states [Phys. Rev. A **95**, 062327 (2017)]
Khaled Ben Dana, María García Díaz, Mohamed Mejatty, and Andreas Winter
Phys. Rev. A **96**, 059903 – Published 9 November 2017

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 $\Delta\circ\mathcal{E}\circ\Delta=\Delta\circ\mathcal{E}$. 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.

Theorem

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, even when supplemented with an arbitrary ancilla.

Result 2: Approximate Case

Result 2: Approximate Case

Lemma

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*

$$\mathcal{E} \circ \Delta = \Delta \circ \mathcal{E}, \tag{10}$$

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*

$$\mathcal{D}\left(\mathcal{E}_\tau \ , \ H^{\otimes n}\right) \geq \frac{1}{2}\left(1 - \frac{1}{2^n}\right). \tag{11}$$

Result 2: Approximate Case

Lemma

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*

$$\mathcal{E} \circ \Delta = \Delta \circ \mathcal{E}, \tag{10}$$

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*

$$\mathcal{D}\left(\mathcal{E}_\tau \ , \ H^{\otimes n}\right) \geq \frac{1}{2}\left(1 - \frac{1}{2^n}\right). \tag{11}$$

Theorem

Given the ability to perform incoherent unitaries, computational basis measurements and classical control, it is impossible to implement a single Hadamard to within induced trace distance of $\frac{1}{4}$.

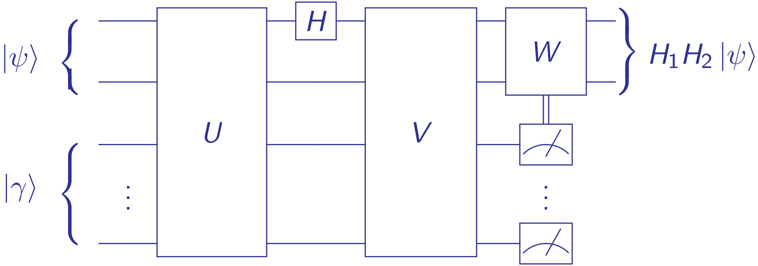
Extensions

Perhaps the above results were a special case, could we use an ancilla and a single Hadamard to implement 2 Hadamards?

Extensions

Perhaps the above results were a special case, could we use an ancilla and a single Hadamard to implement 2 Hadamards?

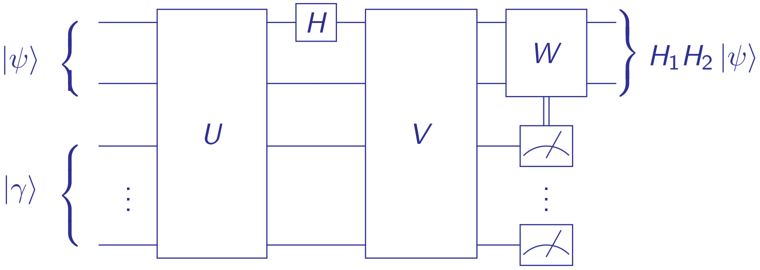
i.e. what about circuits of the following form, for U, V, W incoherent:



Extensions

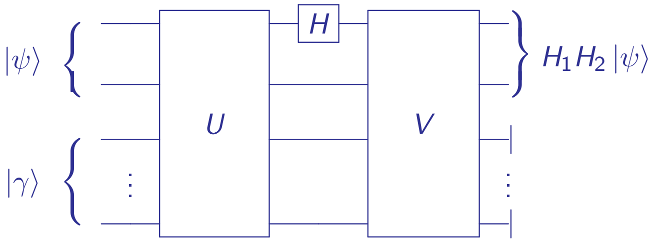
Perhaps the above results were a special case, could we use an ancilla and a single Hadamard to implement 2 Hadamards?

i.e. what about circuits of the following form, for U, V, W incoherent:



Again we could write this as . . .

Extension to k Hadamards



$$VH_1 U |\psi\rangle |\gamma\rangle = H_1 H_2 |\psi\rangle |\gamma_\psi\rangle \quad (12)$$

For incoherent U and V, and some $|\gamma_\psi\rangle$ that could a priori depend on $|\psi\rangle$.

Extension to k Hadamards

Suppose that

$$VH_1 U |\psi\rangle |\gamma\rangle = H_1 H_2 |\psi\rangle |\gamma_\psi\rangle \tag{13}$$

Extension to k Hadamards

Suppose that

$$VH_1 U |\psi\rangle |\gamma\rangle = H_1 H_2 |\psi\rangle |\gamma_\psi\rangle \tag{13}$$

- $|\gamma_\psi\rangle \equiv |\gamma'\rangle$ must be independent of ψ - from a no-cloning type argument.

Extension to *k* Hadamards

Suppose that

$$VH_1 U |\psi\rangle |\gamma\rangle = H_1 H_2 |\psi\rangle |\gamma_\psi\rangle \tag{13}$$

- $|\gamma_\psi\rangle \equiv |\gamma'\rangle$ must be independent of ψ - from a no-cloning type argument.
- So we have

$$VH_1 U |\psi\rangle |\gamma\rangle = H_1 H_2 |\psi\rangle \left|\gamma'\right\rangle \tag{14}$$

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

Extension to k Hadamards

Suppose that

$$VH_1 U |\psi\rangle |\gamma\rangle = H_1 H_2 |\psi\rangle |\gamma_\psi\rangle \quad (13)$$

- $|\gamma_\psi\rangle \equiv |\gamma'\rangle$ must be independent of ψ - from a no-cloning type argument.
- So we have

  $$VH_1 U |\psi\rangle |\gamma\rangle = H_1 H_2 |\psi\rangle |\gamma'\rangle \quad (14)$$

  for some state $|\gamma'\rangle$.
- We now need to introduce the coherence rank.

Coherence Rank

Coherence Rank

Definition

The *coherence rank* [4] 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 $\chi(|\psi\rangle)$.

Coherence Rank

Definition

The *coherence rank* [4] 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 $\chi(|\psi\rangle)$.

- E.g. $\chi(|x\rangle) = 1$ for any computational basis state $|x\rangle$, and $\chi(|+\rangle^{\otimes n}) = 2^n$. We also have that $\chi(|\psi\rangle \otimes |\phi\rangle) = \chi(|\psi\rangle)\chi(|\phi\rangle)$.

Coherence Rank

Definition

The *coherence rank* [4] 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 $\chi(|\psi\rangle)$.

- E.g. $\chi(|x\rangle) = 1$ for any computational basis state $|x\rangle$, and $\chi(|+\rangle^{\otimes n}) = 2^n$. We also have that $\chi(|\psi\rangle \otimes |\phi\rangle) = \chi(|\psi\rangle)\chi(|\phi\rangle)$.
- By inputting $|\psi\rangle \in \{|00\rangle, |{++}\rangle\}$ we get a contradiction in terms of the coherence rank of both sides of the equation.

Coherence Rank

Definition

The *coherence rank* [4] 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 $\chi(|\psi\rangle)$.

- E.g. $\chi(|x\rangle) = 1$ for any computational basis state $|x\rangle$, and $\chi(|+\rangle^{\otimes n}) = 2^n$. We also have that $\chi(|\psi\rangle \otimes |\phi\rangle) = \chi(|\psi\rangle)\chi(|\phi\rangle)$.
- By inputting $|\psi\rangle \in \{|00\rangle, |{+}{+}\rangle\}$ we get a contradiction in terms of the coherence rank of both sides of the equation.

$$VH_1 U |\psi\rangle |\gamma\rangle = H_1 H_2 |\psi\rangle |\gamma'\rangle \qquad (15)$$

Coherence Rank

Definition

The *coherence rank* [4] 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 $\chi(|\psi\rangle)$.

- E.g. $\chi(|x\rangle) = 1$ for any computational basis state $|x\rangle$, and $\chi(|+\rangle^{\otimes n}) = 2^n$. We also have that $\chi(|\psi\rangle \otimes |\phi\rangle) = \chi(|\psi\rangle)\chi(|\phi\rangle)$.
- By inputting $|\psi\rangle \in \{|00\rangle, |{+}{+}\rangle\}$ we get a contradiction in terms of the coherence rank of both sides of the equation.

$$VH_1U|\psi\rangle|\gamma\rangle = H_1H_2|\psi\rangle|\gamma'\rangle \tag{15}$$

$$VH_1U|00\rangle|\gamma\rangle = |{+}{+}\rangle|\gamma'\rangle \tag{16}$$

$$VH_1U|{+}{+}\rangle|\gamma\rangle = |00\rangle|\gamma'\rangle . \tag{17}$$

Bounding the coherence rank

$$VH_1 U |00\rangle |\gamma\rangle = |{+}{+}\rangle |\gamma'\rangle \tag{18}$$

$$VH_1 U |{+}{+}\rangle |\gamma\rangle = |00\rangle |\gamma'\rangle . \tag{19}$$

Bounding the coherence rank

$$VH_1 U |00\rangle |\gamma\rangle = |{+}{+}\rangle |\gamma'\rangle \quad (18)$$

$$VH_1 U |{+}{+}\rangle |\gamma\rangle = |00\rangle |\gamma'\rangle . \quad (19)$$

Lemma: $VH_1 U$ can at most (least) double (halve) the coherence rank.

Bounding the coherence rank

$$VH_1 U |00\rangle |\gamma\rangle = |{+}{+}\rangle |\gamma'\rangle \tag{18}$$

$$VH_1 U |{+}{+}\rangle |\gamma\rangle = |00\rangle |\gamma'\rangle . \tag{19}$$

Lemma: $VH_1 U$ can at most (least) double (halve) the coherence rank.

Letting $r := \chi(|\gamma\rangle)$ and $r' := \chi(|\gamma'\rangle)$, the above equations then imply

Bounding the coherence rank

$$VH_1 U |00\rangle |\gamma\rangle = |{+}{+}\rangle |\gamma'\rangle \tag{18}$$
$$VH_1 U |{+}{+}\rangle |\gamma\rangle = |00\rangle |\gamma'\rangle . \tag{19}$$

Lemma: $VH_1 U$ can at most (least) double (halve) the coherence rank.

Letting $r := \chi(|\gamma\rangle)$ and $r' := \chi(|\gamma'\rangle)$, the above equations then imply

$$4r' \in [\frac{r}{2}, 2r] \tag{20}$$

Bounding the coherence rank

$$VH_1 U |00\rangle |\gamma\rangle = |{+}{+}\rangle |\gamma'\rangle \tag{18}$$
$$VH_1 U |{+}{+}\rangle |\gamma\rangle = |00\rangle |\gamma'\rangle . \tag{19}$$

Lemma: $VH_1 U$ can at most (least) double (halve) the coherence rank.

Letting $r := \chi(|\gamma\rangle)$ and $r' := \chi(|\gamma'\rangle)$, the above equations then imply

$$4r' \in [\frac{r}{2}, 2r] \tag{20}$$
$$r' \in [2r, 8r] \quad \Longrightarrow \; 4r' \in [8r, 32r],$$

Bounding the coherence rank

$$VH_1U|00\rangle|\gamma\rangle = |{++}\rangle|\gamma'\rangle \tag{18}$$
$$VH_1U|{++}\rangle|\gamma\rangle = |00\rangle|\gamma'\rangle\,. \tag{19}$$

Lemma: VH_1U can at most (least) double (halve) the coherence rank.

Letting $r := \chi(|\gamma\rangle)$ and $r' := \chi(|\gamma'\rangle)$, the above equations then imply

$$4r' \in [\frac{r}{2}, 2r] \tag{20}$$
$$r' \in [2r, 8r] \quad \implies 4r' \in [8r, 32r], \tag{21}$$

which is a contradiction (as $r \geq 1$).

Result 3

Result 3

Lemma

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

$$Tr_2 \left(U\rho \otimes |\gamma\rangle\langle\gamma| \, U^\dagger \right) = H^{\otimes n} \rho H^{\otimes n} \qquad \forall \rho, \tag{22}$$

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

Result 3

Lemma

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*

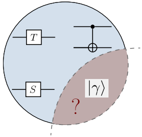
$$Tr_2\left(U\rho \otimes |\gamma\rangle\langle\gamma|\, U^\dagger\right) = H^{\otimes n}\rho H^{\otimes n} \qquad \forall\rho, \tag{22}$$

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

Theorem

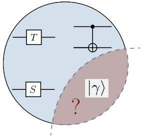
Given the ability to perform incoherent unitaries and k *Hadamards, computational basis measurements, classical control, and access to an arbitrary ancilla, it is impossible to implement* n *Hadamards exactly for* $n > k$*.*

Summary



- We have shown that you cannot replace the Hadamard gate with a resourceful state in Clifford + T.

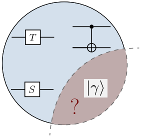
Summary



- We have shown that you cannot replace the Hadamard gate with a resourceful state in Clifford + T.

- We have argued that some coherence must be present in the operations for universal quantum computation.

Summary

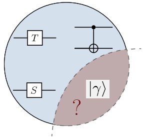


- We have shown that you cannot replace the Hadamard gate with a resourceful state in Clifford + T.

- We have argued that some coherence must be present in the operations for universal quantum computation.

- This is in direct contrast with the resources of magic and entanglement!

Summary



- We have shown that you cannot replace the Hadamard gate with a resourceful state in Clifford + T.

- We have argued that some coherence must be present in the operations for universal quantum computation.

- This is in direct contrast with the resources of magic and entanglement!

- Our proofs went via the resource theory of coherence.

Table of Contents

Future Directions

Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.

Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.
- Incorporate MBQC:

Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.
- Incorporate MBQC:
  - Universality in circuit model: implementing any unitary, Universality in MBQC: preparing any state [5].

Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.
- Incorporate MBQC:
  - Universality in circuit model: implementing any unitary,
    Universality in MBQC: preparing any state [5].
    Need to take dimension of ancilla into account.

Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.
- Incorporate MBQC:
  - Universality in circuit model: implementing any unitary,
    Universality in MBQC: preparing any state [5].
    Need to take dimension of ancilla into account.
  - Connection between coherence and measurement incompatibility?
    i.e. Hadamard vs X and Z measurements.

Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.

- Incorporate MBQC:
  - Universality in circuit model: implementing any unitary,
    Universality in MBQC: preparing any state [5].
    Need to take dimension of ancilla into account.
  - Connection between coherence and measurement incompatibility?
    i.e. Hadamard vs X and Z measurements.

- General resource theories:

Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.

- Incorporate MBQC:
    - Universality in circuit model: implementing any unitary,
      Universality in MBQC: preparing any state [5].
      Need to take dimension of ancilla into account.
    - Connection between coherence and measurement incompatibility?
      i.e. Hadamard vs X and Z measurements.

- General resource theories:
    - Classical control vs quantum control.

Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.
- Incorporate MBQC:
  - Universality in circuit model: implementing any unitary,
    Universality in MBQC: preparing any state [5].
    Need to take dimension of ancilla into account.
  - Connection between coherence and measurement incompatibility?
    i.e. Hadamard vs X and Z measurements.
- General resource theories:
  - Classical control vs quantum control.
  - Trade-off between unitarity and resource generating power.

Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.

- Incorporate MBQC:
  - Universality in circuit model: implementing any unitary,
    Universality in MBQC: preparing any state [5].
    Need to take dimension of ancilla into account.
  - Connection between coherence and measurement incompatibility?
    i.e. Hadamard vs X and Z measurements.

- General resource theories:
  - Classical control vs quantum control. $\mathcal{E}(\rho) = \mathrm{Tr}_2\left(U\rho \otimes |\gamma\rangle\langle\gamma|\, U^\dagger\right)$
  - Trade-off between unitarity and resource generating power.

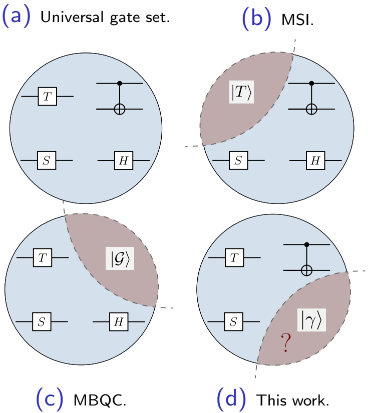
Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.
- Incorporate MBQC:
  - Universality in circuit model: implementing any unitary,
    Universality in MBQC: preparing any state [5].
    Need to take dimension of ancilla into account.
  - Connection between coherence and measurement incompatibility?
    i.e. Hadamard vs X and Z measurements.
- General resource theories:
  - Classical control vs quantum control. $\mathcal{E}(\rho) = \mathrm{Tr}_2\left(U\rho \otimes |\gamma\rangle\langle\gamma|\, U^\dagger\right)$
  - Trade-off between unitarity and resource generating power.
  - Resource injection: boosting the resource content of channels using resourceful states.

Future Directions

- Completing our analysis, approximate bounds on the $k \mapsto n$ case.
- Incorporate MBQC:
  - Universality in circuit model: implementing any unitary,
    Universality in MBQC: preparing any state [5].
    Need to take dimension of ancilla into account.
  - Connection between coherence and measurement incompatibility?
    i.e. Hadamard vs X and Z measurements.
- General resource theories:
  - Classical control vs quantum control. $\mathcal{E}(\rho) = \mathrm{Tr}_2 \left(U \rho \otimes |\gamma\rangle\langle\gamma| \, U^\dagger \right)$
  - Trade-off between unitarity and resource generating power.
  - Resource injection: boosting the resource content of channels using resourceful states.
  - Quantum resources in quantum computation: which resources can be siphoned off to states? Which must remain present in the operations?

Thanks!



[1] Earl T Campbell, Barbara M Terhal, and Christophe Vuillot. "Roads towards fault-tolerant universal quantum computation". In: *Nature* 549.7671 (2017), pp. 172–179.

[2] Yuki Takeuchi, Tomoyuki Morimae, and Masahito Hayashi. "Quantum computational universality of hypergraph states with Pauli-X and Z basis measurements". In: *Scientific reports* 9.1 (2019), pp. 1–14.

[3] Khaled Ben Dana et al. "Resource theory of coherence: Beyond states". In: *Physical Review A* 95.6 (2017), p. 062327.

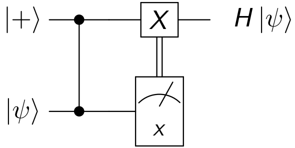
[4] Alexander Streltsov, Gerardo Adesso, and Martin B Plenio. "Colloquium: Quantum coherence as a resource". In: *Reviews of Modern Physics* 89.4 (2017), p. 041003.

[5] M Van den Nest et al. "Fundamentals of universality in one-way quantum computation". In: *New Journal of Physics* 9.6 (2007), p. 204.

arXiv:2312.03515

Hadamard Gadgets

So-called Hadamard gadgets are known to exist, e.g.:



(23)

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