Author:
Jones, Benjamin D M

Title:
Contemporary Quantum Resources

Steering, Incompatibility, Coherence and Entanglement.

Contemporary Quantum Resources:

Steering, Incompatibility, Coherence and Entanglement.

By

Benjamin David Merga Jones

Department of Physics
University of Bristol

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of Doctor of Philosophy in the Faculty of Science.

12th April 2024

Word count: 32,115.

Abstract

Quantum information science is a flourishing field of research, despite its relative nascency. A helpful perspective is to focus on specific features and properties of quantum mechanics, and consider their role as resources for certain scenarios or tasks.

In this thesis, we introduce several novel concepts and definitions by building on ideas present in the existing literature. Specifically we explore research questions relating to quantum steering, measurement incompatibility, coherence, and aspects of entanglement (such as high-dimensionality and the multipartite scenario).

Firstly in Chapter 2, taking inspiration from quantum nonlocality in networks, we consider allowing some of the parties to be trusted, which leads us to a natural notion of quantum network steering. We are able to characterise several scenarios for which only classical correlations can arise, and we also provide examples of when network steering can be exhibited, including an example that appears unique to networks and does not rely on existing steering results.

In Chapter 3, we introduce a notion of dimensionality for sets of quantum measurements, which can also be understood as a form of compression, or as a kind of Schmidt number for measurement incompatibility. We discuss and prove several links to high-dimensional quantum steering, and provide connections between several interesting channels and states via channel-state duality.

We then change gears somewhat, and in Chapter 4 we consider the role of coherence in gadget-based approaches to quantum computation. We construct a general framework for quantum computation involving ‘free’ operations acting on some resourceful state, and prove a no-go result, stating that some coherence must be present in the operations to achieve computational universality: one cannot place this resource in a supplementary state.

Finally, in Chapter 5 we prove a lower bound on the number of copies needed to determine whether a pure multipartite quantum state is either product across some bipartition, or is far away from having this property. Our lower bound is tight compared to known upper bounds up to a logarithmic factor.

In a broad sense, this thesis aims to display the power of quantum resources and to unearth interesting connections between seemingly different notions in quantum information science. The results presented serve as a testament to the variety and richness of research in this field, and expose the exciting realm of future research topics and questions to explore.

Dedication and acknowledgements

I have been extremely fortunate during my PhD, and I am grateful to so many people.

First of all, I extend my deepest thanks to my primary supervisor Paul Skrzypczyk. It has been an immense privilege to learn from and collaborate with such a wonderful researcher and person. I am particularly grateful for your willingness to encourage and support me to pursue my own interests and ideas, and for many pleasant hours spent at the pub, lunchtimes, and summer barbecues.

I am also very grateful to Noah Linden, my second supervisor. I am very thankful for the opportunity to have worked with you on our Hadamard project with Paul, and also for supporting me in having a desk in the Maths building.

Thirdly, I would like to thank Ashley Montanaro. I have thoroughly enjoyed my internship and consultancy work with Phasecraft, and have been immensely grateful for the opportunity. Thank you also for your willingness to undertake a project with me at the university, which I have immensely enjoyed and learnt a great deal from.

Thank you to everyone at the Quantum Engineering Centre for Doctoral Training in Bristol. In particular, I would like to thank the staff for creating a wonderfully warm and friendly environment, and for supporting me throughout my PhD research phase, as well as hosting several writing retreats and fun trips away – special thanks to Sorrel Johnson and Lin Burden. Thank you also to all the members of my cohort (Cohort 6) for being lovely people to have gone through the CDT process with, and in particular for some wonderful memories in our first year.

Being part of the Quantum Information Theory group in Bristol has been an immense privilege. I have loved being part of a research group with such a broad range of interests, yet also a shared desire for academic discussion and collaboration. The stimulating seminars, weekly pub trips, and Christmas parties have all been highlights of my time in Bristol. I have learnt a great deal from post-docs in the group (in particular Ryan Mann and Chung-Yun Hsieh), and I extend particular thanks to Jan Lukas Bosse too: we have gone through our PhDs on a similar timescale and I've been very grateful for our academic brainstorming and friendship. Thank you also to all the permanent members of staff for fostering a healthy and fruitful research environment: Paul Skrzypczyk, Noah Linden, Ashley Montanaro, Nikolas Breuckmann, Tony Short, and Sandu Popescu. I am also thankful to Tony and Sandu for helpful annual progress meetings.

I am also immensely grateful for the interactions I have had with the research group of Nicolas Brunner in Geneva throughout my PhD, which formed the basis of three of my publications. Thank you for hosting me for several months during the pandemic. I would also like to thank Roope Uola in particular for teaching me a great deal in the early stages of my PhD, for many enjoyable whiteboard discussions, and for some tense games of snooker on his visits to Bristol.

My deepest thanks to EPSRC and UK tax payers for funding my PhD, and allowing me to spend my time thinking about maths, physics, computer science, and the quantum world.

I would also like to acknowledge many special friends over the last few years of my life who have supported me and indeed encouraged me to pursue a PhD in the first place. I won't name everyone here, but please know that I am deeply grateful.

Finally, and most importantly, I thank my family. I would never have been able to pursue my academic ambitions without their continued love, support, and never-ending banter. Thank you so much Mum, Dad, Rob, Emma, Beth and Sam.

Author's declaration

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: DATE: 12th April 2024

Table of Contents

Page

List of Tables

List of Figures

Figure **Page**

CHAPTER 1

Introduction

Page

Contents

1.1 Background

1.1.1 History and significance of the field

Humans are always seeking to discover. To learn new skills, and uncover seemingly objective truths. Our insatiable quest for knowledge is matched only by our continued ignorance: the more we know, the more we realise how little we know. One can view the realm of science as a whole as the quest to reveal some objective reality: be it the precise mechanism by which plants convert energy, or the expected properties of a given material, or the fundamental limits on feasible computation in our universe.

Quantum information science arrives at the intersection of several fields: primarily physics and computer science, heavily relying on the mathematical language and formalisms underpinning these domains. It is a marriage between the strange and counter-intuitive world of quantum mechanics, and deep ideas about how to quantify and communicate information, and what it means to compute efficiently.

The first quantum revolution: quantum theory is weird!

Quantum theory emerged in the former half of the 20th century as a formalism for explaining several physical phenomena that classical physics could not. The photoelectric effect demonstrated that light is composed of discrete packets of energy (photons), and the Stern-Gerlach experiment similarly showed that angular momentum is quantised (spin). The double slit experiment provided evidence that matter can can behave like a wave or a particle - apparently depending on whether or not one is observing!

Ultimately, one way of summarising the ‘weirdness’ of quantum theory is as follows: *it seems like the act of measurement cannot be thought of as simply revealing pre-existing values*. Indeed, the standard axioms of quantum theory (see Section 1.3) both allow for objects to be in an indefinite state (superposition), and for the act of measurement to fundamentally change the object itself (wave-function collapse). There are many different interpretations of quantum mechanics, such as Many Worlds, Qbism, Bohmian mechanics, and Superdeterminism [1, 2].

A crucial topic in the realm of quantum foundations is that of Bell nonlocality [3] – see Section 1.4.4 for some technical background. The significance of quantum nonlocality is that by exploring the correlations between two separated parties, we can experimentally distinguish between the predictions of quantum theory, and a universe which obeys *local realism*, that is, the parties must generate their results independently of the other parties choice of measurement, and that objects have well-defined properties independent of measurement. One finds that quantum theory prevails, and the various interpretations strive to make this weirdness more palatable, but cannot eradicate it completely.

The second quantum revolution: the weirdness can be useful!

Claude Shannon introduced the entropy of a probability distribution p as [4]

$$S(p) = -\sum_x p(x) \log_2 p(x), \tag{1.1}$$

which quantifies how uncertain of the outcome you would be when sampling from p. Shannon also introduced two landmark coding theorems, which quantify the amount of information that can be sent through channels under certain assumptions.

Quantum information theory seeks to extend these notions of quantifying information to quantum systems. Here a two-level quantum system (a qubit) plays the analogous role of a bit, and one can extend the Shannon entropy to the so-called Von Neumann entropy of a quantum states ρ as [5]

$$S(\rho) = -\mathrm{Tr}\Big(\rho \log_2 \rho\Big). \tag{1.2}$$

One can then aim to translate the machinery of classical information theory into the quantum setting, such as through the quantum analogues of the coding theorems [6]. As quantum states can encode classical information as a special case, this subfield as a whole can be seen as a generalisation of classical information theory.

The field of quantum cryptography [7] essentially builds upon the facts that a quantum measurement typically disturbs the system, and that it is impossible to perfectly copy an unknown quantum state [8, 9]. These properties can allow two parties to have an high degree of confidence about the security of their shared channel, and they can place their trust in the correctness of quantum theory, as opposed to the computational hardness of a given problem (which could be efficiently solved at some point in the future).

Quantum computation explores the potential for quantum mechanics to provide improved algorithms (i.e. requiring less resources, such as space or time) compared to the best possible approaches using classical computers. Intuitively, quantum algorithms are able to exploit the property of superposition to compute in parallel, with the crucial caveat being that upon measurement only one outcome is seen. Two of the landmark algorithms in quantum computation are attributed to Shor and Grover, which respectively show an exponential and square root speed up compared to the best known classical approaches. There is now a wealth of known quantum algorithms [10, 11], and much research continues both from the fundamental perspective of theoretical computer science, as well as a practical drive for quantum computers to be useful in the near-term (for example in problems relating to quantum chemistry [12]), in the wake of recent quantum computational supremacy experiments [13, 14]. In a recent survey of 37 experts, the majority indicated that they believed it was more than 50% likely that a quantum computer would exist within the next 15 years that was capable of breaking the RSA-2048 cryptosystem within 24 hours [15].

Outlook.

The field of quantum information is still extremely young. It is a field where progress typically involves combining existing concepts from physics and computer science, and reframing ideas about information, communication and computation in the language of quantum mechanics to unearth an advantage for some task. Foundational work (such as in the realm of quantum nonlocality) is critical as it informs our collective knowledge of the universe we live in. At the same time, there is tremendous potential for quantum technologies to significantly improve society – through more secure communication, faster algorithms, or indeed answers to problems that would be completely unattainable even with classical supercomputers.

1.1.2 What is this thesis about?

One unifying theme throughout this thesis relates to introducing new concepts and definitions, and then providing initial insights and results from this novel viewpoint. The remainder of this chapter provides an informal recap of linear algebra, quantum mechanics, and some miscellaneous concepts in quantum information that will be relevant for the rest of this thesis.

In Chapter 2, we combine the concepts of quantum steering and network nonlocality to introduce *network quantum steering*. This is a novel definition, and serves to indicate when a network composed of trusted and untrusted parties is exhibiting genuinely quantum behaviour. In addition to introducing this new definition, our contributions include studying which quantum states are necessary and sufficient for the parties to share in order to witness genuinely quantum network correlations. This chapter is based on the following paper [16]:

Benjamin DM Jones, Ivan Šupić, Roope Uola, Nicolas Brunner, and Paul Skrzypczyk.
Network Quantum Steering.
Physical Review Letters, 127(17):170405, 2021.

In Chapter 3, we introduce a new notion of compression for a set of measurements, and show multiple connections with quantum steering. This definition can also be thought of as a kind of Schmidt number, or quantifier of dimensionality, for measurement incompatibility. Chapter 3 is based on the following two companion papers [17, 18], but mainly drawing from the former:

Benjamin DM Jones, Roope Uola, Thomas Cope, Marie Ioannou,
Sébastien Designolle, Pavel Sekatski, and Nicolas Brunner.
Equivalence between simulability of high-dimensional measurements and high-dimensional steering.
Physical Review A, 107(5):052425, 2023.

Marie Ioannou, Pavel Sekatski, Sébastien Designolle,
Benjamin DM Jones, Roope Uola, and Nicolas Brunner.
Simulability of high-dimensional quantum measurements.
Physical Review Letters, 129(19):190401, 2022.

In Chapter 4 we study various models of quantum computation, and in particular the role of coherence in gadget based approaches. Our main contribution is a no-go result, showing that some amount of coherence is necessary to have in the operations for universal quantum computation, it cannot be siphoned off to a supplementary state, unlike in the cases of entanglement or magic. This chapter is fully based on the following arXiv preprint [19]:

Benjamin DM Jones, Paul Skrzypczyk, and Noah Linden.
The Hadamard gate cannot be replaced by a resource state in universal quantum computation.
arXiv preprint arXiv:2312.03515, 2023.

In Chapter 5 (based on unpublished work with Ashley Montanaro), we provide a technical no-go result in the realm of quantum property testing. We show that up to constant factor, at least $n/\log n$ copies are needed to test the property of an n-partite state being not genuinely multipartite entangled, which closely matches a corresponding upper bound in the literature. The bulk of this work was technical in nature, using methods involving the symmetric subspace.

We conclude in Chapter 6 with some reflections on the field in general, as well as summarising various research questions that arose during my PhD.

1.1.3 My PhD journey

My PhD has been part of the Quantum Engineering Centre for Doctoral Training (QECDT) at the University of Bristol, UK. This degree is typically 4 years, with an initial training year provided by the QECDT, followed by a more conventional 3 year research project. I greatly benefited from the first year of the program, taking theory classes in quantum information, quantum optics, and classical algorithms, as well as undertaking some experimental projects (including performing a Bell test of nonlocality). It was also wonderful to be part of a cohort with 10 other students.

In the summer of 2020 I moved to Geneva, Switzerland, as I started the research phase of my PhD, to collaborate with the group of Nicolas Brunner at the University of Geneva. I was there for around 8 months in total, amidst some complications regarding the pandemic and Brexit. It was in this period that I completed my first research paper on network quantum steering, and laid the foundation for some other works in collaboration with the group in Geneva.

I took a 2 month break from my PhD in the summer of 2021 due to personal circumstances, and resumed my studies in Bristol in September 2021. I started a project with my supervisors

Paul Skrzypczyk and Noah Linden, and had desks in both the Physics and Mathematics departments.

In the academic year of 2021-2022 I also organised a 'Careers in Quantum' event with other members of my QECDT cohort.

In the summer of 2022 I paused my PhD for 3 months to do an internship with Phasecraft, a quantum computing startup with offices in Bristol and London (I was based in Bristol). I then stayed as a consultant with them until December 2023, working part-time. My work with Phasecraft has been on near-term quantum algorithms, with no overlap with my PhD research (so this thesis does not contain any of my work with them).

In terms of teaching, I marked homeworks for the Quantum Information Theory module in the academic years 2020-2021 and 2021-2022. I then co-taught a Quantum Information module for first year QECDT students in the autumn of 2023, which involved in-person lecturing and homework marking.

I also revived and co-organised the group meetings for the Quantum Information Theory Group in Bristol during 2023.

Altogether I took 5 months formal suspension, and combined with officially switching to part-time studies for teaching meant that my thesis hand-in deadline moved from September 2023 to April 2024.

During my PhD I attended and presented at several conferences:

- Quantum Measurement Theory 2022 in Bad Honnef, Germany – I presented a poster.
- A summer school in 2022 in Bad Honnef, Germany on Quantum Computing.
- Quantum Computing Theory in Practice 2023 in Cambridge, UK.
- Quantum Information Processing 2022 (California, US) & 2023 (Ghent, Belgium) – I presented posters at both.
- Quantum Resource Theories 2023 in Singapore – I gave an accepted talk with video here.
- I also gave talks on two occasions at the Bristol Quantum Information Theory seminar series.

Research-wise, I also worked and collaborated on some projects that have not made it into this thesis, either because the projects fizzled out, are ongoing, or I did not contribute sufficiently to be an author. These topics include: Buscemi nonlocality, entanglement and Schmidt number in infinite dimensions, experimental verification of the dimension of a channel, simulation of matchgate circuits, and the generalised quantum Stein's lemma.

Finally, I opted to write up my thesis remotely from January 2024, combining working with some travel around Latin America.

1.1.4 Highlighted references

There are several wonderful references which have helped me tremendously throughout my studies. Nielsen & Chuang [20] is considered the undisputed bible of quantum information. There are also many excellent books and lecture notes available, such as those of Wilde [21], Watrous [22], de Wolf [23], Walter [24], Tomamichel [25], Heinosaari and Ziman [26], and Aaronson [27].

We also list some review articles of particular relevance to this thesis: entanglement [28, 29], nonlocality [3], steering [30, 31], measurement incompatibility [32, 33], coherence [34], resource theories [35], property testing [36], measurement based quantum computation [37, 38], and error correction [39].

1.2 Mathematical preliminaries

1.2.1 Notation

- $[d] = \{0, ..., d-1\}$.
- $\mathbb{C}$ denotes the field of complex numbers.
- $\mathbb{R}$ denotes the field of real numbers.
- $\mathcal{L}(\mathcal{H})$ denotes the set of linear maps on a Hilbert space $\mathcal{H}$. In this thesis all Hilbert spaces are finite-dimensional and isomorphic to $\mathbb{C}^d$ for some d.
- $\mathcal{S}(\mathcal{H})$ denotes the set of quantum states on $\mathcal{H}$, i.e. $\rho \in \mathcal{L}(\mathcal{H})$ such that $\rho \geq 0$ and $\mathrm{Tr}(\rho) = 1$.
- We use ln to denote the natural logarithm and log the logarithm to base 2.
- We denote the trace distance by $D(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1$, where $\|A\|_1 = \mathrm{Tr}(\sqrt{AA^\dagger})$.
- We use $\mathbb{1}$ to denote the identity operator, and sometimes write $\mathbb{1}_d$ to denote it acting on a space of dimension d.
- We use $\mathbb{P}$ for probabilities, and $\mathbb{E}$ for expectation values.
- We use the symbol "$:=$″ to indicate a new definition, and "$\equiv$" to denote equivalence.

We also often use notation such as "$|x\rangle$" to denote some set $\{|x\rangle\}_{x=0}^{d-1}$, and similarly use "$M_{a|x}$" to denote a set of POVM measurements or "$p(a,b|x,y)$" a set of probabilities, in all cases omitting the set braces and index range for convenience.

1.2.2 Linear algebra

Linear algebra is the mathematical language underpinning quantum mechanics in finite dimensions. We refer readers to textbooks [40–42] for a comprehensive guide. Here we give some more informal and intuitive definitions.

A *vector space* V is a set in which the objects can be added together, or multiplied by a number (an element of some *field*, usually $\mathbb{R}$ or $\mathbb{C}$). The canonical example for us will be $\mathbb{C}^d$, where the vectors are composed of d complex numbers, and are written in *Dirac notation* in some fixed basis as

$$|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} \in \mathbb{C}^d. \tag{1.3}$$

We say that some collection of vectors forms a *basis* if any vector can be written as a linear combination of elements. That is, a discrete set $|v_i\rangle$ forms a basis for V if $\forall\,|w\rangle \in V$ there exists $\alpha_i \in \mathbb{C}$ such that

$$|w\rangle = \sum_i \alpha_i \, |v_i\rangle \,. \tag{1.4}$$

The *dimension* of a vector space is the smallest number of vectors required to form a basis. The dimension of $\mathbb{C}^d$ is d.

A *norm* on a vector space is a function that assigns a notion of length to each vector. On $\mathbb{C}^d$ the standard norm is

$$\||v\rangle\| := \sqrt{\sum_i |v_i|^2}. \tag{1.5}$$

A *inner product* captures the overlap between two vectors, taking into account both direction and magnitude. The canonical inner product on $\mathbb{C}^d$ in quantum information is given by

$$\begin{aligned} \Big(|v\rangle \,, |u\rangle \Big) &\equiv \langle v|u\rangle \qquad (1.6) \\ &= \sum_i v_i^* u_i, \qquad (1.7) \end{aligned}$$

which is anti-linear in the first argument. An inner product always induces a norm as follows

$$\||v\rangle\| := \sqrt{\langle v|v\rangle}. \tag{1.8}$$

A basis $|v_i\rangle$ is *orthonormal* if $\langle v_i|v_j\rangle = \delta_{ij}$.

Two ubiquitous inequalities are:

The Triangle Inequality:

$$\||u\rangle + |v\rangle\| \leq \||u\rangle\| + \||v\rangle\|. \tag{1.9}$$

The Cauchy-Schwarz Inequality:

$$|\langle u|v\rangle| \leq \||u\rangle\|\||v\rangle\|. \tag{1.10}$$

Linear maps are functions $A : V \to V$ such that $A(\alpha \left|v\right\rangle + \beta \left|w\right\rangle) = \alpha A \left|v\right\rangle + \beta A \left|w\right\rangle$ for all $\alpha, \beta \in \mathbb{C}$ and $\left|v\right\rangle, \left|w\right\rangle \in V$. These can be represented by matrices, assuming a vector representation for some fixed orthonormal basis.

The dual $A^\dagger$ of a linear map A is defined by

$$\Big(\left|v\right\rangle, A^\dagger \left|u\right\rangle \Big) = \Big(A \left|v\right\rangle, \left|u\right\rangle \Big). \tag{1.11}$$

In matrix notation, this dual or 'dagger' operation corresponds to performing the conjugate transpose of a matrix.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}, \qquad A^\dagger = (A^*)^T = \begin{pmatrix} a_{11}^* & \dots & a_{n1}^* \\ \vdots & \ddots & \vdots \\ a_{n1}^* & \dots & a_{nn}^* \end{pmatrix}, \tag{1.12}$$

$$\left|v\right\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \qquad \left|v\right\rangle^\dagger = \left\langle v\right| = \begin{pmatrix} v_1^* & \dots & v_n^* \end{pmatrix}. \tag{1.13}$$

Note that whilst the transpose and complex conjugate are both basis dependent operations, their combined action as the complex transpose is basis independent.

The *eigenvectors* $\left|v\right\rangle$ and *eigenvalues* λ of a matrix A satisfy

$$A \left|v\right\rangle = \lambda \left|v\right\rangle. \tag{1.14}$$

Name	Definition	Eigenvalues
Unitary	$UU^\dagger = \mathbb{1}$	$\lvert\lambda\rvert = 1$
Hermitian	$H = H^\dagger$	$\lambda \in \mathbb{R}$
Positive Semi-Definite (PSD)	$\left\langle\psi\right| A \left|\psi\right\rangle \geq 0 \qquad \forall \left|\psi\right\rangle$	$\lambda \geq 0$
Projectors	$P = P^\dagger$, $P^2 = P$	$\lambda \in \{0, 1\}$
Identity	$\mathbb{1} \left|\psi\right\rangle = \left|\psi\right\rangle \qquad \forall \left|\psi\right\rangle$	$\lambda = 1$

Table 1.1: Some noteworthy operators in quantum mechanics.

A set of vectors $\left|v_i\right\rangle$ is said to be *linearly independent* if $\sum \alpha_i \left|v_i\right\rangle = 0$ implies that α_i=0 for all i. Otherwise they are said to be *linearly dependent*. In other words, linear independence means that one cannot write any vector from the set as a linear combination of the others.

The *null space* or *kernel* of an operator is the subspace of vectors that get mapped to zero (equivalently, the eigenspace associated with eigenvalue 0). The *nullity* is the dimension of the kernel. The *range* of a matrix is the subspace spanned by the columns. The *support* is the set of vectors which are not mapped to zero. The *image* is the set of vectors of the form $A\left|v\right\rangle$, for $\left|v\right\rangle \in V$. The *rank* of a matrix is the dimension of the range. The *rank-nullity* theorem says that the sum of the rank and the nullity is equal to the dimension of the matrix (number of columns).

The *trace* of a matrix is equal to the sum of the diagonal terms. This definition is basis independent, and equivalent to the following, for $\left|x\right\rangle$ any basis

$$\mathrm{Tr}(A) = \sum_x \left\langle x\right| A \left|x\right\rangle . \tag{1.15}$$

The trace is also equal to the sum of the eigenvalues.

Recall that the following are equivalent (over $\mathbb{C}$):

- A is invertible, i.e. there exists A^{-1} satisfying $AA^{-1} = AA^{-1} = \mathbb{1}$.
- The determinant of A is non-zero.
- A has full rank.
- All the eigenvalues of A are non-zero.

A *diagonal matrix* has only non-zero entries along the leading diagonal. A matrix A is *diagonalisable* if there exists an invertible U and diagonal D s.t. $A = UDU^{-1}$. The following are equivalent (over $\mathbb{C}^d$):

- A is diagonalisable.
- There is a basis consisting of eigenvectors of A.

Note that the properties of being invertible and diagonalisable do not imply each other.

Theorem 1.1 (Spectral Theorem)**.** Let A be a normal matrix, i.e. $AA^\dagger = A^\dagger A$. Let $\{\lambda_a, \left|a\right\rangle\}$ denote the eigenvalues and eigenvectors of A. Then A can be written as

$$A = \sum_a \lambda_a \left|a\right\rangle\!\left\langle a\right| \tag{1.16}$$

Proof. We will use the Schur decomposition, which allows us to write any complex matrix as

$$A = UTU^\dagger \tag{1.17}$$

where U is unitary, and T is an upper triangular matrix. If A is normal, then it immediately follows that T is also normal. But as T is upper triangular, this implies that T must be diagonal. Now note that if $|a\rangle$ is an eigenvector of A with eigenvalue λ_a, then $U^\dagger |a\rangle$ is an eigenvector of T with eigenvalue λ_a. As T is diagonal, this implies that T can be written as $T = \sum_a \lambda_a U^\dagger |a\rangle\langle a| U$. So overall we have

$$A = UTU^\dagger = \sum_a \lambda_a |a\rangle\langle a| \,. \tag{1.18}$$

□

We can define functions on normal matrices by their action on the eigenvalues.

$$A = \sum_a \lambda_a |a\rangle\langle a| \tag{1.19}$$

$$f(A) = \sum_a f(\lambda_a) |a\rangle\langle a| \tag{1.20}$$

$$\text{e.g.} \qquad e^A = \sum_a e^{\lambda_a} |a\rangle\langle a| \,. \tag{1.21}$$

This also coincides with the Taylor expansion of the function, e.g. $e^A = \sum_{n=0}^\infty \frac{A^n}{n!}$. Note that hermitian and unitary matrices are both normal, and one can check that if H is hermitian then e^{iH} is unitary. Indeed suppose we can write H in spectral decomposition as

$$H = \sum_a a |a\rangle\langle a| \tag{1.22}$$

with eigenvalues $a \in \mathbb{R}$. Then we have

$$e^{iH} = \sum_a e^{ia} |a\rangle\langle a| \tag{1.23}$$

is unitary, with eigenvalues e^{ia} on the complex unit circle.

The *tensor product* is a way of forming a vector space from two vector spaces (intuitively it is a way of multiplying vector spaces together). If $|v_i\rangle$ and $|w_i\rangle$ respectively form bases for V and W, then

$$|u_{ij}\rangle := |v_i\rangle \otimes |w_j\rangle \equiv |v_i\rangle |w_j\rangle \equiv |v_i, w_j\rangle \tag{1.24}$$

defines a basis for $V \otimes W$.

For an operator acting on $V \otimes W$, the *partial trace* (on space W) can be defined by its action on basis elements as

$$\mathrm{Tr}_2\Big(|a\rangle\langle b| \otimes |c\rangle\langle d| \Big) = |a\rangle\langle b| \langle c|d\rangle \,, \tag{1.25}$$

which can also be written as

$$\mathrm{Tr}_2\Big(A \otimes B\Big) = \sum_x \langle x| B |x\rangle \;\; A, \tag{1.26}$$

for some basis $|x\rangle$ on W.

Finally to give another example of a vector space, but over the real numbers, we can consider the space of Hermitian matrices. This forms a real vector space, with natural norm $\|A\| = \sqrt{\text{Tr}(A^2)}$ and inner product $(A, B) := \text{Tr}(AB)$. As we can also multiply vectors (matrices) together in this case, it is also an example of an *algebra*.

1.3 The arena of Quantum Mechanics

1.3.1 Quantum Mechanics: pure and simple

There are three natural components to the theory, which encapsulate the procedure of any physical experiment.

- *States*: how to describe a quantum mechanical system.
- *Evolution*: how states change with time.
- *Measurement*: how to explain the results seen on some apparatus.

Definition 1.2. A *pure quantum state* is a vector $|\psi\rangle \in \mathbb{C}^d$, normalised such that $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle} = 1$. This represents a a quantum system with d degrees of freedom.

Next, we describe evolution. We might have a state $|\psi\rangle$ at some time and then perform some operation on it, or let it undergo some change, and then we end up with some state $|\psi'\rangle$. We would want this process to be linear, and to preserve the norm (so that the output is also a valid quantum state). This naturally leads us to unitary operators.

Definition 1.3. A pure quantum state evolves according to the action of a unitary operator U.

$$|\psi\rangle \mapsto U|\psi\rangle \tag{1.27}$$

This is sometimes referred to as *pure* or *coherent* evolution.

Now let us introduce the formalism of quantum measurements.

Definition 1.4. A *(projective) quantum measurement* can be described by a Hermitian matrix H, which is also referred to as an *observable* in this context. By the spectral theorem, H admits a spectral decomposition

$$H = \sum_{\lambda} \lambda \, P_\lambda \tag{1.28}$$

where P_λ are projectors, and the sum is over the spectrum (eigenvalues) of H.

Quantum mechanics then asserts that the probability of observing outcome λ when measuring H on state $|\psi\rangle$ is given by

$$\mathbb{P}(\lambda) = \langle\psi| \, P_\lambda \, |\psi\rangle \tag{1.29}$$

This is generally referred to as the *Born rule*, and note that the spectral theorem guarantees that $\mathbb{P}(\lambda) \geq 0$ and $\sum_\lambda \mathbb{P}(\lambda) = 1$.

Example 1.5. Suppose that we write a quantum state $|\psi\rangle \in \mathbb{C}^d$ in some basis $|x\rangle$

$$|\psi\rangle = \sum_{x=0}^{d-1} \alpha_x \, |x\rangle \tag{1.30}$$

and perform the measurement corresponding to the observable

$$C = \sum_{x=0}^{d-1} x \, |x\rangle\!\langle x| \, . \tag{1.31}$$

Then by the Born rule, we would see outcome $x \in [d-1]$ with probability

$$\begin{aligned} p(x) &= \langle\psi| \;\; |x\rangle\!\langle x| \;\; |\psi\rangle && (1.32)\\ &= |\langle\psi|x\rangle|^2 && (1.33)\\ &= |\alpha_x|^2. && (1.34) \end{aligned}$$

1.3.1.1 Multiple systems and entanglement

An crucial aspect not yet mentioned is how to describe multiple systems. A simple, motivating example is to consider two systems $|\psi\rangle_A \in \mathbb{C}^{d_A}$ and $|\phi\rangle_B \in \mathbb{C}^{d_B}$. '$A$' and '$B$' can be thought of labelling the systems (or the parties in possession of the systems), and d_A and d_B are the local dimensions.

The combined state $|\Psi\rangle_{AB}$ is an element of the tensor product space $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$, which as a vector space is isomorphic to $\mathbb{C}^{d_A d_B}$, but endowed with a bipartite structure though the tensor product. In this example, the joint state $|\Psi\rangle_{AB}$ would be described by

$$|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B \quad \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}. \tag{1.35}$$

An important aspect of the tensor product is that not all vectors in $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ can be themselves written as a tensor product of two vectors [43]

Definition 1.6.

- States $|\Psi\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ that can be written as $|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle$ are referred to as (pure) *product states*.
- States $|\Psi\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ that are not product states are referred to as *entangled states*.

Example 1.7. The canonical maximally entangled state between two d-dimensional systems is given by

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle\, |x\rangle\, . \tag{1.36}$$

1.3.2 Quantum Mechanics: mixed and general

The above formalism is insufficient to describe the outcomes of all experiments, for the following reasons:

- Including classical probability: suppose we flip a coin and decide to prepare one of two quantum states $|\psi_1\rangle$ or $|\psi_2\rangle$, and then perform a measurement.
- Suppose we have an entangled state, and wish to have a local description of one of the subsystems.
- In practice, quantum systems are never perfectly isolated from their environment. Incorporating physical noise is also lacking in the pure state description.

The following definition can be originally attributed to von Neumann [5]

Definition 1.8. General quantum states are described by *density operators* $\rho : \mathbb{C}^d \to \mathbb{C}^d$, which are linear maps with the conditions that $\rho \geq 0$ and $\mathrm{Tr}(\rho) = 1$. The integer d is referred to as the *dimension* of the state.

Example 1.9. Consider preparing the quantum state $|\psi_\lambda\rangle$ with probability $p(\lambda)$. Then the resulting density operator can be written as

$$\rho = \sum_\lambda p(\lambda)\, |\psi_\lambda\rangle\!\langle\psi_\lambda| \,. \tag{1.37}$$

Definition 1.10. General quantum evolution is described by *quantum channels* [44, 45]. These are maps $\Lambda : \mathcal{L}(\mathbb{C}^{d_1}) \to \mathcal{L}(\mathbb{C}^{d_2})$ that are

- Completely positive (CP): $\Lambda \otimes \mathbb{1}\rho \geq 0 \quad \forall \rho \geq 0$.
- Trace preserving (TP): $\mathrm{Tr}(\Lambda(\rho)) = \mathrm{Tr}(\rho)$.

Channels are hence also referred to as *CPTP maps*.

See [20] for an extended discussion on quantum channels.

Proposition 1.11. The following are equivalent for a map $\Lambda : \mathcal{L}(\mathbb{C}^{d_1}) \to \mathcal{L}(\mathbb{C}^{d_2})$:

(i) (Definition) Λ is CPTP.

(ii) (Kraus Decomposition) There exists K_λ s.t $\Lambda(\rho) = \sum_\lambda K_\lambda \rho K_\lambda^\dagger$ with $\sum_\lambda K_\lambda^\dagger K_\lambda = \mathbb{1}$.

(iii) (Stinespring dilation) There exists U s.t.

$$\Lambda(\rho) = \mathrm{Tr}_2 \left(U\rho \otimes |0\rangle\!\langle 0|\, U^\dagger \right). \tag{1.38}$$

See [20, 22] for proofs, and [44, 46] for early references.

Definition 1.12. The *dual channel* Λ^* associated to a channel Λ is defined via the following equation

$$\mathrm{Tr}\left(\Lambda(\rho)\ M\right) = \mathrm{Tr}\left(\rho\ \Lambda^*(M)\right). \tag{1.39}$$

One sometimes refers to channels acting on states as the *Schrödinger* picture, and dual channels acting on measurements as the *Heisenberg* picture. We also have that if a channel Λ is completely positive and trace preserving (CPTP), then the dual channel Λ^* will be completely positive and unital (CPU), where *unital* means that the identity is always mapped to itself: $\Lambda^*(\mathbb{1}) = \mathbb{1}$.

Now let us define quantum measurements in the more general setting.

Definition 1.13. General quantum measurements are defined by positive operator valued measures (POVMs). This is a set of matrices $\{M_a\}_{a\in S}$ such that

$$M_a \geq 0 \quad \forall a \qquad \sum_a M_a = \mathbb{1}. \tag{1.40}$$

The probability of observing outcome a when measuring the POVM $\{M_a\}$ on ρ is given by

$$p(a) = \mathrm{Tr}(M_a\ \rho). \tag{1.41}$$

Remark 1.14.

- A POVM may act on a space of dimension d, but can have any number of outcomes (even countably and uncountably infinite).
- We will often denote a set of POVMs by $M_{a|x}$, where a indexes the outcome and x indexes the POVM. We sometimes refer to this as a *measurement assemblage*.
- POVMs only describe the final outcome probabilities, and say nothing about the final quantum state after measurement.
- The labels a are arbitrary, in the sense that they do not affect the probabilities in any way.
- The name comes from measure theory: for general probability spaces the map $S \mapsto M_S$ for S some measurable set (possible set of outcomes) is similar to a measure but takes values as positive matrices.

The following theorem, known as *Naimark's dilation theorem*, says that any POVM can be interpreted as a projective measurement acting on a higher dimensional space. It is analogous to Stinespring's dilation theorem for channels (see Proposition 1.11 above), and in fact can be viewed as a consequence of it.

Theorem 1.15 (Naimark [47])**.** Given a POVM M_a, we can always find a projective measurement P_a acting on a higher dimensional space such that for all ρ

$$\mathrm{Tr}\Big(M_a\rho\Big) = \mathrm{Tr}\Big(P_a\rho\otimes|0\rangle\langle 0|\Big). \tag{1.42}$$

A proof is given in [22].

Quantum instruments are needed to describe the post-measurement states of POVMs.

Definition 1.16.

- A *quantum subchannel* is a completely positive, trace non-increasing map.
- A *quantum instrument* is a collection of subchannels Λ_λ such that $\sum_\lambda \Lambda_\lambda$ is a channel.

That is, if one performs the measurement associated to the instrument Λ_λ on a state ρ, one would observe outcome λ with probability $\mathrm{Tr}(\Lambda_\lambda(\rho))$, and the resulting final state would be $\Lambda_\lambda(\rho)/\mathrm{Tr}(\Lambda_\lambda(\rho))$.

If we have a bipartite system ρ_{AB}, then the description of the state of system A is given by partial tracing out of system B, namely $\rho_A = \mathrm{Tr}_2(\rho_{AB})$.

We also have the following definition of entanglement for density operators [48].

Definition 1.17. For density operators, a state ρ is called *product* if it can be written as $\rho = \sigma \otimes \tau$ for some states σ and τ. A state ρ is called *separable* if it can be written as the convex combination of product states, namely as

$$\rho = \sum_\lambda p(\lambda)\ \sigma_\lambda \otimes \tau_\lambda. \tag{1.43}$$

for probabilities $p(\lambda)$. If a state is not separable it is *entangled*.

This concludes our overview of finite dimensional quantum mechanics, see Table 1.2 for a summary. There are many topics we have omitted in this review, such as quantum hamiltonians, and the infinite dimensional case – see e.g. the following textbooks for further information [49, 50].

1.4 Quantum Foundations, Information and Computation

In this section we detail some topics that will be of importance in later chapters in this thesis. First of all, we introduce the *trace distance*, which provides an important way of defining distances between quantum states and channels.

Definition 1.18. The *trace distance* on quantum states is defined as

$$D(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1, \tag{1.44}$$

where $\|A\|_1 = \mathrm{Tr}(\sqrt{A^\dagger A})$.

	States	Evolution		Measurements
		Schrödinger	Heisenberg	

Pure	$\lvert\psi\rangle \in \mathbb{C}^d$
	$\lVert \lvert\psi\rangle \rVert = 1$
		Unitary $U : UU^\dagger = \mathbb{1}$
		$\lvert\psi\rangle \mapsto U \lvert\psi\rangle$
			Unitary $U : UU^\dagger = \mathbb{1}$
			$O \mapsto U^\dagger O U$
				Observable = Hermitian
				$H = \sum aP_a$
				Prob(outcome a)
				$= \langle\psi\rvert P_a \lvert\psi\rangle$

Mixed	$\rho : \mathbb{C}^d \to \mathbb{C}^d$ $\rho \geq 0$ $\mathrm{Tr}(\rho) = 1$	Channel Λ : CPTP $\rho \mapsto \Lambda(\rho)$	Dual Channel Λ^* : CPU $M_a \mapsto \Lambda^*(M_a)$	POVM M_a $M_a \geq 0 \quad \sum_a M_a = \mathbb{1}$ Prob(outcome a) $= \mathrm{Tr}(M_a \rho)$

Table 1.2: The arena of quantum mechanics: how states, evolution, and measurements are described in the pure and mixed descriptions.

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:

$$\mathcal{D}(\mathcal{E}, \mathcal{V}) := \max_{\rho} \ D\Big(\mathcal{E}(\rho), \mathcal{V}(\rho)\Big). \tag{1.45}$$

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.

We now review some relevant areas of quantum information that will be integral to this thesis.

1.4.1 Generalised channel state duality

We recall the generalised form of *channel-state duality*, see e.g. [51, 52], which will be of particular importance in Chapter 3. This subsection is based upon Appendix A in [17].

For any fixed state $\sigma \in \mathcal{L}(\mathcal{H}_B)$ of full rank, there is a one-to-one correspondence between bipartite states $\rho \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ with marginal $\mathrm{Tr}_1(\rho) = \sigma$, and quantum channels $\Lambda : \mathcal{L}(\mathcal{H}_B) \longrightarrow \mathcal{L}(\mathcal{H}_A)$. Explicitly, this is given by

$$\rho_\Lambda := \Lambda \otimes \mathbb{1} \, |\Omega\rangle\langle\Omega| \tag{1.46}$$

$$\Lambda^*_\rho(X) := \sigma^{-\frac{1}{2}} \mathrm{Tr}_1(X \otimes \mathbb{1}\rho)^T \sigma^{-\frac{1}{2}} \tag{1.47}$$

$$\iff \quad \Lambda_\rho(Y) = \mathrm{Tr}_2(\mathbb{1} \otimes (\sigma^{-\frac{1}{2}} Y \sigma^{-\frac{1}{2}})^T \rho), \tag{1.48}$$

where Λ^* is the dual channel to Λ, $\sigma \equiv \mathrm{Tr}_1(\rho) \equiv \sum_n s_n |n\rangle\!\langle n|$ in spectral decomposition, $|\Omega\rangle = \sum_n \sqrt{s_n}\, |n\rangle\, |n\rangle$ is a purification of σ, and $(\cdot)^T$ denotes transpose in the $|n\rangle$ basis. One can easily verify that $\Lambda_{\rho_\Lambda} = \Lambda$ and $\rho_{\Lambda_\rho} = \rho$, hence the correspondence $\rho \longleftrightarrow \Lambda_\rho$ is a bijection for every fixed state $\sigma \in \mathcal{L}(\mathcal{H}_B)$ of full rank. Note that for states σ not of full rank we can apply the above correspondence by restricting to the support of σ, i.e., a subspace $\mathcal{H}'_B \subseteq \mathcal{H}_B$ of dimension $\mathrm{rank}(\sigma)$. The above correspondence is sometimes referred to as the *Choi-Jamiolkowski isomorphism*, and the state ρ_Λ is often called the *Choi state* of the channel Λ.

The most common version of this duality appears by taking $\sigma = \frac{\mathbb{1}}{d}$ in the above, which leads to the following simpler forms:

$$\rho_\Lambda := \Lambda \otimes \mathbb{1} \left|\Phi^+\middle\rangle\!\middle\langle\Phi^+\right| \tag{1.49}$$

$$\Lambda_\rho(\sigma) := \mathrm{Tr}_1(\mathbb{1} \otimes \sigma\ \rho), \tag{1.50}$$

where $|\Phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle\, |x\rangle$ is the canonical maximally entangled state.

1.4.2 Entanglement

The following definitions will be of relevance to Chapter 3 and Chapter 5.

Definition 1.19. The *Schmidt rank* of a pure bipartite quantum state $|\Psi\rangle$ is given by the minimum number of terms to express $|\Psi\rangle$ as a linear combination of product states.

$$\mathrm{SR}(|\Psi\rangle) = \min \quad n \tag{1.51}$$

$$\text{s.t.}\ \ |\Psi\rangle = \sum_{i=1}^{n} \alpha_i\, |v_i\rangle\, |w_i\rangle \tag{1.52}$$

It can be shown that there is always a solution to this minimisation, taking all α_i real and non-negative. Eq. (1.52) is then referred to as the *Schmidt decomposition*, and α_i the *Schmidt coefficients*.

Remark 1.20.

- The Schmidt decomposition can be reformulated as a singular value decomposition.
- Schmidt coefficients satisfy $\sum |\alpha_i|^2 = 1$, are bounded between 0 and 1, and the max Schmidt coefficient is bounded between $1/\sqrt{d}$ and 1 (for d the minimum of the local dimensions).
- The Schmidt rank is equal to the rank of either reduced density matrix, and the Schmidt coefficients are square roots of the eigenvalues of either reduced density matrix.

As the Schmidt rank is only defined for pure quantum states, a natural question is then how to construct a natural notion of entanglement dimensionality for general density operators. This is achieved by the following definition, which in words says that a state has Schmidt number at most n if it can be written as a convex combination of pure states each with Schmidt rank at most n – see also Fig. 1.1.

Definition 1.21. The *Schmidt number* [53] of a density operator ρ is defined as

$$\begin{aligned} \mathrm{SN}(\rho) := \min_{\{p_k,\ |\psi_k\rangle\}} \ \max_{k} \quad & \mathrm{SR}(|\psi_k\rangle) \\ \text{s.t} \quad & \rho = \sum_k p_k \, |\psi_k\rangle\!\langle\psi_k| \, . \end{aligned} \tag{1.53}$$

We also have the following analogous notion for quantum channels, which describes channels that map all states to states of Schmidt number at most n when acting on one half of the state.

Definition 1.22. A channel is *n-partially entanglement breaking* (n-PEB) if

$$\mathrm{SN}(\Lambda \otimes \mathbb{1} \ \rho) \leq n \qquad \forall \rho. \tag{1.54}$$

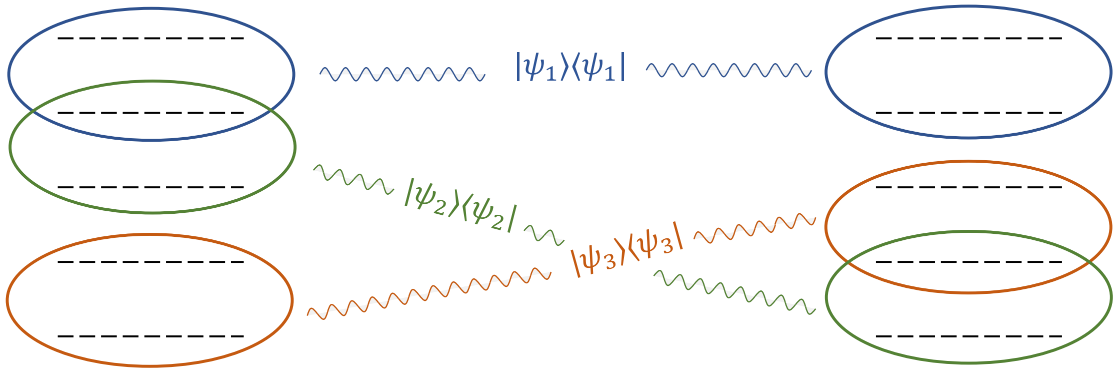

$|\psi_1\rangle\langle\psi_1|$
$|\psi_2\rangle\langle\psi_2|$
$|\psi_3\rangle\langle\psi_3|$

Figure 1.1: Illustration of Schmidt number. If the joint state of two 5-level quantum systems can be composed as a mixture of states of only 2-level entanglement, then the overall state has Schmidt number 2 despite being of dimension 5.

Lemma 1.23. The following are equivalent:

(i) Λ is n-PEB.

(ii) $\mathrm{SN}(\rho_\Lambda) \leq n$ for any choice of the marginal state in the generalised channel-state duality – see Eq. (1.48).

(iii) There exists a Kraus decomposition of $\Lambda(Y) = \sum_\lambda K_\lambda Y K_\lambda^\dagger$ such that $\mathrm{rank}(K_\lambda) \leq n$ for all λ.

See [17] for proof.

We also give the following definitions relating to multipartite entanglement, which will be central to Chapter 5.

Definition 1.24. Consider a state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ consisting of n parties, each of local dimension d. We say that it is

- *Genuinely multipartite entangled* (GME) if it is entangled across any bipartition of the n parties.
- *Bipartite product* (BP) if it is not GME, that is, there exists some non-trivial partition $S \subset [n]$ such that the state is product across this bipartition.
- *Mulitpartite product* (MP) if the state is product across every bipartition, i.e. the state can be written as the tensor product of n local states.

1.4.3 Measurement incompatibility

The main concept here is that a set of measurements is considered *compatible* or *jointly measurable*, if we instead could perform an alternative 'parent' measurement and post-process to get all the values of the other measurements (in a single round, not after gathering statistics). The following references serve as helpful review articles [32, 54].

Recall that a set of measurements is represented by POVMs $M_{a|x}$, i.e. matrices such that $M_{a|x} \geq 0 \quad \forall a, x$ and $\sum_a M_{a|x} = \mathbb{1} \quad \forall x$. Formally, a set of POVMs is said to be *compatible* if they can be written as

$$M_{a|x} = \sum_\lambda p(a|x,\lambda) G_\lambda \tag{1.55}$$

for some parent POVM G_λ and probabilities $p(a|x,\lambda)$.

Now consider a POVM $G_{\mathbf{a}}$ with outcomes labelling the possible outcomes of all the measurements: $\mathbf{a} = (a_1, \dots, a_n)$. For example, outcome $\mathbf{a} = (+1, -1, -1)$ would indicate that outcome $+1$ occurred for the first measurement and outcome -1 for the latter two measurements.

It turns out that these two notions are equivalent, see e.g. [32] for a proof sketch of the following fact.

Proposition 1.25. Given a set of POVMs $M_{a|x}$, the following are equivalent:

(i) There exists probabilities $p(a|x,\lambda)$ and a POVM G_λ such that

$$M_{a|x} = \sum_\lambda p(a|x,\lambda) G_\lambda \tag{1.56}$$

(ii) There exists a POVM $G_{\mathbf{a}}$ such that

$$M_{a|x} = \sum_{\mathbf{a}\,:\,a_x = a} G_{\mathbf{a}} \tag{1.57}$$

It is also known that for any compatible measurements, one can find Naimark dilations such that the corresponding projective measurements commute [32].

1.4.4 Nonlocality

Bell nonlocality is a crucial aspect of quantum information and foundations [3, 55]. It provides one of the most striking examples of the boundary between classical and quantum physics, and forms the basis of studies into entanglement, measurement incompatibility, and quantum steering. Early studies into this phenomenon date back to John Bell [56], and Boris Tsirelson [57–59]. There is the following quote from Valerio Scarani's book [55]: "Bell locality means that

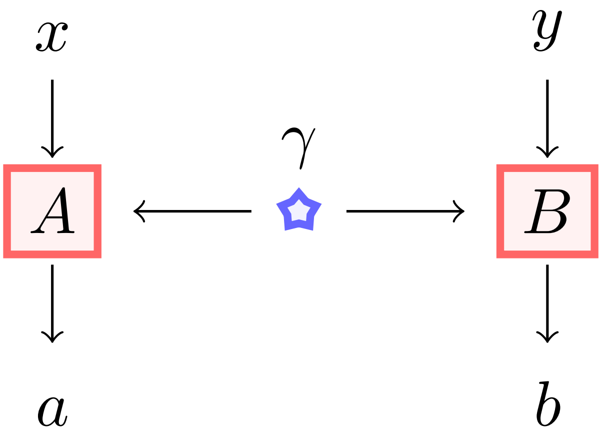


Figure 1.2: Bell nonlocality scenario. Two parties receive inputs x and y and respectively give outputs a and b. The information gathered in this scenario is the probabilities $p(a,b|x,y)$.

the process by which each player generates the output does not take into account the other player's input".

Consider two spatially separated parties, Alice and Bob, who respectively are given inputs labelled x and y, and give respective outputs a and b – see Fig. 1.2. After many rounds, we can describe the observed data by conditional probability distributions $p(a,b|x,y)$.

Suppose that Alice and Bob possess some shared information, described by the random variable λ, but have no access to the input of the other party – this is typically enforced by requiring the output to be given in a timeframe shorter than the time it would take light to pass from Alice to Bob. In this case, Alice's output can be described by the conditional distribution $p(a|x,\lambda)$, but does not depend on y. The overall resulting distributions, termed *local hidden variable* (LHV) models, are thus of the form

$$p(a,b|x,y) = \sum_{\lambda} p(\lambda)p(a|x,\lambda)p(b|y,\lambda). \tag{1.58}$$

Now consider distributions arising from the laws of quantum mechanics. Alice and Bob perform POVM measurements, respectively labelled as $M_{a|x}$ and $N_{b|y}$, and each may possess part of a shared quantum state ρ. The resulting probabilities are hence of the form

$$p(a,b|x,y) = \mathrm{Tr}\left(M_{a|x} \otimes N_{b|y}\ \rho\right) \tag{1.59}$$

Crucially, there are distributions arising from quantum mechanics that cannot be written with a local hidden variable model.

Let us briefly discuss some relevant aspects of quantum nonlocality. Given a set of probabilities $p(a,b|x,y)$, also referred to as a *behaviour*, one can think of this list of numbers as a point in $\mathbb{R}^d$, for some d. Clearly all valid probability distributions must satisfy the linear constraints $p(a,b|x,y) \geq 0 \quad \forall a,b,x,y$ and $\sum_{a,b} p(a,b|x,y) = 1 \quad \forall x,y$. It turns out that the set of behaviours admitting a local hidden variable model is a convex polytope in this space – often referred to as the *local set*. The set of behaviours admitting a quantum model (strictly greater than the local set) is also convex, but not a polytope. There is also the set of no-signalling behaviours, namely those that satisfy

$$p(a|x,y) = p(a|x,y') \qquad \forall a,x,y,y' \tag{1.60}$$
$$p(b|x,y) = p(b|x',y) \qquad \forall b,y,x,x'. \tag{1.61}$$

This set is strictly bigger than the set of quantum behaviours, and is a convex polytope. *Bell inequalities* can be thought of as hyperplanes that separate the quantum set from the local set.

One can observe that both entanglement and measurement incompatibility in both parties measurements are necessary to witness quantum nonlocality. Namely, if the state $\rho = \sum_\lambda p(\lambda)\sigma_\lambda \otimes \tau_\lambda$ is separable, then any behaviour can be written as

$$\begin{aligned} p(a,b|x,y) &= \mathrm{Tr}\Big(M_{a|x} \otimes N_{b|y}\ \rho\Big) && (1.62)\\ &= \sum_\lambda p(\lambda)\mathrm{Tr}\Big(M_{a|x}\sigma_\lambda\Big)\mathrm{Tr}\Big(N_{b|y}\tau_\lambda\Big) && (1.63)\\ &= \sum_\lambda p(\lambda)p(a|x,\lambda)p(b|y,\lambda), && (1.64)\end{aligned}$$

showing that one can never witness quantum nonlocality with a separable state. Similarly, suppose that e.g. Alice's measurements are compatible: $M_{a|x} = \sum_\lambda p(a|x,\lambda)G_\lambda$. Then

$$\begin{aligned} p(a,b|x,y) &= \mathrm{Tr}\Big(M_{a|x} \otimes N_{b|y}\ \rho\Big) && (1.65)\\ &= \sum_\lambda p(a|x,\lambda)\mathrm{Tr}\Big(G_\lambda \otimes N_{b|y}\ \rho\Big) && (1.66)\\ &= \sum_\lambda p(\lambda)p(a|x,\lambda)\mathrm{Tr}\Big(N_{b|y}\sigma_\lambda\Big) && (1.67)\\ &= \sum_\lambda p(\lambda)p(a|x,\lambda)p(b|y,\lambda), && (1.68)\end{aligned}$$

hence measurement incompatibility in both parties is also necessary to witness quantum nonlocality.

Therefore, one can think of Bell nonlocality as a *device independent* test of entanglement and measurement incompatibility of both parties. Device independence [60] refers to the fact that we do not trust the exact actions of Alice and Bob, only the outcome distributions.

1.4.4.1 Network nonlocality

Recently, there has been much interested generated in exploring notions of nonlocality in quantum networks, see [61] for a recent review. The principal idea is to consider multiple statistically independent sources, distributing quantum states to the various parties in the network.

A key development has been the discovery of non-classical correlations in networks in which the parties only perform a fixed measurement, i.e. have no input. One primary object of study has been the triangle network [62] (see Fig. 1.3), for which non-classical correlations not resting on standard Bell nonlocality have recently been proposed [63].

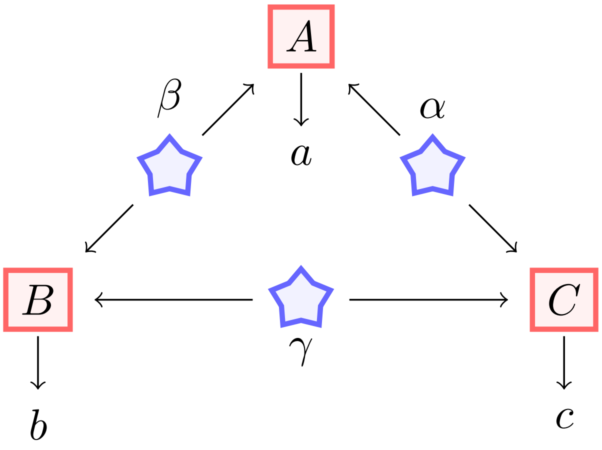


Figure 1.3: The triangle network nonlocality scenario.

These ideas will be of high relevance in Chapter 2.

1.4.5 Quantum steering

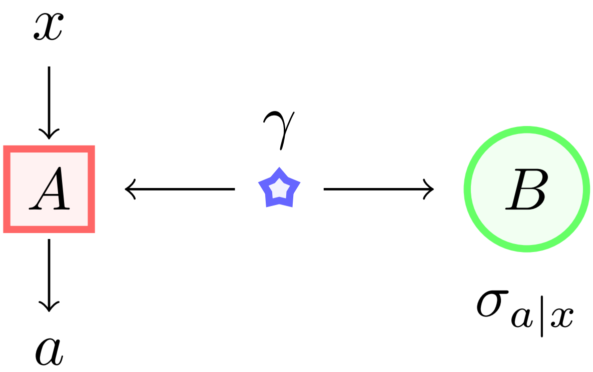


Figure 1.4: Quantum steering scenario. One party produces output a upon receiving input x and is considered untrusted (indicated here by a red box), and the other party is considered trusted (indicated here by a green circle) and has complete information about their system. The data produced can be expressed via an assemblage $\sigma_{a|x}$, where $\sigma_{a|x} \geq 0 \; \forall a, x$, and $\sum_a \sigma_{a|x} = \rho_B \quad \forall x$, for some state ρ_B.

This subsection is based on parts of [16]. In a bipartite steering scenario, one party performs measurements on a shared state ρ^{AB}, which 'steers' the quantum state of the other particle.

If Alice performs a set of measurements, labelled by x, with outcomes a, and corresponding POVM elements $M_{a|x}$, then the collection of sub-normalised 'steered states' of Bob are

$$\sigma^B_{a|x} := \mathrm{Tr}_1(M^A_{a|x} \otimes \mathbb{1}^B \rho^{AB}), \tag{1.69}$$

where $p(a|x) = \mathrm{Tr}(\sigma_{a|x})$ are the statistics of Alice's measurements – see also Fig. 1.4. The collection of sub-normalised states $\{\sigma_{a|x}\}_{a,x}$ are commonly referred to as a *steering assemblage* [64]. If the assemblage can be explained by a *local hidden state* (LHS) model, of the form

$$\sigma_{a|x} = \sum_\lambda p(\lambda)\ p(a|x,\lambda)\sigma_\lambda, \tag{1.70}$$

where λ is a hidden variable, distributed according to $p(\lambda)$, σ_λ are 'hidden states' of Bob, and $p(a|x,\lambda)$ are local 'response functions' of Alice, then we say that it has LHS form, or does not demonstrate steering [65]. If there exist measurements such that $\sigma_{a|x}$ does not admit such an LHS decomposition, we say that the state ρ^{AB} is *steerable* from A to B. If for all measurements we can never demonstrate steering with a given state, we say it is unsteerable (from A to B). Note that steering can be asymmetrical; some states are steerable from Alice to Bob, but not the other way around [66].

Quantum steering is often described as a *semi-device independent* (SDI) scenario, as one of the parties is considered untrusted (we only consider the resulting probabilities), and the other party is considered trusted (i.e. can perform full tomography).

The original notions of quantum steering can be dated back to Schrödinger [43, 67], also see [30, 31, 68] for review articles on quantum steering.

1.4.5.1 Connections between quantum steering and measurement incompatibility

There are two main connections between measurement incompatibility and quantum steering. Firstly, recall the relevant data in these two scenarios:

$$\underline{\text{Quantum steering}} \qquad\qquad \underline{\text{Measurement Incompatibility}} \tag{1.71}$$

$$\sigma_{a|x} \geq 0 \qquad\qquad M_{a|x} \geq 0 \tag{1.72}$$

$$\sum_a \sigma_{a|x} = \rho_B \quad \forall x \qquad\qquad \sum_a M_{a|x} = \mathbb{1} \quad \forall x \tag{1.73}$$

We have the following equivalence [31]:

Proposition 1.26.

(i) If $\sigma_{a|x}$ is LHS then $M_{a|x} := \rho_B^{-\frac{1}{2}} \sigma_{a|x} \rho_B^{-\frac{1}{2}}$ is compatible.

(ii) If $M_{a|x}$ is compatible then $\sigma_{a|x} := \rho_B^{\frac{1}{2}} M_{a|x} \rho_B^{\frac{1}{2}}$ is LHS, for any state ρ_B.

The second relationship is very similar to something already discussed in the nonlocality case – see Eq. (1.66) and subsequent equations. We have that if $M_{a|x}$ is compatible, then

$$\sigma_{a|x} = \mathrm{Tr}_1\Big(M_{a|x} \otimes \mathbb{1}\ \rho\Big) \tag{1.74}$$

will be LHS for any shared state ρ.

1.4.6 Stabilisers, Cliffords, and magic

This subsection will prove relevant to Chapter 4, as our results are inspired by ideas from magic state injection.

The *computational basis* refers to some preferred set of basis states, labelled by bitstrings $\{|x\rangle\}_{x\in\{0,1\}^n}$. One can also think of this as the *incoherent basis* – see Section 1.4.7.1.

The *Pauli matrices* are

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1.75}$$

and the n-qubit *Pauli group* $\mathcal{P}_n$ is generated by tensor products of Pauli matrices, elements being referred to simply as 'Paulis'. They can all be written as

$$i^c\ X^{a_1} Z^{b_1} \otimes \ldots X^{a_n} Z^{b_n} \tag{1.76}$$

for $c \in \{0,1,2,3\}$ and $a_i, b_j \in \{0,1\}$.

Paulis serve a special role in quantum information for several reasons. They are both unitary and hermitian, meaning that they can describe both evolution and measurement. The Pauli matrices all square to the identity, are traceless, and satisfy the following expressions

$$XY = iZ \qquad YZ = iX \qquad ZX = iY. \tag{1.77}$$

The n-qubit Pauli group also spans the space of $2^n \times 2^n$ complex matrices.

The *Clifford group* $\mathcal{C}_n$ is defined as the normaliser of $\mathcal{P}_n$:

$$\mathcal{C}_n = \{U\ :\ UPU^\dagger \in \mathcal{P}_n \quad \forall P \in \mathcal{P}_n\} \tag{1.78}$$

and is generated by (tensor products of) the following gates

$$\begin{array}{ccc} \underline{\text{Hadamard}} & \underline{\text{Phase}} & \underline{\text{Controlled-NOT}} \\ H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, & S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, & CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \end{array} \tag{1.79}$$

There are several equivalent definitions for a state $|\psi\rangle$ being a *stabiliser state*:

- There exists a Clifford unitary U such that $|\psi\rangle = U|0^n\rangle$, where $|0^n\rangle$ is the all zero computational basis state.
- There exists an abelian subgroup S of $\mathcal{P}_n$ of size $|S| = 2^n$ and $P|\psi\rangle = |\psi\rangle$ for all $P \in S$.
- There exists an affine subspace $A \subseteq \{0,1\}^n$ (where $\{0,1\}$ is interpreted as the field of two elements), a linear function l and a quadratic function q (with respect to the field operations) such that (see [69, 70] for proof)

$$|\psi\rangle = \sum_{x\in A} i^{l(x)} (-1)^{q(x)} |x\rangle . \tag{1.80}$$

The T gate and the T state are respectively defined as

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}, \qquad |T\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{i\pi}{4}}|1\rangle\right). \tag{1.81}$$

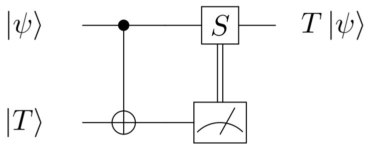
A set of quantum gates (unitaries) is considered *universal* if a sequence of gates from the set can approximate any unitary to arbitrary precision [20]. The most common universal gate set considered in quantum information is the *Clifford + T* gate set.

The *Gottesman–Knill Theorem* [20, 71–73] states that any quantum computation composed of the following operations is efficiently classically simulable:

- Preparation of computational basis states.
- Unitaries from the Clifford group.
- Classical control.
- Measurement in the computational basis.

Here "*efficiently classically simulable*" means the overall process only requires resources (time and space) that scale at most polynomially with the number of qubits n (whereas naively one would need memory scaling like $\sim 2^n$ just to store the state of the system).

Magic state injection refers to a model of quantum computation in which only Clifford unitaries can be performed, and one implements the T gate using the following circuit (also called a *gadget*).



(1.82)

In words, this circuit depicts a controlled-NOT gate being applied between the input $|\psi\rangle$ and a $|T\rangle$ state, followed by a phase gate on the input register conditioned on measuring the second register in the computational basis.

The benefit of this approach is that one can use an error correcting code that is well suited to Clifford gates, and separate the process of preparing T states as a subroutine. In particular, one can consider procedures that accept multiple noisy or imperfect T states and output a state that is closer to a T state – this process is referred to as *magic state distillation* [39, 74, 75].

1.4.7 Resource theories

Parts of this subsection are based on [19]. Quantum resource theories [35] 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 [76], coherence [34], magic [77, 78], and incompatibility [32]. There are multiple approaches: one can take some well-motivated free set of states and define the free channels as those preserving this set, or start with operationally motivated free operations and define the free states as those which can be generated using free operations alone.

There are several common resource quantifiers. Here we define them for states, although there exist analogous quantities for channels, measurements, and other quantum objects. Let $\mathcal{F}$ denote the free set of states. Firstly, we have the *robustness*:

$$\mathcal{R}_Y(\rho) = \min_{\sigma \in Y} \left\{ r \geq 0 \;\middle|\; \frac{\rho + r\sigma}{1+r} \in \mathcal{F} \right\} \tag{1.83}$$

where $Y \subseteq \mathcal{S}(\mathcal{H})$. If $Y = \mathcal{F}$ is the free set, this is the *standard robustness*. If $Y = \mathcal{S}(\mathcal{H})$ is the full set of states, this is the *generalised robustness*. If $Y = \{\frac{\mathbb{1}}{d}\}$ is the maximally mixed state, this is the *random robustness*.

We also have the *weight* of a resource, which will appear in Chapter 3.

$$\mathcal{W}(\rho) = \min_{\substack{\sigma \in \mathcal{F} \\ \tau \in \mathcal{S}}} \left\{ w \geq 0 \;\middle|\; \rho = (1-w)\sigma + w\tau \right\}. \tag{1.84}$$

1.4.7.1 Coherence

We now provide some more explicit detail on the resource theory of coherence, as it is will be of importance to Chapter 4.

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

$$\rho = \sum_x p_x |x\rangle\langle x| , \tag{1.85}$$

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

$$U = \sum_{x=1}^{d} e^{i\theta_x} |\pi(x)\rangle\!\langle x| \tag{1.86}$$

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 1.27. 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 1.28. Note that if a unitary cannot create any superpositions, then it must be of the form

$$U = \sum_{x} \alpha_x |\pi(x)\rangle\!\langle x| \tag{1.87}$$

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. (1.86), then it must neccesarily 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

$$\Delta(\rho) := \sum_{x} |x\rangle\!\langle x|\, \rho\, |x\rangle\!\langle x| \tag{1.88}$$

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 [34, 79] for summaries. We review several of them here. *Maximally Incoherent Operations* (MIO) are those which map incoherent states to other incoherent states, namely $\mathcal{E}$ is a MIO if $\mathcal{E}(\mathcal{I}) \subseteq \mathcal{I}$.

Lemma 1.29. 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 $\sum_x \alpha_x \left|\pi(x)\right\rangle\!\left\langle x\right|$ 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 quantum channels that can be realised via performing a global incoherent unitary on the input state and some incoherent ancillary state, followed by an incoherent measurement and classical processing [80]. 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 [80]

$$PIO \subsetneq SIO \subsetneq DIO \subsetneq MIO. \tag{1.89}$$

1.4.8 Random states and the symmetric subspace

The following content will prove relevant to Chapter 5.

Consider k quantum systems of local dimension d, i.e. some state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes k}$. Define unitaries U_α that permute the k systems for some permutation α in the symmetric group $\mathcal{S}_k$:

$$U_\alpha |x_1, \dots, x_k\rangle = \left| x_{\alpha^{-1}(1)}, \dots, x_{\alpha^{-1}(k)} \right\rangle. \tag{1.90}$$

Note that $U_\alpha U_\beta = U_{\alpha\beta}$. One can then define the symmetric subspace [81] as follows:

$$\mathrm{Sym}_d^k := \left\{ |\psi\rangle \in (\mathbb{C}^d)^{\otimes k} \quad : \quad U_\alpha |\psi\rangle = |\psi\rangle \quad \forall\, \alpha \in \mathcal{S}_k \right\}, \tag{1.91}$$

which can equivalently be defined as the span of states of the form $|\psi\rangle = |\phi\rangle^{\otimes k}$ for $|\phi\rangle \in \mathbb{C}^d$. We can write the projector Π_d^k onto the symmetric subspace as

$$\Pi_d^k := \mathop{\mathbb{E}}_{\alpha \in \mathcal{S}_k} [U_\alpha] = \frac{1}{k!} \sum_{\alpha \in \mathcal{S}_k} U_\alpha. \tag{1.92}$$

Now let $d\psi$ denote the Haar measure on quantum states. Then a well-known fact [81] is that integration over k copies of a state $|\psi\rangle \in \mathbb{C}^d$ is proportional to the projector onto the symmetric subspace, specifically we have

$$\binom{k+d-1}{k}\int d\psi\,|\psi\rangle\!\langle\psi|^{\otimes k} = \Pi_d^k. \tag{1.93}$$

1.4.9 Some important states and channels

Here we detail some miscellaneous objects that are of general importance in quantum information, and will appear intermittently throughout this thesis.

We define the 2 qubit Bell states as

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \qquad \left|\phi^-\right\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big) \tag{1.94}$$

$$\left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) \qquad \left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) \tag{1.95}$$

A *measure and prepare channel* is one that consists of performing a measurement on the given state, and preparing another state depending on the outcome. Specifically they can be written as

$$\Lambda(\rho) = \sum_\lambda \mathrm{Tr}\Big(G_\lambda \rho\Big)\sigma_\lambda, \tag{1.96}$$

for G_λ some POVM and σ_λ some set of states.

An extreme case of this is when the POVM is trivial (has one outcome). The resulting *preparation channel* simply corresponds to discarding the input and preparing another fixed state.

$$\Lambda(\rho) = \sigma \qquad \forall\rho \tag{1.97}$$

Intuitively, these channels can be thought of as the 'opposite' of unitary channels: unitary channels are precisely the channels that preserve all of the quantum information content of a state (and can be inverted), whereas preparation channels preserve none of the quantum information content of the original state.

We also remark that the dual of a measure and prepare channel is a *prepare and measure channel*:

$$\Lambda^*(M) = \sum_\lambda \mathrm{Tr}\Big(M\sigma_\lambda\Big)G_\lambda. \tag{1.98}$$

Measure and prepare channels also happen to coincide exactly with *entanglement breaking channels* [28], namely channels such that $\Lambda \otimes \mathbb{1}\rho$ is separable for all ρ – these are also 1-PEB channels as in Definition 1.22.

A channel Λ is *incompatibility breaking* if it maps any measurement assemblage to a compatible one in the Heisenberg picture, i.e. if $\Lambda^*(M_{a|x})$ is compatible for all $M_{a|x}$.

We now introduce some important one-parameter families of channels. In the below, we take the input $\rho \in \mathcal{S}(\mathbb{C}^d)$ to be a d-dimensional input state.

The *depolarising channel* is defined as

$$\Lambda_\mu(\rho) = \mu\rho + (1-\mu)\frac{\mathbb{1}}{d}. \tag{1.99}$$

The *dephasing channel* is defined as

$$\Lambda_\mu(\rho) = \mu\rho + (1-\mu)\mathrm{diag}(\rho), \tag{1.100}$$

where $\mathrm{diag}(\rho)$ signifies setting the off-diagonal terms in ρ to zero (note that this is a valid channel in itself).

The *erasure channel* is defined as

$$\Lambda_\eta(\rho) = \eta\rho + (1-\eta)\left|d\middle\rangle\middle\langle d\right|, \tag{1.101}$$

which formally maps a d dimensional state to a $d+1$ dimensional state.

The *isotropic states* [28] are defined as

$$\rho(\mu) = \mu\left|\phi^+\middle\rangle\middle\langle\phi^+\right| + (1-\mu)\frac{\mathbb{1}}{d}, \tag{1.102}$$

which is the (standard) Choi state of the depolarising channel.

Werner states [28, 82] are defined as those which are invariant under the action of $U \otimes U$, for any local unitary U. For two qubits one can write this family of states as

$$\rho(\mu) = \mu\left|\psi^-\middle\rangle\middle\langle\psi^-\right| + (1-\mu)\frac{\mathbb{1}}{d}. \tag{1.103}$$

We call a bipartite state ρ *local* if it cannot be used to witness Bell nonlocality. Formally, that means for all POVMs $M_{a|x}$ and $N_{b|y}$ there exists a local hidden variable model, i.e. probabilities $p(\lambda)$, $p(a|x,\lambda)$, $p(b|y,\lambda)$, such that

$$\mathrm{Tr}\Big(M_{a|x} \otimes N_{b|y}\rho\Big) = \sum_\lambda p(\lambda)p(a|x,\lambda)p(b|y,\lambda) \tag{1.104}$$

If a state is not *local* we refer to it as *nonlocal*.

We call a bipartite state ρ *unsteerable* if it cannot be used to witness quantum steering. Formally, that means for all POVMs $M_{a|x}$ there exists a local hidden state model, i.e. probabilities $p(\lambda)$, $p(a|x,\lambda)$, and states σ_λ, such that

$$\mathrm{Tr}_1\Big(M_{a|x} \otimes \mathbb{1}\ \rho\Big) = \sum_\lambda p(\lambda)p(a|x,\lambda)\sigma_\lambda \tag{1.105}$$

If a state is not *unsteerable* we refer to it as *steerable*.

An important fact is that there exist entangled yet unsteerable states, and steerable yet local states. A standard example of this is via the isotropic states in Eq. (1.102). It is known that these states are separable for $\mu \leq \frac{1}{d+1}$ [28], unsteerable for $\mu \leq \frac{3d-1}{d+1}(d-1)^{d-1}d^{-d}$ [31], and local for $\mu \leq \frac{(d-1)^{(d-1)}(3d-1)}{(d+1)d^d}$ [3], for which there exists a separation for all dimensions d.

We summarise some of the above in the following table, which also depicts some relationships between the states and channels via standard channel-state duality.

Channel	State
$\Lambda_\rho(\sigma) = \mathrm{Tr}_2(\mathbb{1} \otimes \sigma\rho) \quad \longleftrightarrow$	$\rho_\Lambda = \Lambda \otimes \mathbb{1}\, |\Phi^+\rangle\langle\Phi^+|$
Λ CP	$\rho \geq 0$
Λ TP	$\mathrm{Tr}(\rho) = 1$
Λ unitary	ρ pure
Λ prepare	ρ product
Λ n-PEB	$SN(\rho) = n$
Λ incompatibility breaking	ρ unsteerable
Λ dephasing	isotropic

Table 1.3: Some special channels and their corresponding Choi states, see Section 1.4.1 for details of this correspondence.

1.5 Concluding remarks

In this introductory chapter, we have provided some context to the field of a whole, and set the stage for the remaining chapters. We reviewed key concepts from linear algebra and finite-dimensional quantum mechanics, as well as discussing various notions from quantum information which will be important background for the rest of this thesis. Next, in Chapter 2 we will outline our first research contribution by studying quantum steering in network scenarios.

Chapter 2

Network quantum steering

Chapter Summary

The development of large-scale quantum networks promises to bring a multitude of technological applications as well as shed light on foundational topics, such as quantum nonlocality. It is particularly interesting to consider scenarios where sources within the network are statistically independent, which leads to so-called network nonlocality, even when parties perform fixed measurements. Here we promote certain parties to be trusted and introduce the notion of network steering and network local hidden state (NLHS) models within this paradigm of independent sources. In one direction, we show how results from Bell nonlocality and quantum steering can be used to demonstrate network steering. We further show that it is a genuinely novel effect, by exhibiting unsteerable states that nevertheless demonstrate network steering, based upon entanglement swapping, yielding a form of activation. On the other hand, we provide no-go results for network steering in a large class of scenarios, by explicitly constructing NLHS models.

This chapter is based on the following publication:

Benjamin DM Jones, Ivan Šupić, Roope Uola, Nicolas Brunner, and Paul Skrzypczyk.
Network Quantum Steering.
Physical Review Letters, 127(17):170405, 2021.

Relevant background: quantum nonlocality and steering (Section 1.4.4 and Section 1.4.5), miscellaneous states and channels (Section 1.4.9): such as separable, unsteerable and local states, Werner states, and the erasure channel.

Page

Contents

2.1 Introduction

Quantum correlations expose a rich structure when considered in scenarios with many parties. A case of particular interest is that of quantum networks, featuring a number of distant parties connected by several quantum sources. Significant further work is still required to reach a deeper theoretical understanding of these scenarios, whilst also keeping inline with experimental and technological developments towards quantum networks (with applications such as secure quantum communication) [83].

Recently, a generalisation of the concept of Bell locality [56] was proposed to tackle the question of quantum nonlocality in networks – see [61] for a recent review. The key idea is to consider the various sources in the network to be statistically independent [84–86]. This independence leads to non-convexity in the space of relevant correlations, undermining the use of pre-existing tools and creating a need for new approaches, both analytically [87–95] and numerically [96]. The network structure offers new interesting effects, such as the possibility to certify quantum nonlocality "without inputs" (i.e. a scenario where each party performs a fixed quantum measurement) [63, 85, 86, 97, 98]. Also, the use of non-classical measurements allows for novel forms of quantum nonlocal correlations that are genuine to networks [99]. In parallel, several works have explored the structure of quantum states assuming a certain underlying network structure [62, 100–102].

A central scenario of study has been the so-called "triangle network" [62, 93, 97], consisting of three parties, pairwise connected by independent sources, each performing a fixed measurement, yielding statistics $p(a,b,c)$. Whilst it is possible to embed standard Bell nonlocality into this scenario [86], the existence of correlations with a high degree of symmetry and no classical description indicate that these phenomena may be unique to networks [63].

In this chapter, motivated by the difficulty in characterising quantum networks both conceptually and computationally, we consider quantum network scenarios in which some of the parties are trusted while the others are untrusted. This naturally connects to the notion of quantum steering [65] (see [30, 31] for reviews, and Section 1.4.5 for an overview) which captures quantum correlations in a scenario involving a trusted and an untrusted party. While the notion of multipartite steering has been previously considered [103, 104], this work explores a different direction, targeting the scenario of networks with independent sources.

Our main focus here will be on the simplest setting of a linear network with trusted endpoints and intermediate untrusted parties who each perform a fixed measurement. We begin by formalising the notions of *network local hidden state* (NLHS) models, and network steering. We then leverage standard steering and nonlocality scenarios to provide simple examples of network steering. Next, we outline a surprising effect in which two-way unsteerable states can demonstrate network steering through entanglement swapping, leading to a form of activation. Finally, we characterise some natural scenarios that always admit an NLHS model by identifying properties of the sources. We conclude the chapter by listing some promising future avenues for research.

2.1.1 Summary of results

Main conceptual contributions:

- We introduce a novel definition of quantum steering for networks.
- We provide no-go results of when network steering is not possible
- We give concrete examples of network steering, including a form of activation using unsteerable states.

Main technical calculations:

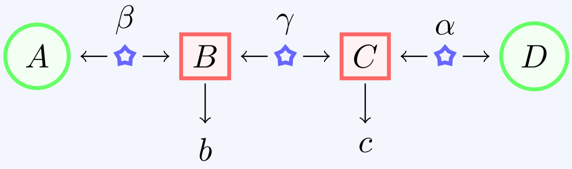
Lemma 2.8. Define the Doubly-Erased Werner (DEW) state as

$$\rho_{\texttt{DEW}}(\eta,\omega) := \Lambda_\eta \otimes \Lambda_\eta \left(\omega \, |\psi^-\rangle\!\langle\psi^-| + (1-\omega)\frac{\mathbb{1}}{4} \right), \tag{2.1}$$

where $\Lambda_\eta(\rho) = \eta\rho + (1-\eta)\mathrm{Tr}(\rho)\,|d\rangle\!\langle d|$ is the erasure channel and $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. Then projecting $|\psi^-\rangle\!\langle\psi^-|$ onto two copies of $\rho_{\texttt{DEW}}(\eta,\omega)$ leads to $\rho_{\texttt{DEW}}(\eta,\omega^2)$, with probability $\eta^2/4$. Namely,

$$\mathrm{Tr}_{BC}\left(\left[\mathbb{1}_A \otimes |\psi^-\rangle\langle\psi^-|_{BC} \otimes \mathbb{1}_D \right] \left[\rho_{\text{DEW}}(\eta,\omega)_{AB} \otimes \rho_{\text{DEW}}(\eta,\omega)_{CD} \right] \right) = \frac{\eta^2}{4}\rho_{\text{DEW}}(\eta,\omega^2)_{AD} \quad (2.2)$$

Theorem 2.9. Consider a four party network scenario with trusted endpoints and untrusted central parties who perform fixed measurements, as in the following figure (also Fig. 2.3(b)):



Ordering the sources as $\{\rho^{AB},\ \rho^{B'C},\ \rho^{C'D}\}$ and denoting **SEP** as the set of separable states, **LOC** as the set of Bell-local states, and $\mathbf{UNSTEER}_{\rightarrow}$ as the set of unsteerable states (in an appropriate direction) we have that $\{$**SEP**, **LOC**, **SEP**$\}$, $\{\mathbf{UNSTEER}_{\leftarrow}$, **SEP**, $\mathbf{UNSTEER}_{\rightarrow}\}$, $\{$**SEP**, $\mathbf{UNSTEER}_{\rightarrow}$, $\mathbf{UNSTEER}_{\rightarrow}\}$ and (by symmetry) $\{\mathbf{UNSTEER}_{\leftarrow}$, $\mathbf{UNSTEER}_{\leftarrow}$, **SEP**$\}$ all admit *network local hidden state* models, for any measurements. That is for any measurements $M_b^{BB'}$ and $M_c^{CC'}$, the resulting network assemblage

$$\sigma_{b,c}^{AD} = \mathrm{Tr}_{BB'CC'}\left(\left[\mathbb{1}^A \otimes M_b^{BB'} \otimes M_c^{CC'} \otimes \mathbb{1}^D\right]\rho^{AB} \otimes \rho^{B'C} \otimes \rho^{C'D}\right), \quad (2.3)$$

can be written in the following network local hidden state form

$$\sigma_{b,c}^{AD} = \sum_{\alpha,\beta,\gamma} p(\alpha)p(\beta)p(\gamma)p(a|\beta,\gamma)p(b|\alpha,\gamma)\sigma_\alpha^A \otimes \sigma_\beta^D. \quad (2.4)$$

for probability distributions $p(\alpha)$, $p(\beta)$, $p(\gamma)$, $p(a|\beta,\gamma)$, $p(b|\alpha,\gamma)$, and states σ_α^A, σ_β^D. This is captured in Fig. 2.2(b).

Open questions:

- Understanding the role of measurement incompatibility in network steering scenarios.
- Obtaining tight classifications of network local hidden state models in terms of properties of the sources (separable, unsteerable, local).

Prior work and concepts:

- Quantum nonlocality in networks [61], for example in the triangle network [62, 63]. Specifically the idea of when network nonlocality is simply standard Bell nonlocality 'in disguise', and when there is some novel phenomena unique to networks.
- Quantum steering [30, 31], and the idea of trusted and untrusted parties, and semi-device independent quantum information. Furthermore, the idea of encoding all of the relevant information as sets of sub-normalised states (i.e. steering assemblages).

2.2 Network steering scenarios

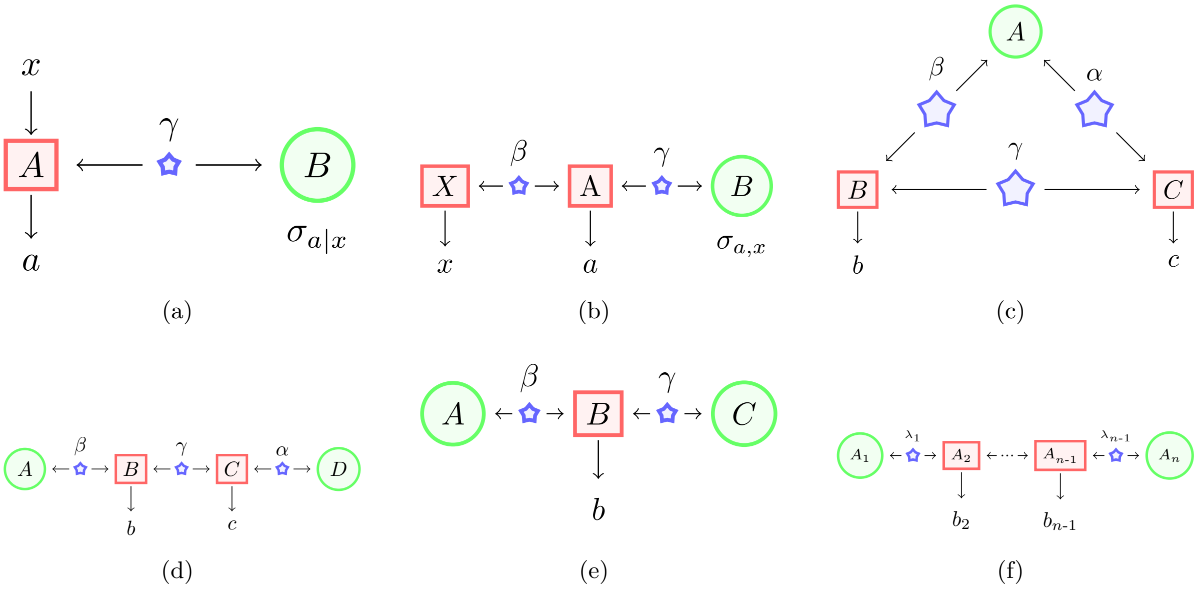


Figure 2.1: Network steering scenarios. Green circles represent trusted parties, and red squares represent untrusted parties. (a) Standard steering scenario. (b) Steering scenario without inputs. (c) Triangle scenario with a trusted party. (d) Triangle scenario interpreted as a line. (e) Entanglement swapping scenario with trusted endpoints. (f) Generalised line scenario with trusted endpoints.

Let us introduce our main new notion, that of network steering. Suppose we have a collection of independent sources which distribute quantum states to a subset of parties. In the standard network nonlocality scenario all parties are assumed to be untrusted, and to perform 'black-box' measurements. Here, in contrast, inspired by the steering scenario, we will consider allowing some of the parties to be trusted. We refer to this general set-up as *network steering*.

Definition 2.1. A *network steering scenario* is described by a graphical structure, where nodes represent parties, and edges represent quantum sources shared between the corresponding parties. Each party may be untrusted, meaning that we only assume access to the resulting output probability distribution, or trusted, representing the ability to perform full quantum tomography, and hence the resulting output data is a quantum state. In addition, each untrusted party may receive a classical input, as in the standard nonlocality case.

We will be interested in the (sub-normalised) states that are prepared for the trusted parties by the measurements of the untrusted parties. Note that if all the parties are untrusted, the quantity of interest is the observed statistics $p(a, b, \dots | x, y, \dots)$, and we recover the standard notion of network nonlocality. When at least one party is trusted this is replaced by some collection of quantum states $\sigma_{a,b,\dots|x,y,\dots}$. Let us see a concrete example.

Consider a simple scenario with three parties and two sources (see Fig. 2.1(e)), as in entanglement swapping [105]. Here the first two parties share a state ρ^{AB} and the second and third parties share a state $\rho^{B'C}$, and the central party performs a fixed measurement $M_b^{BB'}$. The sub-normalised states prepared for A and C by this measurement are

$$\sigma_b^{AC} = \mathrm{Tr}_{BB'}\Big(\Big[\mathbb{1}^A \otimes M_b^{BB'} \otimes \mathbb{1}^C\Big]\rho^{AB} \otimes \rho^{B'C}\Big), \tag{2.5}$$

which occur with probability $p(b) = \mathrm{Tr}(\sigma_b^{AC})$. We will refer to objects such as $\{\sigma_b\}_b$ as a *network assemblage*.

In order to determine when this network assemblage demonstrates network steering we need to introduce the notion of a *network local hidden state* (NLHS) model, which in this case takes the form

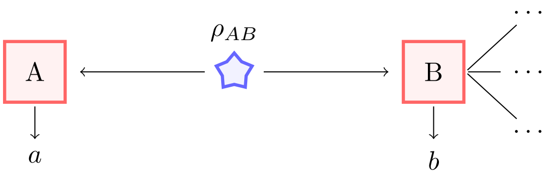
$$\sigma_b^{AC} = \sum_{\beta,\gamma} p(\beta)p(\gamma)\; p(b|\beta,\gamma)\; \sigma_\beta^A \otimes \sigma_\gamma^C, \tag{2.6}$$

where β and σ_β^A are the hidden variable and hidden states of the first source, γ and σ_γ^C those of the second source, and $p(b|\beta,\gamma)$ the local response function of Bob. If there is no such model that can explain the network assemblage σ_b, then we say it demonstrates *network steering*. Interestingly, whereas conventional quantum steering requires multiple measurements to be performed by the untrusted party, just as with network nonlocality, we shall see here that even a fixed measurement can suffice to demonstrate network steering.

We now make some basic observations and simplifications about network steering scenarios. A key observation that will prove useful is the following equivalence between networks, a generalisation from the network nonlocality case [86].

Observation 2.2. Any network with an untrusted party A that has an input x, received with probability $p(x)$, and outcome a, is equivalent to a network with an additional untrusted party A' who shares an additional source with A, neither of whom now has an input. In this new network, the outcome of A' is x, the old input of A. The relation between the network assemblages in the first and second scenarios are $p(x)\sigma^{A\ldots}_{a,\ldots|x,\ldots} = \sigma^{AA'\ldots}_{a,x,\ldots}$.

We also note that we can take this additional source to be separable without loss of generality. That is, in the following scenario, we can take ρ_{AB} to be separable without loss of generality.



Suppose the overall state (or probabilities, if all other nodes are untrusted) is

$$\sigma_{a,b,\ldots} = \mathrm{Tr}_{AB\ldots}\Big(M^A_a \otimes M^{B\ldots}_b \otimes \ldots \Big[\rho_{AB} \otimes \ldots\Big]\Big) \tag{2.7}$$

$$= \mathrm{Tr}_{B\ldots}\Big(M^{B\ldots}_b \otimes \ldots \Big[\mathrm{Tr}_1\Big(M_a \otimes \mathbb{1}\rho_{AB}\Big) \otimes \ldots\Big]\Big). \tag{2.8}$$

Now set ρ'_{AB} as

$$\rho'_{AB} = \sum_{a'} |a'\rangle\langle a'| \otimes \mathrm{Tr}_{A'}(M_{a'} \otimes \mathbb{1}\rho_{A'B}) \tag{2.9}$$

which is normalised. Then also set

$$N^A_a = |a\rangle\langle a| \tag{2.10}$$

This gives

$$\mathrm{Tr}_{AB\ldots}\Big(N^A_a \otimes M^{B\ldots}_b \otimes \ldots \Big[\rho'_{AB} \otimes \ldots\Big]\Big) = \mathrm{Tr}_{B\ldots}\Big(M^{B\ldots}_b \otimes \ldots \Big[\mathrm{Tr}_1\Big(M_a\rho_{AB}\Big) \otimes \ldots\Big]\Big) \tag{2.11}$$

as before, reproducing the same assemblage/probabilities using a separable state and projective measurement N_a.

Observation 2.3. Endpoint sources between untrusted nodes with no inputs can be taken to be separable.

By virtue of the fact that quantum mechanics admits local tomography, we can also note the following:

Observation 2.4. A trusted party connected to n independent sources can without loss of generality be replaced by n endpoint trusted parties, each connected to a single source.

This allows us, for example, to interpret linear networks as rings with a single trusted party – e.g. the four party linear network with trusted endpoints can also be viewed as the triangle network where one of the parties is trusted, as in Fig. 2.1(c) and Fig. 2.1(d). This observation motivates our choice to focus our discussion on linear networks, which we understand now to be relevant for more complex, non-linear networks.

We further remark that in Eq. (2.6), each σ_b^{AC} is in fact separable. Thus the presence of entanglement in any single σ_b suffices to rule out an NLHS model, and therefore demonstrates network steering.

The above generalises in a natural way to the n-party line network depicted in Fig. 2.1(f), with outcomes $b_2, \dots, b_{n-1}$. We explicitly include the straightforward generalisation of Eq. (2.5) and Eq. (2.6) as follows.

For n parties, here an observed set of states would be described by

$$\sigma^{A_1 A_n}_{b_2,\dots,b_{n-1}} = \mathrm{Tr}_{A_2 A_2' \dots A_{n-1} A_{n-1}'} \Bigg(\Big[\mathbb{1}^{A_1} \otimes M_{b_2}^{A_2 A_2'} \otimes \cdots \otimes M_{b_{n-1}}^{A_{n-1} A_{n-1}'} \otimes \mathbb{1}^{A_n} \Big] \times \rho^{A_1 A_2} \otimes \rho^{A_2' A_3} \otimes \cdots \otimes \rho^{A_{n-1}' A_n} \Bigg). \tag{2.12}$$

The NLHS condition here generalises to

$$\sigma^{A_1 A_n}_{b_2,\dots,b_{n-1}} = \sum_{\lambda_1,\dots,\lambda_{n-1}} p(\lambda_1) \dots p(\lambda_{n-1}) \times p(b_2|\lambda_1, \lambda_2) \dots p(b_{n-1}|\lambda_{n-2}, \lambda_{n-1}) \times \sigma^{A_1}_{\lambda_1} \otimes \sigma^{A_n}_{\lambda_{n-1}}. \tag{2.13}$$

Hence we see that the following observation holds generally:

Observation 2.5. For any linear network with trusted endpoints, the entanglement of a single $\sigma_{b_2,\dots,b_{n-1}}$ is sufficient to rule out an NLHS model, and thus demonstrate network steering.

This observation will be important to provide our example of activation in Section 2.3.2, in which we show that two-way unsteerable states can be used to demonstrate network steering.

2.3 Demonstrating network steering.

2.3.1 Porting existing results from nonlocality and steering

We now begin our exploration of demonstrating network steering, and explain how and when steerable states will lead to network steering when placed in a network. We consider first the scenario of Fig. 2.1(b). If one source distributes a state which is steerable in the standard steering scenario, then Observation 2.3 would seem to indicate that even if the second source distributes only separable states (which we will refer to as a *separable source*), it should still be possible to use this to encode the "input" to the measurement, and thus demonstrate network steering. Here we make this intuition precise.

Consider the network scenario depicted in Fig. 2.1(b), with two untrusted parties without inputs steering a third, leading to a network assemblage $\sigma_{a,x}$. Here the NLHS condition reads

$$\sigma_{a,x} = \sum_{\beta,\gamma} p(\beta)p(\gamma)\ p(x|\beta)p(a|\beta,\gamma)\sigma_\gamma. \tag{2.14}$$

We can then observe the following:

Lemma 2.6. If $\sigma_{a,x}$ has an NLHS model, then $\sigma_{a|x} := \sigma_{a,x}/p(x)$ has an LHS model, where $p(x) = \mathrm{Tr}(\sum_a \sigma_{a,x})$.

Proof. We can write Eq. (2.14) as

$$\sigma_{a,x} = p(x)\sum_{\gamma} p(\gamma)\ p(a|x,\gamma)\sigma_\gamma \tag{2.15}$$

where $p(x) := \mathrm{Tr}(\sum_a \sigma_{a,x}) = \sum_\beta p(\beta)p(x|\beta)$ and $p(a|x,\gamma) := \frac{1}{p(x)}\sum_\beta p(\beta)p(x|\beta)p(a|\beta,\gamma)$. The result then follows. □

This is an analogous result to that proved in [86] relating Bell scenario statistics $p(a,b|x,y)$ to network nonlocality statistics $p(a,b,x,y)$, the corresponding distribution without inputs. We link this to the scenario from Fig. 2.1(e) where both endpoints are trusted.

Lemma 2.7. If σ_b has an NLHS model, then $\sigma_{b,x} := \mathrm{Tr}_1([M_x^A \otimes \mathbb{1}^C]\sigma_b)$ has an NLHS model, for any measurement M_x.

Proof. When σ_b has an NLHS model of the form in Eq. (2.6), it follows that

$$\sigma_{b,x} = \sum_{\beta,\gamma} p(\beta)p(\gamma)\ \mathrm{Tr}(M_x\sigma_\beta)p(b|\beta,\gamma)\sigma_\gamma, \tag{2.16}$$

which is an NLHS model of the form in Eq. (2.14), with $p(x|\beta) := \mathrm{Tr}(M_x\sigma_\beta)$. □

Putting this together, suppose that $\rho^{B'C}$ is steerable, such that $\sigma_{b|x} := \mathrm{Tr}(M_{b|x} \otimes \mathbb{1}\rho^{B'C})$ demonstrates steering for some $M_{b|x}$. Let $\rho^{AB} = \sum_x \frac{1}{d}\,|x\rangle\!\langle x| \otimes |x\rangle\!\langle x|$ where d is the number of measurements x, and $\{|x\rangle\}_x$ form an orthonormal basis, and $M_b = \sum_{x'} |x'\rangle\!\langle x'| \otimes M_{b|x'}$. The resulting network assemblage σ_b, from Eq. (2.5), is seen to be

$$\sigma_b = \sum_x \frac{1}{d}\,|x\rangle\!\langle x| \otimes \sigma_{b|x}. \tag{2.17}$$

Now, from the above claims we can see that this must demonstrate network steering. Indeed, if instead it had an NLHS model, then from Lemma 2.7, $\sigma_{b,x} := \mathrm{Tr}_1(|x\rangle\langle x| \otimes \mathbb{1}^C \sigma_b) = \frac{1}{d}\sigma_{b|x}$ would have an NLHS model with $p(x) = 1/d$. Then, from Lemma 2.6, $\sigma_{b,x}$ would have an LHS model, but by assumption it does not. This shows that all steerable states can lead also to network steering when placed in a network with an appropriate separable state. Interestingly, this occurs even though σ_b is separable.

Similar arguments apply for showing that in the line with four parties from Fig. 2.1(d), we can always demonstrate network steering when the central state is nonlocal, and the adjacent endpoint sources are suitable separable states, providing the inputs. That is, if $\sigma_{b,c}$ has an NLHS model, then by A and D applying measurements M_x and M_y the associated probability distributions $p(b,c,x,y)$ and $p(b,c|x,y)$ necessarily have *network local hidden variable* (NLHV) and LHV models respectively (see [86]). So for any nonlocal central source, we can find appropriate measurements and adjacent separable sources such that $\sigma_{b,c}$ demonstrates network steering.

2.3.2 Activation

The above constructions of network steering relied on steering or nonlocality in standard scenarios. Here we show that network steering is possible even when using only (two-way) unsteerable states, which can be viewed as a form of activation. Note that this complements previous examples of activation of steering in the standard bipartite scenario [106].

Recall that the erasure channel is given by (see also Eq. (1.101))

$$\Lambda_\eta(\rho) = \eta\rho + (1-\eta)\mathrm{Tr}(\rho)\,|d\rangle\langle d|\,. \tag{2.18}$$

For example, this channel acting on a qubit state would result in a qutrit state, where now the original qubit state ρ is viewed as being embedded in the $\{|0\rangle, |1\rangle\}$ subspace, and loss of the system is represented by the $|2\rangle$ state.

We define the Doubly-Erased Werner (DEW) state as the two-qubit Werner state (see Eq. (1.103)) after both subsystems have undergone an identical erasure channel:

$$\rho_{\mathrm{DEW}}(\eta,\omega) := \Lambda_\eta \otimes \Lambda_\eta\Big(\omega\,|\psi^-\rangle\langle\psi^-| + (1-\omega)\frac{\mathbb{1}}{4}\Big), \tag{2.19}$$

where $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. $\rho_{\mathrm{DEW}}(\eta,\omega)$ is entangled when $\omega > \frac{1}{3}$ (and $\eta \neq 0$) [3], and is unsteerable (in both directions) when $\eta \leq \frac{2}{3}(1-\omega)$. The latter follows from a result in [107], which states that $\Lambda_\eta \otimes \mathbb{1}\rho^{AB}$ is unsteerable from Alice to Bob (for arbitrary measurements) if

$$\max_{\mathbf{x}}\left[(1-3\eta)|\mathbf{a}.\mathbf{x}| + \frac{3\eta}{2}(1+(\mathbf{a}\cdot\mathbf{x})^2) + \|T\mathbf{x}\|\right] \leq 1. \tag{2.20}$$

where $\mathbf{a}$ is Alice's local Bloch vector, T is the bipartite correlation matrix with entries $T = \mathrm{Tr}(\rho\ \sigma_i \otimes \sigma_j)$ for σ_i the Pauli matrices, and the maximisation is over unit vectors $\mathbf{x}$ in

$\mathbb{R}^3$. For $\rho^{AB} = \rho_W(\omega) = \omega\,|\psi^-\rangle\!\langle\psi^-| + (1-\omega)\mathbb{1}/4$ the Werner state, we have $a = 0$ and $T = \mathrm{diag}(-\omega, -\omega, -\omega)$ and this condition becomes

$$\eta \leq \frac{2}{3}(1-\omega). \tag{2.21}$$

Now as $\mathbb{1}^A \otimes \Omega^B[\rho^{AB}]$ is unsteerable from Alice to Bob for any channel Ω if ρ^{AB} is unsteerable from Alice to Bob [108], we have that the the Doubly-Erased Werner (DEW) state

$$\rho_{\text{DEW}}(\eta,\omega) := \Lambda_\eta \otimes \Lambda_\eta\Big(\omega\,|\psi^-\rangle\!\langle\psi^-| + (1-\omega)\frac{\mathbb{1}}{4}\Big) \tag{2.22}$$

is unsteerable in both directions for $\eta \leq \frac{2}{3}(1-\omega)$.

We also have that in the context of entanglement swapping, projecting $|\psi^-\rangle\!\langle\psi^-|$ onto two copies of $\rho_{\text{DEW}}(\eta,\omega)$ leads to $\rho_{\text{DEW}}(\eta,\omega^2)$ (with probability $\eta^2/4$), that is to a DEW state with squared visibility.

Lemma 2.8. Projecting $|\psi^-\rangle\!\langle\psi^-|$ onto two copies of $\rho_{\text{DEW}}(\eta,\omega)$ leads to $\rho_{\text{DEW}}(\eta,\omega^2)$, with probability $\eta^2/4$. Namely,

$$\mathrm{Tr}_{BC}\Big(\Big[\mathbb{1}_A \otimes |\psi^-\rangle\!\langle\psi^-|_{BC} \otimes \mathbb{1}_D\Big]\Big[\rho_{\text{DEW}}(\eta,\omega)_{AB} \otimes \rho_{\text{DEW}}(\eta,\omega)_{CD}\Big]\Big) = \tfrac{\eta^2}{4}\rho_{\text{DEW}}(\eta,\omega^2)_{AD} \tag{2.23}$$

Proof. Expanding out the DEW state gives

$$\begin{aligned}\Lambda_\eta \otimes \Lambda_\eta \rho_W(\omega) =& \eta^2\rho_W(\omega) + \eta(1-\eta)\frac{\mathbb{1}_2}{2} \otimes |2\rangle\!\langle 2| \\ &+ \eta(1-\eta)\,|2\rangle\!\langle 2| \otimes \frac{\mathbb{1}_2}{2} + (1-\eta)^2\,|2\rangle\!\langle 2| \otimes |2\rangle\!\langle 2|\,.\end{aligned} \tag{2.24}$$

Now consider entanglement swapping with projector $|\psi^-\rangle\!\langle\psi^-|$ (on the $\{|0\rangle, |1\rangle\}$ subspace) onto two DEW states. We can write this as

$$\mathrm{Tr}_{BB'}\Big(\mathbb{1}^A \otimes |\psi^-\rangle\!\langle\psi^-|^{BB'} \otimes \mathbb{1}^C\Big[\Lambda_\eta \otimes \Lambda_\eta\rho_W(\omega)^{AB}\Big] \otimes \Big[\Lambda_\eta \otimes \Lambda_\eta\rho_W(\omega)^{B'C}\Big]\Big) \tag{2.25}$$

$$= \mathrm{Tr}_{BB'}\Big(\mathbb{1} \otimes |\psi^-\rangle\!\langle\psi^-| \otimes \mathbb{1}\Big[\eta^2\rho_W(\omega) + \eta(1-\eta)\,|2\rangle\!\langle 2| \otimes \frac{\mathbb{1}_2}{2} \tag{2.26}$$

$$+ \eta(1-\eta)\frac{\mathbb{1}_2}{2} \otimes |2\rangle\!\langle 2| + (1-\eta)^2\,|2\rangle\!\langle 2| \otimes |2\rangle\!\langle 2|\Big]^{\otimes 2}\Big). \tag{2.27}$$

Note that any term with $\langle\psi^-|$ acting on a $|2\rangle$ subspace vanishes, so we can simplify this to

$$\begin{aligned}
&\mathrm{Tr}_{BB'}\Big(\mathbb{1}\otimes|\psi^-\rangle\!\langle\psi^-|\otimes\mathbb{1}\Big[\eta^4\rho_W(\omega)\otimes\rho_W(\omega)+\eta^3(1-\eta)\rho_W(\omega)\otimes\frac{\mathbb{1}_2}{2}\otimes|2\rangle\!\langle 2| \\
&\qquad +\eta^3(1-\eta)\,|2\rangle\!\langle 2|\otimes\frac{\mathbb{1}_2}{2}\otimes\rho_W(\omega)+\eta^2(1-\eta)^2\,|2\rangle\!\langle 2|\otimes\frac{\mathbb{1}_2}{2}\otimes\frac{\mathbb{1}_2}{2}\otimes|2\rangle\!\langle 2|\Big]\Big) \qquad (2.28)\\
&=\frac{1}{4}\Big(\eta^4\rho_W(\omega^2)+\eta^3(1-\eta)\frac{\mathbb{1}_2}{2}\otimes|2\rangle\!\langle 2| \qquad (2.29)\\
&\qquad +\eta^3(1-\eta)\,|2\rangle\!\langle 2|\otimes\frac{\mathbb{1}_2}{2}+\eta^2(1-\eta)^2\,|2\rangle\!\langle 2|\otimes|2\rangle\!\langle 2|\Big) \qquad (2.30)\\
&=\frac{\eta^2}{4}\Lambda_\eta\otimes\Lambda_\eta\rho_W(\omega^2) \qquad (2.31)\\
&=\frac{\eta^2}{4}\rho_{\mathrm{DEW}}(\eta,\omega^2). \qquad (2.32)
\end{aligned}$$

In lines Eq. (2.28) - Eq. (2.29) we used the fact that entanglement swapping of two Werner states leads to another Werner state with the product of the visibilities. Hence entanglement swapping of two DEW states (with the same erasure parameter and Werner visibility) leads to another DEW state with the Werner visibility equal to the square of the original Werner visibility. □

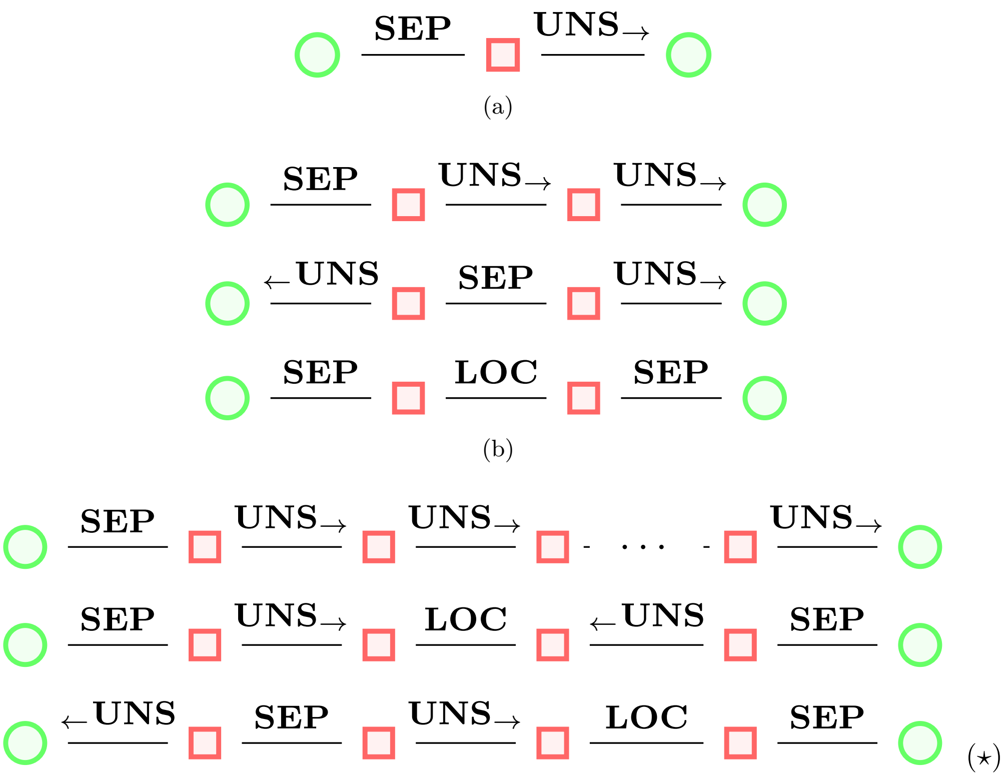
Consider now the line network from Fig. 2.1(f) with each source distributing a copy of $\rho_{\mathrm{DEW}}(\eta,\omega)$, and all untrusted parties performing the fixed measurement $M_0=|\psi^-\rangle\!\langle\psi^-|$, $M_1=\mathbb{1}-|\psi^-\rangle\!\langle\psi^-|$, leading to the network assemblage $\sigma_{b_2,\ldots,b_{n-1}}$. Now, if we choose $\eta=\frac{2}{3}(1-\omega)$ and $1>\omega>(\frac{1}{3})^{\frac{1}{n}}$, then each DEW is entangled but unsteerable, and we find, due to the entanglement-swapping property noted above, that the element $\sigma_{0,\ldots,0}$ (corresponding to a successful swap in each case), will be proportional to the state $\rho_{\mathrm{DEW}}(\eta,\omega')$ with $\omega'>\frac{1}{3}$, and therefore entangled. From Observation 2.5, this precludes an NLHS model description, and therefore demonstrates network steering, even though each DEW state was unsteerable.

2.4 Classes of NLHS models

2.4.1 The simplest scenario

We finish our exploration by considering to what extent the properties of the quantum sources directly affect the possibility of an NLHS model. We will refer to a source as being *separable*, *unsteerable* or *local* if it is only capable of generating separable, unsteerable or local states respectively (also see Section 1.4.9 for definitions here). As an illustrative example, in the three-party scenario of Fig. 2.1(e) if one source is separable and the other source is unsteerable (towards the trusted party), then for any fixed central measurement the network assemblage σ_b will always be NLHS. Indeed taking $\rho^{AB}=\sum_\gamma p(\gamma)\sigma_\gamma^A\otimes\sigma_\gamma^B$, and inserting into Eq. (2.5) gives

$$\sigma_b=\sum_\gamma p(\gamma)\;\sigma_\gamma^A\otimes\mathrm{Tr}_{BB'}\Big(M_b\otimes\mathbb{1}^C\Big[\sigma_\gamma^B\otimes\rho^{B'C}\Big]\Big). \qquad (2.33)$$



(a)

(b)

(c)

Figure 2.2: Classifying the structure of some NLHS models. Green circles represent trusted parties, and red squares represent untrusted parties who perform a fixed measurement. In the scenario of Fig. 2.1(e), when one source is separable (**SEP**), this acts as an input to the adjacent measurements, and by taking the second source as unsteerable in an appropriate direction (**UNS**$_\rightarrow$) then this always leads to an NLHS model. Similar results hold in the "unwrapped" triangle scenario (Fig. 2.1(d)) and general line scenarios, where now sources can also be taken as local, (**LOC**). The example indicated by ($\star$) is discussed in the main text, at the end of Section 2.4.3.

Defining $M_{b|\gamma} := \mathrm{Tr}_B(M_b \sigma_\gamma^B \otimes \mathbb{1}^C)$ as a set of valid measurement operators leads us to write

$$\sigma_b = \sum_\gamma p(\gamma)\ \sigma_\gamma^A \otimes \mathrm{Tr}_{B'}\Big(M_{b|\gamma} \otimes \mathbb{1}^C \Big[\rho^{B'C}\Big]\Big). \tag{2.34}$$

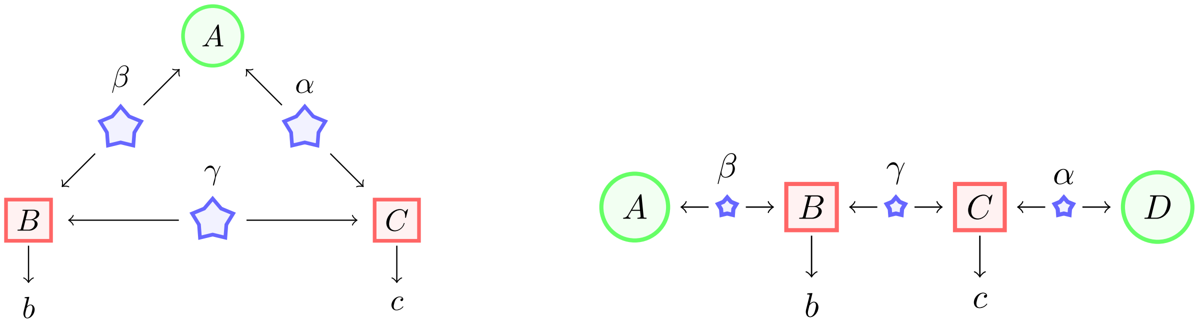
If $\rho^{B'C}$ is unsteerable from B' to C, this allows us to extract a LHS model, yielding

$$\begin{aligned}\sigma_b &= \sum_\gamma p(\gamma)\ \sigma_\gamma^A \otimes \Big(\sum_\lambda p(\lambda)\ p(b|\lambda,\gamma)\sigma_\lambda^C\Big) && (2.35)\\ &= \sum_{\gamma,\lambda} p(\gamma)p(\lambda)\ p(b|\lambda,\gamma)\sigma_\gamma^A \otimes \sigma_\lambda^C, && (2.36)\end{aligned}$$

which is an NLHS model (Eq. (2.6)). Hence the combination of a separable and unsteerable source (to the trusted party) can never lead to network steering, as shown in Fig. 2.2(a).

2.4.2 The triangle scenario

We can naturally extend this to the line with four parties and trusted endpoints, equivalently viewing this as the triangle network with a single trusted party (Fig. 2.3(a)).



(a)

(b)

Figure 2.3: Line scenario with four parties, or alternatively the triangle scenario with a single trusted party.

Here the quantum description would be

$$\sigma^{AD}_{b,c} = \mathrm{Tr}_{BB'CC'}\left(\left[\mathbb{1}^A \otimes M^{BB'}_b \otimes M^{CC'}_c \otimes \mathbb{1}^D\right]\rho^{AB}\otimes\rho^{B'C}\otimes\rho^{C'D}\right), \tag{2.37}$$

and the network assemblage $\sigma^{AD}_{b,c}$ would admit an NLHS description if it could be written in the form

$$\sigma^{AD}_{b,c} = \sum_{\alpha,\beta,\gamma} p(\alpha)p(\beta)p(\gamma)p(a|\beta,\gamma)p(b|\alpha,\gamma)\sigma^A_\alpha\otimes\sigma^D_\beta. \tag{2.38}$$

We will now consider how NLHS models can naturally arise by considering properties of the three sources. If the central source is separable, i.e. $\rho^{B'C} = \sum_\gamma p(\gamma)\sigma^{B'}_\gamma\otimes\sigma^C_\gamma$. Inserting this into Eq. (2.37) yields

$$\begin{aligned}
\sigma^{AD}_{b,c} &= \mathrm{Tr}_{BB'CC'}\left(\left[\mathbb{1}^A \otimes M^{BB'}_b \otimes M^{CC'}_c \otimes \mathbb{1}^D\right]\rho^{AB}\otimes\rho^{B'C}\otimes\rho^{C'D}\right) && (2.39)\\
&= \sum_\gamma p(\gamma)\ \mathrm{Tr}_{BB'CC'}\left(\left[\mathbb{1}^A \otimes M^{BB'}_b \otimes M^{CC'}_c \otimes \mathbb{1}^D\right]\rho^{AB}\otimes\sigma^{B'}_\gamma\otimes\sigma^C_\gamma\otimes\rho^{C'D}\right) && (2.40)\\
&= \sum_\gamma p(\gamma)\ \mathrm{Tr}_{BB'}\left(\left[M^{BB'}_b\otimes\mathbb{1}^A\right]\rho^{AB}\otimes\sigma^{B'}_\gamma\right)\otimes\mathrm{Tr}_{CC'}\left(\left[M^{CC'}_c\otimes\mathbb{1}^D\right]\sigma^C_\gamma\otimes\rho^{C'D}\right) && (2.41)\\
&= \sum_\gamma p(\gamma)\ \mathrm{Tr}_B\left(\left[M^B_{b|\gamma}\otimes\mathbb{1}^A\right]\rho^{AB}\right)\otimes\mathrm{Tr}_{C'}\left(\left[M^{C'}_{c|\gamma}\otimes\mathbb{1}^D\right]\rho^{C'D}\right), && (2.42)
\end{aligned}$$

where we defined $M^B_{b|\gamma} := \mathrm{Tr}_{B'}\left(M^{BB'}_b\mathbb{1}^B\otimes\sigma^{B'}_\gamma\right)$ and $M^{C'}_{c|\gamma} := \mathrm{Tr}_C\left(M^{CC'}_c\sigma^C_\gamma\otimes\mathbb{1}^{C'}\right)$ as valid sets of measurements. Then if ρ^{AB} and $\rho^{C'D}$ are *unsteerable* towards A and D respectively (but possibly entangled; see Section 1.4.9 and [31]), we can extract a *local hidden state* (LHS) model to obtain

$$\sigma^{AD}_{b,c} = \sum_{\gamma} p(\gamma) \left(\sum_{\alpha} p(\alpha) p(b|\alpha,\gamma) \sigma^A_\alpha \right) \otimes \left(\sum_{\beta} p(\beta) p(c|\beta,\gamma) \sigma^D_\beta \right) \tag{2.43}$$

$$= \sum_{\alpha,\beta,\gamma} p(\alpha)p(\beta)p(\gamma)\ p(b|\alpha,\gamma)p(c|\beta,\gamma)\ \sigma^A_\alpha \otimes \sigma^D_\beta, \tag{2.44}$$

which has exactly the same form as the NLHS condition in Eq. (2.38). Therefore taking ρ^{AB} as separable and ρ^{AB} and $\rho^{C'D}$ unsteerable towards A and D respectively, we will always arrive at an NLHS model, for any intermediate measurements $M^{BB'}_b$ and $M^{CC'}_c$.

Similarly suppose now that the source $\rho^{AB} = \sum_\alpha p(\alpha) \sigma^A_\alpha \otimes \sigma^B_\alpha$ is separable. Then we find

$$\sigma_{b,c} = \sum_{\alpha} p(\alpha)\ \sigma^A_\alpha \otimes \mathrm{Tr}_{BB'CC'} \left(\left[M^{BB'}_b \otimes M^{CC'}_c \right] \sigma^B_\alpha \otimes \rho^{B'C} \otimes \rho^{C'D} \right) \tag{2.45}$$

If $\rho^{C'D}$ is also separable, and $\rho^{B'C}$ is *local* (in the Bell nonlocality sense, see Section 1.4.9 and [3]), we get

$$\sigma_{b,c} = \sum_{\alpha,\beta} p(\alpha)p(\beta)\ \mathrm{Tr}_{BB'CC'} \left(\left[M^{BB'}_b \otimes M^{CC'}_c \right] \sigma^B_\alpha \otimes \rho^{B'C} \otimes \sigma^{C'}_\beta \right) \sigma^A_\alpha \otimes \sigma^D_\beta \tag{2.46}$$

$$= \sum_{\alpha,\beta} p(\alpha)p(\beta)\ \mathrm{Tr}_{BB'CC'} \left(\left[M^{B'}_{b|\alpha} \otimes M^{C}_{c|\beta} \right] \rho^{B'C} \right) \sigma^A_\alpha \otimes \sigma^D_\beta \tag{2.47}$$

$$= \sum_{\alpha,\beta,\gamma} p(\alpha)p(\beta)p(\gamma)\ p(b|\alpha,\gamma)p(c|\beta,\gamma) \sigma^A_\alpha \otimes \sigma^D_\beta \tag{2.48}$$

where in the final line we extracted a *local hidden variable* (LHV) model using the locality of $\rho^{B'C}$. Hence taking the central source $\rho^{B'C}$ as local, and the adjacent sources as separable will also always lead to an NLHS model, for any measurements.

Still taking ρ^{AB} as separable as in Eq. (2.45), if instead now $\rho^{B'C}$ and $\rho^{C'D}$ are unsteerable towards C and D respectively, we have

$$\sigma_{b,c} = \sum_{\alpha} p(\alpha)\ \sigma^A_\alpha \otimes\ \mathrm{Tr}_{CC'} \left(\left[M^{CC'}_c \otimes \mathbb{1}_D \right] \mathrm{Tr}_{BB'} \left(\left[M^{BB'}_b \otimes \mathbb{1}_C \right] \sigma^B_\alpha \otimes \rho^{B'C} \right) \otimes \rho^{C'D} \right) \tag{2.49}$$

$$= \sum_{\alpha} p(\alpha)\ \sigma^A_\alpha \otimes\ \mathrm{Tr}_{CC'} \left(\left[M^{CC'}_c \otimes \mathbb{1}_D \right] \mathrm{Tr}_{BB'} \left(\left[M^{BB'}_{b|\alpha} \otimes \mathbb{1}_C \right] \rho^{B'C} \right) \otimes \rho^{C'D} \right) \tag{2.50}$$

$$= \sum_{\alpha} p(\alpha)\ \sigma^A_\alpha \otimes\ \mathrm{Tr}_{CC'} \left(\left[M^{CC'}_c \otimes \mathbb{1}_D \right] \left(\sum_{\gamma} p(\gamma) p(b|\alpha,\gamma) \sigma^C_\gamma \right) \otimes \rho^{C'D} \right) \tag{2.51}$$

$$= \sum_{\alpha,\gamma} p(\alpha)p(\gamma)\ \sigma^A_\alpha \otimes\ p(b|\alpha,\gamma)\ \mathrm{Tr}_{C'} \left(\left[M^{C'}_{c|\gamma} \otimes \mathbb{1}_D \right] \rho^{C'D} \right) \tag{2.52}$$

$$= \sum_{\alpha,\gamma,\beta} p(\alpha)p(\beta)p(\gamma)\ p(b|\alpha,\gamma)p(c|\beta,\gamma)\ \sigma^A_\alpha \otimes \sigma^D_\beta \tag{2.53}$$

also leading to a NLHS model.

We summarise the preceding calculations in the following result.

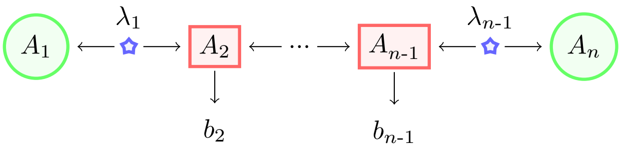


Figure 2.4: A general linear network with no inputs and trusted endpoints.

Theorem 2.9. Consider a four party network scenario with trusted endpoints and untrusted central parties who perform fixed measurements, as in Fig. 2.3(b). Ordering the sources as $\{\rho^{AB}, \rho^{B'C}, \rho^{C'D}\}$ and denoting **SEP** as the set of separable states, **LOC** as the set of Bell-local states, and $\mathbf{UNSTEER}_{\rightarrow}$ as the set of unsteerable states (in the appropriate direction) we have that $\{\mathbf{SEP}, \mathbf{LOC}, \mathbf{SEP}\}$, $\{\mathbf{UNSTEER}_{\leftarrow}, \mathbf{SEP}, \mathbf{UNSTEER}_{\rightarrow}\}$, $\{\mathbf{SEP}, \mathbf{UNSTEER}_{\rightarrow}, \mathbf{UNSTEER}_{\rightarrow}\}$ and (by symmetry) $\{\mathbf{UNSTEER}_{\leftarrow}, \mathbf{UNSTEER}_{\leftarrow}, \mathbf{SEP}\}$ all admit NLHS models, for any measurements.

This result is captured in Fig. 2.2(b). Recalling that there exist entangled yet unsteerable states, and steerable yet Bell-local states (that is $\mathbf{SEP} \subsetneq \mathbf{UNS}_{\rightarrow} \subsetneq \mathbf{LOC}$) shows that these models are indeed non-trivial. Indeed network steering is truly a novel phenomena, and fully characterising the resources needed to demonstrate it is an open and fascinating new research question.

2.4.3 General line/ring networks

We can generalise this to an arbitrary line network with trusted endpoints (Fig. 2.4), which again could be interpreted as a ring network with a single trusted party.

For n parties, here an observed set of states would be described by (repeated from Eq. (2.12))

$$\sigma^{A_1 A_n}_{b_2,\ldots,b_{n-1}} = \mathrm{Tr}_{A_2 A'_2 \ldots A_{n-1} A'_{n-1}} \Big(\Big[\mathbb{1}^{A_1} \otimes M^{A_2 A'_2}_{b_2} \otimes \cdots \otimes M^{A_{n-1} A'_{n-1}}_{b_{n-1}} \otimes \mathbb{1}^{A_n} \Big] \\ \times \rho^{A_1 A_2} \otimes \rho^{A'_2 A_3} \otimes \cdots \otimes \rho^{A'_{n-1} A_n} \Big). \quad (2.54)$$

The NLHS condition here generalises to (repeated from Eq. (2.13))

$$\sigma^{A_1 A_n}_{b_2,\ldots,b_{n-1}} = \sum_{\lambda_1,\ldots,\lambda_{n-1}} p(\lambda_1)\ldots p(\lambda_{n-1}) \times p(b_2|\lambda_1,\lambda_2)\ldots p(b_{n-1}|\lambda_{n-2},\lambda_{n-1}) \times \sigma^{A_1}_{\lambda_1} \otimes \sigma^{A_n}_{\lambda_{n-1}}. \quad (2.55)$$

We first recall that as stated in Observation 2.5, $\sum_{b_i} \sigma_{b_2,\ldots,b_{n-1}}$ is a product state for any b_i, and so the entanglement of a single $\sigma_{b_2,\ldots,b_{n-1}}$ suffices to demonstrate network steering, being incompatible with Eq. (2.13).

From the previous calculations for the line with four parties (Eq. (2.39) - Eq. (2.53)), we see more generally how taking certain sources as separable can introduce natural sufficient conditions on the other sources to result in an NLHS model overall. For example if a single source is separable, then taking all other sources as unsteerable (in the direction away from this source) leads to an overall NLHS model for a line of any length – this is a generalisation from the above Eq. (2.49) to Eq. (2.53). Similarly, if a given source is unsteerable then upon receiving some input (for example from an adjacent separable source), the resulting LHS assemblage can serve as an input to the next party. This idea of "percolation of inputs " allows to write down a large class of NLHS models, for arbitrary linear networks.

As a small example, we discuss the scenario in Fig. 2.2(c) marked with ($\star$). The separable source second from the left provides an input to the adjacent sources, from which arises natural steering assemblages such as $\mathrm{Tr}(M_{b|\lambda}^{B'} \otimes \mathbb{1}^C \rho_{B'C})$. If these adjacent sources are steerable in the appropriate direction, we can extract an LHS model, whose corresponding state assemblages can act as an input to the next party. As the parties second and third from the right now receive effective inputs, the relevant condition on the second source from the right to admit a local model is of *locality.* Therefore taking the sources as described would lead to an overall NLHS model for any measurements performed. These type of arguments would hold more generally for arbitrary linear network structures.

2.5 Conclusions

We have introduced the notions of network steering and network local hidden state models. We discussed illustrative examples, and showed that the network scenario leads to a form of activation of steering. Finally, we have started a characterisation of NLHS models based solely upon properties of the sources. There are many fascinating and novel future questions to tackle.

First, it would be interesting to determine if either NLHS assemblages or the full set of network assemblages can be characterized via techniques based on semi-definite programming, using for instance the approach of [95]. A related direction is to further classify NLHS models based on the properties of the sources. For instance, consider four parties sharing *separable*, *local* and *unsteerable* sources, or five parties sharing *separable*, *local*, *local*, and *separable* sources. In neither of these cases do we currently know if network steering can arise or not.

Here we have focused primarily on the properties of the sources, but it would also be interesting to consider the measurements, and understand which of their properties (e.g. entanglement or incompatibility) are relevant for network steering. In particular, as it is known that measurement incompatibility is required to witness standard nonlocality and steering, it is at present not clear how this resource manifests itself in the network setting, in which non-classical correlations can arise when the parties each perform a single fixed measurement.

Future work could also consider the significance for quantum repeaters [83], explore links with superactivation of quantum steering [106], or extend recent work on post-quantum steering [109] to this setting.

Finally, our initial motivation for this work was to attempt to gain clarity on network nonlocality problems, such as those in the triangle network [61, 62]. It is our hope that developing our framework further will lead to discovering novel nonlocal correlations, unique to networks.

2.6 Acknowledgements and contributions

This project was the first project I undertook during my PhD, and involved collaboration with the Quantum Theory group of Prof. Nicolas Brunner at the Universitè de Genève in Switzerland. I was based in Geneva and visited this group from August to December 2020, and then from March to June 2021 (around 8 months in total).

The group in Geneva had already been interested in network nonlocality, and in particular the triangle network. Our primary starting point was to ask, what happens to the triangle scenario if we promote a party to being trusted?

The research was a collaborative effort, with myself organising meetings and performing the bulk of the technical calculations under the suggestions of my collaborators (in particular the question of activation was discussed at length). I also independently came up with the classes of NLHS models. I wrote the paper, with multiple rounds of edits and suggestions from my co-authors.

I would like to thank all of my collaborators on this project: Ivan Šupić, Roope Uola, Nicolas Brunner, and Paul Skrzypczyk. We are also grateful to Marco Túlio Quintino for helpful discussions.

Chapter 3

High dimensional measurement incompatibility

Chapter Summary

We introduce a notion of compression for a set of quantum measurements, which can be thought of as a quantifier of measurement incompatibility in terms of dimension. We make several direct connections to the recently introduced concept of genuine high-dimensional quantum steering, which relates to certifying the Schmidt number of bipartite state when only one of the parties is trusted (also referred to as a one-sided device independent scenario). Our two main connections are that high-dimensional measurements are necessary to witness genuine high-dimensional steering, and then by exploiting a known connection between measurement incompatibility and quantum steering, we show that these concepts are in fact mathematically equivalent, using the machinery of channel-state duality. Finally, we discuss further connections and implications for classes of quantum channels.

This chapter is based on the following publications (primarily the former):

Benjamin DM Jones, Roope Uola, Thomas Cope, Marie Ioannou,
Sébastien Designolle, Pavel Sekatski, and Nicolas Brunner.
Equivalence between simulability of high-dimensional measurements and high-dimensional steering.
Physical Review A, 107(5):052425, 2023.

Marie Ioannou, Pavel Sekatski, Sébastien Designolle,
Benjamin DM Jones, Roope Uola, and Nicolas Brunner.
Simulability of high-dimensional quantum measurements.
Physical Review Letters, 129(19):190401, 2022.

Relevant background: measurement incompatibility (Section 1.4.3), channel state duality (Section 1.4.1), high-dimensional entanglement (e.g. Schmidt number and n-partially entanglement breaking channels – Section 1.4.2), quantum nonlocality and steering (Section 1.4.4 and Section 1.4.5), and miscellaneous states and channels (Section 1.4.9): such as separable and unsteerable states, and incompatibility breaking channels.

Page

Contents

3.1 Introduction

High-dimensional quantum systems feature a number of interesting phenomena, beyond what is possible for qubit systems. For example, the effect of entanglement is known to become increasingly robust to noise when higher dimensions are considered [110, 111]. In turn, the nonlocal correlations obtained from measurements on high-dimensional systems also feature significantly increased robustness. Indeed, these effects offer interesting perspectives for quantum information processing, allowing, e.g. for quantum communications over very noisy channels.

In this chapter, we consider the effect of genuine high-dimensional steering (GHDS), which has been recently introduced [112]. The original formulation of quantum steering (see Section 1.4.5) encapsulates the essence of the Einstein-Podolsky-Rosen paradox. This aspect has been demonstrated in various works, such as [113–116]. A possible quantum information interpretation of this phenomenon is given via certification of entanglement between an untrusted party (Alice) and a trusted one (Bob) [117]. Hence steering is sometimes referred to as being a one-sided device-independent (SDI) entanglement detection protocol. The key point of GHDS is to go beyond entanglement detection by certifying the minimal dimensionality of entanglement (specifically the Schmidt number) required for producing the observed correlations in a SDI scenario. More formally, this approach introduces the notion of n-preparable assemblages, i.e. those assemblages being preparable based on any possible entangled state of Schmidt rank at most n; 1-preparable assemblages being then simply those assemblages that cannot demonstrate steering. Next, one can construct a steering inequality for n-preparable assemblages, the violation of which implies the presence of genuine $(n+1)$-dimensional steering. This was demonstrated in a quantum optics experiment (based on photon-pairs entangled in orbital angular momentum) reporting the SDI certification of 14-dimensional entanglement [112].

A natural question at this point is to understand what are the resources required in terms of measurements for demonstrating GHDS. Indeed, the effect of steering uses not only an entangled state as a resource, but also a well-chosen set of local measurements for Alice.

The latter must be incompatible, but it turns out that steering has a direct connection to measurement incompatibility [51, 118–120] – see also Section 1.4.5.1.

The present chapter explores this question, and establishes a general connection between GHDS and the notion of n-dimensional simulability (or n-simulability) of high-dimensional measurements which has been recently introduced in [18]. This notion generalises the concept of joint measurability and provides a quantification of measurement incompatibility in terms of a dimension. The connection we uncover generalises the well-known relations between quantum steering and joint measurability. Moreover, we also extend the connection to quantum channels, in particular the characterisation of their high-dimensional properties. These general tripartite connections between high-dimensional steering, measurements and channels, allow for results of one area to be directly translated in others, which we illustrate with several examples. See also Fig. 3.1 for illustrations of these concepts.

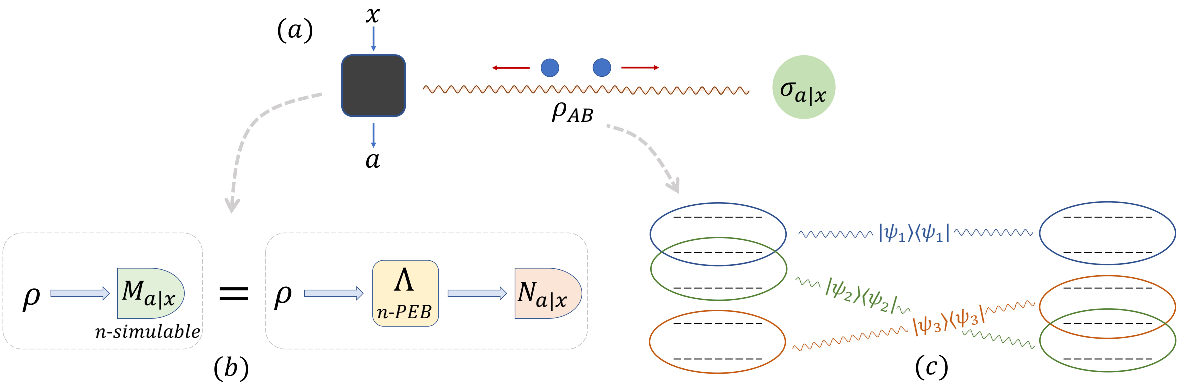


Figure 3.1: Concepts and connections that appear in this chapter. (a) Quantum steering scenario. (b) A set of measurements is n-simulable if they can be replaced by an n-partially entanglement breaking channel (n-PEB) followed by some measurements. (c) Illustration of the Schmidt number (SN) of a bipartite state (repeated from Fig. 1.1): the state of two 5 level systems is a combination of states with only qubit entanglement, hence the overall state has SN at most 2.

3.1.1 Summary of results

Main conceptual contributions:

- We introduce a new definition of high-dimensional measurement incompatibility for a set of measurements, which can also be viewed as a form of compression.
- We show that this definition is equivalent to high-dimensional quantum steering.
- We introduce n-partially incompatibility breaking channels and characterise their Choi states.

Main technical calculations:

Theorem 3.5 Consider a steering assemblage $\sigma_{a|x}$ and measurements $M_{a|x}$ such that $M_{a|x} = \rho_B^{-\frac{1}{2}} \sigma_{a|x} \rho_B^{-\frac{1}{2}}$, where $\rho_B := \sum_a \sigma_{a|x}$ is a quantum state of full rank. Then $M_{a|x}$ is n-simulable if and only if $\sigma_{a|x}$ is n-preparable. That is, $M_{a|x}$ can be written as $\Lambda^*(N_{a|x})$ for some n-PEB channel Λ and measurements $N_{a|x}$, if and only if $\sigma_{a|x}$ can be written as $\text{Tr}_1(N'_{a|x} \otimes \mathbb{1}\ \rho)$ for some state ρ of Schmidt number n and measurements $N'_{a|x}$.

Theorem 3.7 Let E_n be the set of states with Schmidt number at most n, S_n be the set of of n-simulable measurements assemblages, and P_n the set of n-preparable steering assemblages. For some set of objects $\mathcal{O}$ (e.g. states, measurements, channels, assemblages) and free set $\mathcal{F}$ define the weight as

$$\begin{aligned} \mathcal{W}_F(x) := \min \quad & \lambda && (3.1)\\ \text{s.t.} \quad & x = (1-\lambda)y + \lambda z && (3.2)\\ & y \in \mathcal{F} && (3.3)\\ & z \in \mathcal{O}. && (3.4) \end{aligned}$$

Given an assemblage $\sigma_{a|x} = \text{Tr}_1(M_{a|x} \otimes \mathbb{1}\ [\rho_{AB}])$, we then have the following inequality:

$$\mathcal{W}_{P_n}(\sigma_{a|x}) \leq \mathcal{W}_{S_n}(M_{a|x}) \mathcal{W}_{E_n}(\rho_{AB}). \tag{3.5}$$

Open questions:

- Exploring the nonlocality case, for example the characterisation of quantum channels with Choi state of FDI-SN n.

Prior work and concepts:

- High dimensional entanglement: quantifying entanglement dimensionality via the Schmidt rank (for pure states) the Schmidt number (for mixed states) [53], and n-partially entanglement breaking channels [121].
- High dimensional steering [112]: the idea of a steering assemblage not only being able to certify that the underlying state is entangled, but that it has Schmidt number at least n.

- Measurement incompatibility, and connections with steering: specifically the equivalence between an assemblage being LHS and the corresponding set of POVMs being compatible [31, 120].

- Notions of compression for sets of measurements, see for example the work of Andreas Bluhm [122–124] and references therein. As a specific example, in [122] a related notion of 'n-compressibility' of a set of quantum measurements is proposed, whereby the set of measurements must be preserved under first passing through a 'compression channel' to a space of lower dimension, followed by a 'decompression channel' back to the original space. A notable distinction between their definition and the one presented in this chapter is that in [122] a single measurement may have a compression dimension strictly greater than 1, whereas for us all individual measurements have compression dimension (or simulability dimension) equal to 1, which is a intended generalisation of the fact that any single measurement is jointly measurable (1-simulable, in our language).

3.2 A new definition

Loosely speaking, we say that a set of measurements $M_{a|x}$, defined on a Hilbert space of dimension d, is said to be n-simulable when the statistics of this set of measurements on any possible quantum state can be exactly recovered using a form of compression of quantum information to a lower n-dimensional space. Our main motivation is to use the existing connections between measurement incompatibility and steering to translate results across about high-dimensional steering, which we now discuss.

In [112], the concept of *genuine high-dimensional steering* (GHDS) was introduced, where one asks whether a given assemblage $\sigma_{a|x}$ can be produced using a bipartite state ρ_{AB} of Schmidt number at most n, in which case we term the assemblage *n-preparable*. In this framework, an assemblage is LHS if and only if it is 1-preparable, as any separable state leads to an LHS assemblage and any LHS assemblage can be prepared with some separable state [125, 126]. Hence if an assemblage is not n-preparable, this guarantees that the underlying state ρ_{AB} is of Schmidt number at least $n+1$. This represents a SDI certification of entanglement dimensionality, illustrated in a recent quantum optics experiment certifying up to 14-dimensional entanglement [112].

So far, the focus of GHDS is on the dimensionality of the shared entangled state. There is however another resource that is crucial for observing quantum steering, namely the set of measurements performed by Alice, which must be incompatible. More generally, there exist in fact a deep connection between measurement incompatibility (in the sense of being not jointly measurable) and quantum steering [118–120]. In particular, this implies that any set of incompatible measurements for Alice can be combined with an appropriate state ρ_{AB} for demonstrating steering.

This naturally raises the question of what are the necessary resources in terms of measurements for demonstrating GHDS. Intuitively, the latter should also require a minimal "dimensionality" for the set of measurements. below we will make this intuition precise, by using the concept of n-simulability of a set of measurements. More generally, we will establish a deep connection between GHDS (more precisely the notion of n-preparability of an assemblage) and n-simulability of set of measurements. This generalises the previously known connection between steering and measurement incompatibility.

To provide concrete motivation, consider a steering scenario in which the underlying distribution can be achieved with a state of at most Schmidt number n. That is

$$\sigma_{a|x} = \mathrm{Tr}_1(M_{a|x} \otimes \mathbb{1}\ \rho) \tag{3.6}$$

for some measurements $M_{a|x}$ and and $\mathrm{SN}(\rho) \leq n$. Recall that we can write any state of Schmidt number at most n as

$$\rho = \Lambda \otimes \mathbb{1}\tau \tag{3.7}$$

for Λ n-PEB and some τ (in fact, we can take Λ as the Choi channel of ρ in generalised channel state duality – see Section 1.4.1).

Using the Heisenberg picture we can write this as

$$\begin{aligned} \sigma_{a|x} &= \mathrm{Tr}\Big(M_{a|x} \otimes \mathbb{1}\ \rho\Big) && (3.8)\\ &= \mathrm{Tr}\Big(M_{a|x} \otimes \mathbb{1}\ \Lambda \otimes \mathbb{1}\tau\Big) && (3.9)\\ &= \mathrm{Tr}\Big(\Lambda^*(M_{a|x}) \otimes \mathbb{1}\ \tau\Big) && (3.10) \end{aligned}$$

where $\Lambda^*(M_{a|x})$ defines a new set of POVMs. Hence we can immediately see that if either of the measurements used in a Bell scenario or steering scenario can be written in the form $\Lambda^*(M_{a|x})$ for Λ n-PEB and arbitrary $M_{a|x}$, then the resulting distribution/assemblage will be n-preparable. This motivates our new definition:

Definition 3.1. A set of measurements $M_{a|x}$ is said to be n-simulable if there exists an n-PEB channel Λ and a set of arbitrary measurements $N_{a|x}$ such that

$$M_{a|x} = \Lambda^*(N_{a|x}) \tag{3.11}$$

It turns out that this definition is equivalent to a notion of compression, as originally introduced in [18]. Consider for example Alice (e.g. on the Moon), sending an arbitrary state ρ to a distant party Bob (e.g. on Earth), who will perform a set of POVMs $M_{a|x}$. Which POVM Bob performs depends on some input x. The expected (target) data is given by $p(a|x,\rho) = \mathrm{Tr}\Big(M_{a|x}\rho\Big)$. As resource, we consider here the dimensionality of the quantum channel between Alice and Bob, while a classical channel is always available for free. The goal is then to compress as much as possible the initial state of Alice, in order to use a quantum channel with minimal dimension, while still recovering exactly the target data. More formally, we demand that

$$M_{a|x} = \sum_{\lambda} \Lambda_{\lambda}^{*}(N_{a|x,\lambda}) \tag{3.12}$$

where $\Lambda = \{\Lambda_\lambda\}_\lambda$ denotes the instrument (compressing from dimension d to n), with classical output λ, and $N_{a|x,\lambda}$ is a set of n-dimensional POVMs performed by Bob upon receiving the input x and the classical information λ communicated by Alice. Here Λ_λ^* refers to the Heisenberg picture of Λ_λ.

Proposition 3.2. A set of d-dimensional measurements $M_{a|x}$ is n-simulable if and only if there exists a quantum instrument Λ_λ mapping from dimension d to n, such that

$$M_{a|x} = \sum_{\lambda} \Lambda_{\lambda}^{*}\left(N_{a|x,\lambda}\right) \tag{3.13}$$

See [18] for the proof.

An important case is 1-simulability, i.e., when the full quantum information can be compressed to purely classical one. This is possible if and only if the set of POVMs is jointly measurable, i.e., $M_{a|x} = \sum_\lambda \, p(a|x,\lambda) \, G_\lambda$, for some probability distribution $p(a|x,\lambda)$ and a "parent" measurement G_λ, see [33, 127] for reviews on the topic. To see this, one can note that instruments with a 1-dimensional output space are POVMs on their input space, and POVMs on a 1-dimensional space are probability distributions. A set of POVMs that is not jointly measurable (hence called *incompatible*), can nevertheless be n-simulable, for some n with $2 \leq n \leq d$.

Remark 3.3. $M_{a|x}$ is 1-simulable if and only if it is jointly measurable.

We note that although we may talk about high-dimensional properties of measurements, we do always mean properties of *sets* of measurements. This is due to the fact that any POVM is jointly measurable with itself and, hence, a trivial pair of measurement and itself is 1-simulable.

In the rest of the chapter, we will first establish precisely the connection between n-preparability and n-simulability. Finally, in the last section of the chapter, we will also extend the connection to quantum channels and their characterisation in terms of dimension. This will provide a full tripartite connection, for characterising dimension in steering assemblages, incompatibility of sets of measurements, and quantum channels.

3.3 High-dimensional steering and simulability of measurements

In this section, we present in detail the structural connection between n-preparability of steering assemblages and n-simulability of sets of measurements.

We start with a first result clearly identifying the resource for GHDS. More precisely, the following theorem implies that observing GHDS, i.e., an assemblage which is not n-preparable, implies that (i) the shared entangled state ρ_{AB} has at least Schmidt number $n+1$, and (ii) the set of measurements $\{M_{a|x}\}$ performed by Alice is not n-simulable. In other words, one really needs both high-dimensional entanglement and high-dimensional measurement incompatibility to witness genuine high-dimensional steering.

More formally we can prove the following.

Theorem 3.4. If $M_{a|x}$ is n-simulable or ρ_{AB} has Schmidt number at most n, then the assemblage

$$\sigma_{a|x} := \mathrm{Tr}_1\Big(M_{a|x} \otimes \mathbb{1}\ [\rho_{AB}]\Big) \tag{3.14}$$

is n-preparable.

Proof. If ρ_{AB} has SN at most n, this simply follows from the definition of n-preparability. Now suppose that $M_{a|x}$ is n-simulable. Then there exists a n-PEB channel Λ and measurements $N_{a|x}$ such that $M_{a|x} = \Lambda^*(N_{a|x})$. By the definition of the dual, we can hence write

$$\sigma_{a|x} = \mathrm{Tr}_1\left(\Lambda^*(N_{a|x}) \otimes \mathbb{1}[\rho_{AB}]\right) \tag{3.15}$$

$$= \mathrm{Tr}_1\left((N_{a|x} \otimes \mathbb{1})(\Lambda \otimes \mathbb{1})[\rho_{AB}]\right) \tag{3.16}$$

and as Λ is n-PEB, then $\Lambda \otimes \mathbb{1}[\rho_{AB}]$ has SN at most n, so $\sigma_{a|x}$ is n-preparable. □

Our next result establishes a general equivalence between any n-preparable assemblage and a set of POVMs that is n-simulable, and vice versa. The main idea is that a set of quantum measurements $M_{a|x}$ and a steering assemblage $\sigma_{a|x}$ are very similar types of mathematical objects: both are composed of positive semi-definite matrices, and $\sum_a M_{a|x} = \mathbb{1} \quad \forall x$ whereas $\sum_a \sigma_{a|x}$ will be equal to some fixed state $\rho_B = \mathrm{Tr}_1(\rho_{AB})$ for all x. A direct connection can be established, namely that $\sigma_{a|x}$ is LHS if and only if $\rho_B^{-1/2}\sigma_{a|x}\rho_B^{-1/2}$ is jointly measurable (when interpreted as a set of measurements) [120]. The theorem below can be considered a generalisation of this result, in the sense that the proof of [120] corresponds to the case $n = 1$.

Theorem 3.5. Consider a steering assemblage $\sigma_{a|x}$ and measurements $M_{a|x}$ such that $M_{a|x} = \rho_B^{-\frac{1}{2}}\ \sigma_{a|x}\ \rho_B^{-\frac{1}{2}}$, where $\rho_B := \sum_a \sigma_{a|x}$ is of full rank. Then $M_{a|x}$ is n-simulable if and only if $\sigma_{a|x}$ is n-preparable.

Proof. Let $N_{a|x}$ be a measurement assemblage and ρ_{AB} be a state such that $\mathrm{Tr}_1(\rho_{AB}) = \rho_B$. Let $(\cdot)^T$ denote the transpose with respect to an eigenbasis of ρ_B. We then have the following equivalences

$$\begin{aligned}
&\sigma_{a|x} = \mathrm{Tr}_1(N_{a|x} \otimes \mathbb{1}\ \rho_{AB}) && (3.17)\\
\iff\ & M_{a|x} = \ \rho_B^{-\frac{1}{2}}\ \mathrm{Tr}_1(N_{a|x} \otimes \mathbb{1}\ \rho_{AB})\ \rho_B^{-\frac{1}{2}} && (3.18)\\
\iff\ & M_{a|x}^T = \ \rho_B^{-\frac{1}{2}}\ \mathrm{Tr}_1(N_{a|x} \otimes \mathbb{1}\ \rho_{AB})^T\ \rho_B^{-\frac{1}{2}} && (3.19)\\
\iff\ & M_{a|x}^T = \Lambda^*_{\rho_{AB}}\Big(N_{a|x}\Big), && (3.20)
\end{aligned}$$

where in the third line we used the fact that $(\rho_B^{-\frac{1}{2}})^T = \rho_B^{-\frac{1}{2}}$, as the transpose is taken in an eigenbasis of ρ_B, and in the last line we have invoked the form of channel-state duality from [51], see also Section 1.4.1.

Now observe that the existence of a state ρ_{AB} in the above with Schmidt number at most n is equivalent to $\sigma_{a|x}$ being n-preparable. We can also see that there exists ρ_{AB} with $\mathrm{SN}(\rho_{AB}) \leq n$ if and only if $M_{a|x}^T$ is n-simulable, as such a state corresponds to $\Lambda_{\rho_{AB}}$ being n-PEB (see Lemma 1.23). To finalise the proof we must show that $M_{a|x}$ is n-simulable if and only if $M_{a|x}^T$ is n-simulable. This can be seen as follows. First note that $M_{a|x}^T$ defines a valid collection of measurements. Suppose that $M_{a|x} = \Lambda^*(N_{a|x})$ with Λ n-PEB and $N_{a|x}$ arbitrary measurements. Then letting $\mathcal{T}$ denote the transpose map, we have that $M_{a|x}^T = (\mathcal{T} \circ \Lambda^*)(N_{a|x}) = (\Lambda \circ \mathcal{T}^*)^*(N_{a|x})$. As Λ is n-PEB, $\Lambda \circ \mathcal{T}^*$ is also n-PEB. Hence $M_{a|x}^T$ is n-simulable. The converse direction follows from $(M_{a|x}^T)^T = M_{a|x}$. □

As a technical remark, note that as for any a and x the support of $\sigma_{a|x}$ is contained within the support of $\rho_B = \sum_a \sigma_{a|x}$ (this follows as $\sigma_{a|x}$ are all positive semi-definite), we can still invoke the above theorem in the case where ρ_B is not full rank, by restricting $\sigma_{a|x}$ to the support of ρ_B.

Theorem 3.5 also allows to prove the following result, which complements Theorem 3.4. This shows that for any set of POVMs that is not n-simulable, one can always find an entangled state such that the resulting assemblage is not n-preparable. Again, this generalizes some previous results stating that any incompatible set of POVMs can lead to steering [118, 119], which corresponds to the case $n = 1$ of the proposition below.

Proposition 3.6. If $M_{a|x}$ is not n-simulable, then the assemblage

$$\sigma_{a|x} := \mathrm{Tr}_1\Big(M_{a|x} \otimes \mathbb{1} \; \big|\Phi^+\big\rangle\big\langle\Phi^+\big|\Big) \tag{3.21}$$

is not n-preparable, where $|\Phi^+\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle$.

Proof. We have that

$$\sigma_{a|x} = \mathrm{Tr}_1\Big(M_{a|x} \otimes \mathbb{1} \; \big|\Phi^+\big\rangle\big\langle\Phi^+\big|\Big) = \frac{1}{d}\; M_{a|x}^T. \tag{3.22}$$

By the proof of Theorem 3.5, if $M_{a|x}$ is not n-simulable, then $M_{a|x}^T$ is not n-simulable. Then invoking Theorem 3.5 with $\rho_B = \frac{\mathbb{1}}{d}$, we have that that $\sigma_{a|x}$ is not n-preparable. □

In the final part of this section, we show that the trade-off between high-dimensional entanglement, high-dimensional measurement incompatibility, and high-dimensional steering can be made quantitative. For this, we use a specific resource quantifiers known as the convex weight [128]. Consider for example the quantification of entanglement via the weight. For any entangled state ρ, we can measure its entanglement through its weight (see Section 1.4.7), given by the following quantity

$$\begin{aligned} \mathcal{W}_F(\rho) := &\min \lambda \\ &\text{s.t. } \rho = (1-\lambda)\rho_{sep} + \lambda\sigma, \end{aligned} \tag{3.23}$$

where the minimisation runs over any state ρ_{sep} that is separable, and σ an arbitrary state. As expected, $\mathcal{W}_F(\rho) = 0$ when ρ is separable. More generally, this quantifier can apply to objects such as states, measurements or steering assemblages, with respective free sets E_n: the set of states with Schmidt number at most n, S_n: the set of of n-simulable measurements assemblages, and P_n: the set of n-preparable steering assemblages. We can now state our next result, which quantitatively illustrates the necessity of high-dimensional measurement incompatibility and entanglement for GHDS:

Theorem 3.7. Given an assemblage $\sigma_{a|x} = \mathrm{Tr}_1(M_{a|x} \otimes \mathbb{1}\; [\rho_{AB}])$, we have the following inequality:

$$\mathcal{W}_{P_n}(\sigma_{a|x}) \leq \mathcal{W}_{S_n}(M_{a|x})\mathcal{W}_{E_n}(\rho_{AB}). \tag{3.24}$$

For the case $n = 1$ we get a quantitative connection among steering, measurement incompatibility and entanglement.

Proof. We first note that the sets E_n, S_n and P_n are all convex, which can be readily verified (see for example Refs. [53, 129]).

$$\begin{aligned}\sigma_{a|x} &= \mathrm{Tr}_1[(M_{a|x} \otimes \mathbb{1})\rho_{AB}] && (3.25)\\ &= [(1 - \mathcal{W}_{S_n}(M_{a|x})]\mathcal{W}_{E_n}(\rho_{AB})\tau^{(1)}_{a|x} && (3.26)\\ &+ \mathcal{W}_{S_n}(M_{a|x})[1 - \mathcal{W}_{E_n}(\rho_{AB})]\tau^{(2)}_{a|x} && (3.27)\\ &+ [1 - \mathcal{W}_{S_n}(M_{a|x})][1 - \mathcal{W}_{E_n}(\rho_{AB})]\tau^{(3)}_{a|x} && (3.28)\\ &+ \mathcal{W}_{S_n}(M_{a|x})\mathcal{W}_{E_n}(\rho_{AB})\kappa_{a|x}, && (3.29)\end{aligned}$$

where $\tau^{(i)}_{a|x}$ is an n-preparable state assemblage for $i = 1, 2, 3$ and $\kappa_{a|x}$ is an arbitrary assemblage. The fact that $\tau^{(i)}_{a|x}$ are all n-preparable follows directly from Theorem 3.4. Now note that the coefficients of the first three terms sum to $1 - \mathcal{W}_{S_n}(M_{a|x})\mathcal{W}_{E_n}(\rho_{AB})$, hence we can write the sum of these first three terms as

$$(1 - \mathcal{W}_{S_n}(M_{a|x})\mathcal{W}_{E_n}(\rho_{AB}))\tau_{a|x} \tag{3.30}$$

where $\tau_{a|x}$ is a convex combination of $\tau^{(1)}_{a|x}$, $\tau^{(2)}_{a|x}$ and $\tau^{(3)}_{a|x}$, and hence is itself n-preparable. Putting this together, we have that

$$\begin{aligned}\sigma_{a|x} &= (1 - \mathcal{W}_{S_n}(M_{a|x})\mathcal{W}_{E_n}(\rho_{AB}))\tau_{a|x} && (3.31)\\ &+ \mathcal{W}_{S_n}(M_{a|x})\mathcal{W}_{E_n}(\rho_{AB})\kappa_{a|x}, && (3.32)\end{aligned}$$

so we see that $\mathcal{W}_{S_n}(M_{a|x})\mathcal{W}_{E_n}(\rho_{AB})$ is a feasible solution for the convex weight of $\sigma_{a|x}$ with respect to P_n. As the convex weight is a minimisation the inequality

$$\mathcal{W}_{P_n}(\sigma_{a|x}) \leq \mathcal{W}_{S_n}(M_{a|x})\mathcal{W}_{E_n}(\rho_{AB}). \tag{3.33}$$

follows. □

3.4 Quantum channels

An important superset of entanglement breaking channels is that of incompatibility breaking channels [54], which are channels Λ such that $\Lambda^*(M_{a|x})$ is jointly measurable for any $M_{a|x}$. Via channel-state duality these channels correspond respectively to separable and unsteerable states (where the direction of steerability corresponds to whether the channel is applied on the first or second system in the definition of channel-state duality). The connections between high-dimensional steering, n-simulability and n-PEB channels motivate the following definition:

Definition 3.8. A channel Λ is n**-partially incompatibility breaking** (n-PIB) if for any measurement assemblage $N_{a|x}$ the resulting measurement assemblage $\Lambda^*(N_{a|x})$ is n-simulable[a].

[a] We note that our definition here is different to the notion of n-incompatibility breaking channels defined in [54], which denotes channels who break the incompatibility of any n observables.

Hence, just as $\Lambda \otimes \mathbb{1}$ maps all bipartite states to states with Schmidt number n for Λ a n-PEB channel, an n-PIB channel maps any measurement assemblage to an n-simulable one (in the Heisenberg picture). We can also gain insight from considering the structure of n-PIB channels and their relation to n-PEB channels. Unpicking Definition 3.8, for Λ to be n-PIB we require that for all measurement assemblages $N_{a|x}$, there exists an n-PEB channel Ω and a set of measurements $M_{a|x}$ such that

$$\Lambda^*(N_{a|x}) = \Omega^*(M_{a|x}). \tag{3.34}$$

Therefore, by simply taking $\Omega := \Lambda$ and $M_{a|x} := N_{a|x}$ in Eq. (3.34), we immediately arrive at the following result:

Proposition 3.9. Every n-PEB channel is n-PIB.

It is illuminating to consider the corresponding Choi states. For n-PEB channels, the Choi states are exactly the states with Schmidt number n [121]. For n-PIB channels, we have the following result:

Theorem 3.10. Λ is n-PIB if and only if ρ_Λ only leads to n-preparable assemblages.

Proof. Let $\sigma = \mathrm{Tr}_1(\rho_\Lambda)$ fix the channel-state correspondence. Suppose Λ is n-PIB, that is, for all measurements $N_{a|x}$, we have that $\Lambda^*(N_{a|x})$ is n-simulable. By Theorem 3.5, this is equivalent to $\sigma^{\frac{1}{2}}\Lambda^*(N_{a|x})^T\sigma^{\frac{1}{2}}$ being n-preparable for all $N_{a|x}$. Via channel-state duality, this is equivalent to

$$\mathrm{Tr}_1(N_{a|x} \otimes \mathbb{1}\rho) \tag{3.35}$$

being n-preparable for all $N_{a|x}$. □

The result of the above theorem is put into context of other similar connections between a channel and its Choi state in Table 3.1.

3.5 Conclusions

We have uncovered deep connections between high-dimensional versions of quantum steering, measurement incompatibility, and quantum channels, and demonstrated how a rich transfer of information is possible between these areas. In particular, we showed that the concept of n-simulability for sets of POVMs is equivalent to n-preparability for state assemblages in steering. This generalises the well-known connection between steering and joint measurability, which simply corresponds here to the case $n = 1$.

Channel	State	Reference
Entanglement breaking	Separable	[28]
Incompatibility breaking	Unsteerable	[51, 54]
n-PEB	SN n	[53, 121]
n-PIB	SDI-SN n	Theorem 3.10.

Table 3.1: Connections between channels and their Choi states. Our work naturally extends this picture by generalising both incompatibility breaking channels and unsteerable states in terms of dimension, and proving that they directly correspond to each other through generalised channel state-duality. SDI-SN n refers to when a state can only lead to n-preparable steering assemblages, or equivalently a staet for which one can only certify a Schmidt number of n in a semi-device independent scenario.

We identified the resources required for observing GHDS, in particular that both high-dimensional measurements and high-dimensional entanglement are necessary. In the light of these results, we conclude that the experiment of [112] also demonstrates measurements in pairs of MUBs that are highly incompatible, in the sense that are they not 14-simulable.

A natural further question would be to explore these questions in the context of nonlocality [3], which can be thought of as a fully-device independent (FDI) regime. Analogously to the steering case, one could define a behaviour $p(a, b|x, y)$ to be n-preparable if it could have arisen from a shared state of Schmidt number at most n, and define a state to have fully-device independent Schmidt number n (FDI-SN n) if it can only lead to n-preparable behaviours. This is related to [130], where the authors introduce the concept of dimension witnesses to lower bound the dimension of the underlying state. One can quickly see in this scenario that if either of the two parties use n-simulable measurements, then the resulting behaviour will be n-preparable. Similarly, any measurements on an n-preparable assemblage can only result in an n-preparable behaviour. However, it is less clear how one could characterise the corresponding channels whose Choi states have FDI-SN n. In the steering case we were able to exploit and generalise known connections with measurement incompatibility, but it seems that new tools may be needed to attack this problem in the fully device independent regime.

3.6 Acknowledgements and contributions

My part in this work came about through discussions with Roope Uola at the blackboard in Geneva, when I was visiting the group of Prof. Nicolas Brunner for around 8 months during the pandemic. The starting point was to consider genuine high-dimensional steering (GHDS), and find a necessary definition on the measurements in order to witness GHDS. Then due to the existing connection between steering and incompatibility, we were keen to see if our definition also generalised this. Proving this uncovered a rich structure of connections involving high-dimensional entanglement, quantum channels, channel-state duality and translating between the Schrödinger and Heisenberg pictures.

In parallel, other collaborators in Geneva were exploring a more operationally motivated definition of compression. In particular, considering a scenario where e.g. Alice was on the Moon, trying to send quantum messages to Bob on Earth, who can perform some set of quantum measurements. Taking classical control as a free resource, the question was to see when it was possible for Alice and Bob to replace the quantum channel with one of a lower dimension, viewed as a property of Bobs measurements (Alice can send arbitrary states).

Over the next few months we explored and combined our ideas, and decided to partition the work into two papers: one introducing our new definition of measurements focusing on compression [18], and a second follow up paper (of which I was lead author) [17] making all of the connections with GHDS.

My main contributions included introducing the definition of n-simulability using n-partially entanglement breaking channels (Definition 3.1), proving the connections to GHDS, defining n-partially incompatibility breaking channels and exploring the link with states for which one can only verify a Schmidt number of n in a semi-device independent scenario. I also helped with the proof of Claim 2 and 3 in our first paper [18], and would like to thank Alex Little for useful discussions on Haar integrals in Bristol. I would also like to thank my supervisor Paul Skrzypczyk for helpful discussions. I also contributed towards the simulation models and bounds discussed in [17] (and I produced Figure 2 in this work), although I have omitted these topics in this thesis.

There was also some continuation in this area after these two papers. A recent work has explored issues arising in the infinite dimensional case [131], such as the fact that there exist separable states which cannot be written as a countable convex sum of product states. I was involved in some discussions in this work but did not contribute sufficiently to be listed as an author. There is also an ongoing project involving myself and collaborators in Geneva and Heriot-Watt University, exploring how the ideas introduced in this chapter can be used to certify the dimension of a channel experimentally, without trusting the final measurements.

I would like to thank all of my collaborators: Roope Uola, Thomas Cope, Marie Ioannou, Sébastien Designolle, Pavel Sekatski, and Nicolas Brunner.

CHAPTER 4

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

Chapter Summary

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.

This chapter is based on the following preprint:

Benjamin DM Jones, Paul Skrzypczyk, and Noah Linden.
The Hadamard gate cannot be replaced by a resource state in universal quantum computation.
arXiv preprint arXiv:2312.03515, 2023.

Relevant background: resource theories (Section 1.4.7), stabilisers, Cliffords and magic (Section 1.4.6).

Page

Contents

4.1 Introduction

The more peculiar aspects of quantum mechanics, such as entanglement [76] and incompatibility of measurements [32], 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 [20]. 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.

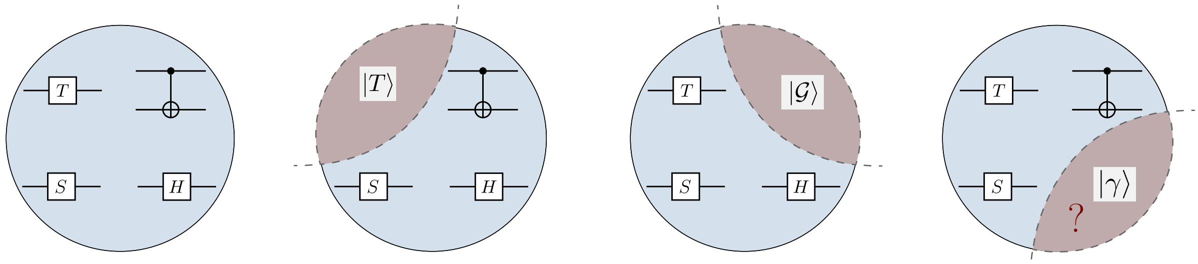
There are various ways of performing universal quantum computation: examples include the circuit model [20], measurement based approaches [37], magic state injection [39], quantum annealing [132], and continuous variable models [133]. An interesting perspective is to consider approaches involving "free" 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 (see also Section 1.4.6 for background). 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 [39].

In contrast, measurement based quantum computation (MBQC) proceeds by adaptively performing single qubit measurements on an entangled resource state, such as a cluster state [134]. 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 [135].

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. 4.1. 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 [35]. 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



(a) Universal gate set. (b) MSI. (c) MBQC. (d) This chapter.

Figure 4.1: (a) A universal set of quantum gates: Hadamard (H), Phase (S), T, and controlled-NOT. (b) Magic state injection: each T gate can be implemented using Clifford operations and a $|T\rangle$ state. (c) Measurement based quantum computation: 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 $T^2 = S$.

coherence [34]. 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.

4.1.1 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 calculations:

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 4.15 (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 [136] (an erratum to [137]) 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 4.19 (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

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

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 4.22 (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 4.9), placing bounds on the coherence rank of a state after k Hadamards have been applied (Lemma 4.11), 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 4.21).

Open questions:

- Achieving tighter bounds and a more complete analysis.
- Uncovering general connections between resource theories and quantum computation.
- Which resource theories have free unitaries that remain free under quantum control?
- Are there quantative trade-offs involving the resource content of a given unitary U and state σ, and the unitarity and resource content of the associated channel $\Lambda(\rho) = \mathrm{Tr}_2(U \; \rho {\otimes} \sigma \; U^\dagger)$?
- What is the relationship (if any) between coherence and measurement incompatibility in quantum computation?

Prior work and concepts:

- The resource theory of coherence [34], and specifically the idea of using a resourceful state and resourceless channel to implement a resourceful channel – see [137] and the associated erratum [136].

- Gadget based approaches to quantum computation, specifically magic state injection [39, 74, 75]

- Measurement-based quantum computation [37, 138], and in particular approaches that achieve universality using only X and Z measurements [135].

4.1.2 Background

The seminal result of the Gottesman-Knill theorem [20, 71–73] 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 [39], 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 4.2 below for further detail here.

Another example of a gadget-based approach can be found in recent work on matchgate circuits [139, 140]. 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 [141]. 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 [141, 142]. Hence nearest-neighbour matchgates can be augmented to universality using SWAP gates, analogously to Clifford circuits and T gates. The work of [139, 140] highlights this connection (see Figure 1 in [140]), 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) [37] 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 [138, 143], 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 [37, 144].

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 [134]), and and the resource state contains all the *entanglement* needed for the computation.

The framework of *quantum resource theories* [35] (see also Section 1.4.7) 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 [34], and is highly relevant to this chapter. 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 [80] – see Section 1.4.7 for some comments.

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. [69, 145, 146]. 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 [134, 147]. 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’ [148]).

In this chapter, 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 chapter, 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 [135], 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.

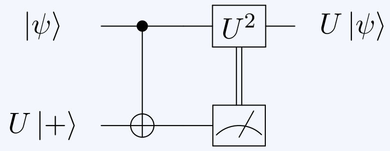
Example 4.1. *Incoherent operations* (IO) are defined as channels admitting a Kraus decomposition $\mathcal{E}(\rho) = \sum_\alpha K_\alpha \rho K_\alpha^\dagger$ such that $K_\alpha \rho K_\alpha^\dagger$ is an incoherent state for each α and each incoherent state ρ. It is known that these channels 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 [137].

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 [136], an erratum to [137] 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 chapter we show that a class of operations motivated by quantum computation gadgets are also unable to harness the power in a supplementary coherent state.

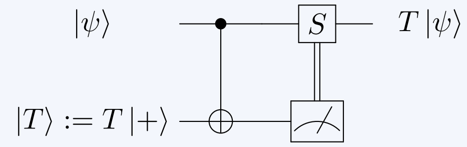
Example 4.2. Consider the gate set of Clifford + T, comprised of gates from $\{CNOT, H, S, T\}$, where H is the Hadamard gate and S is the phase gate. As discussed above, the T gates may be implemented by performing adaptive Clifford operations on supplementary T states. A natural question is: where 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 $|\psi\rangle \in \mathbb{C}^2$.



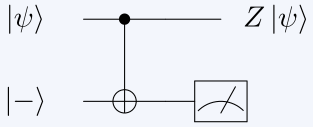
(4.1)

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



(4.2)

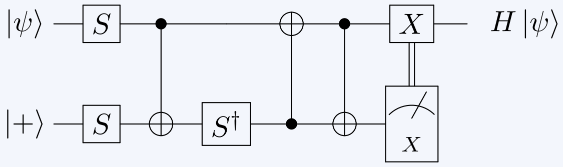
Observe that for $U = Z$, this becomes



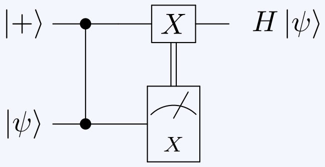
(4.3)

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 4.3. So-called Hadamard gadgets are known to exist [149–151], where they play roles relating to compilation and simulation of quantum circuits. For example, the following circuits appear in [149] and [150] respectively:



(4.4)



(4.5)

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

Example 4.4. In [135] 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 [135] is a hypergraph state [152], 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 4.5. In [153], 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 [154]. 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?

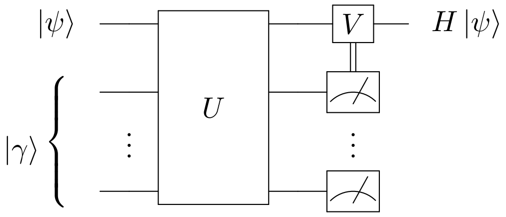
(3) Where can we put the 'cut' between states and operations for quantum computation in general?

(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 chapter 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.

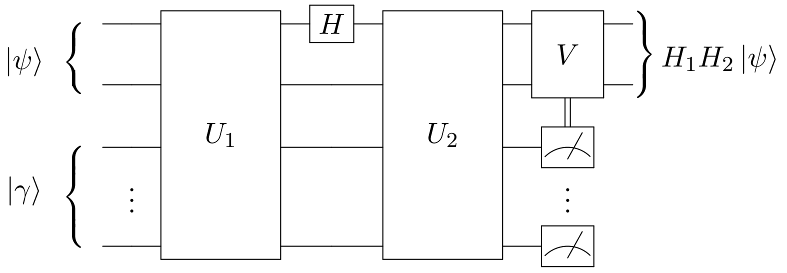
In particular, we rule out the existence of circuits of the following general form, for U and V incoherent unitaries (e.g. products of CNOTs and T gates):



(4.6)

Note that we know that the above diagram is possible with $|\gamma\rangle = |+\rangle$ if we instead allow X measurements, as shown in Example 4.3.

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:



(4.7)

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 chapter. 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. Section 1.4.7 provides further background to resource theories and coherence, and in particular we will use the definitions stated there for the dephasing map, and of states and unitaries being incoherent.

4.2 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 $|\gamma\rangle$. (4.8)

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.

4.2.1 Examples

Many approaches to quantum computation fall into the above framework – see Table 4.1 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 [139]).

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).

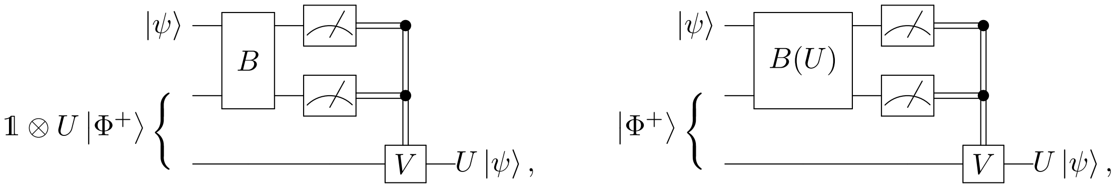
Let us also recall teleportation-based MBQC [37, 144]. Consider the following two circuit identities:

[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.

Model	Operations	State	References
Circuit	Universal gate set	–	[20]
Magic State Injection	Clifford	$\lvert T\rangle^{\otimes p}$	[74]
Matchgates	Nearest neighbour matchgates	$\lvert SWAP\rangle^{\otimes p}$	[139, 140]
1-way MBQC	LOCC	Graph state	[38, 134]
1-way MBQC	Hadamard	Hypergraph state	[135]
Teleportation MBQC	Rotated Bell unitaries Paulis	$\lvert \Phi^+\rangle^{\otimes p}$	[37, 144]

Table 4.1: Comparison of different models of quantum computation that fall into the framework summarised in Eq. (4.8), we are also allowing classical control and computational basis measurement and preparation freely. $\lvert T\rangle$, $\lvert SWAP\rangle$ and $\lvert\Phi^+\rangle$ respectively refer to the T state, the SWAP state [139], 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 [135] for a more extensive summary of MBQC approaches using different measurement bases.



(4.9)

where $B := (H\otimes\mathbb{1})CNOT_{12}$ denotes the Bell unitary, $B(U) := (\mathbb{1}\otimes U)B$ is the rotated Bell unitary, $\lvert\Phi^+\rangle = d^{-\frac{1}{2}}\sum_{k=0}^{d-1}\lvert kk\rangle \in \mathbb{C}^{d^2}$ 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) [155] proceeds by adaptively performing non-destructive Pauli measurements on $\lvert T\rangle$ 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 [134, 147]. 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 4.4.2.

4.2.2 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 4.6. 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

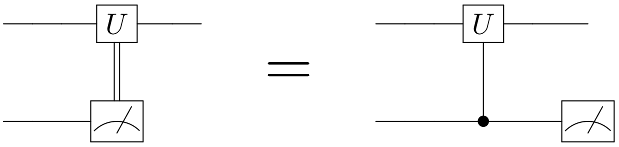
$$\sum_{x\in S} |x\rangle\langle x| \otimes U + \sum_{y\in S^c} |y\rangle\langle y| \otimes \mathbb{1}, \tag{4.10}$$

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 [20, 156] (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. (4.8). 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* [20], see Fig. 4.2. 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.



(4.11)

Figure 4.2: Principle of Deferred Measurement [20].

Observation 4.7. The most general channel possible to implement within the above framework is given by

$$\mathcal{E}(\rho) = \mathrm{Tr}_X\Big(U(\rho \otimes \tau)U^\dagger\Big). \tag{4.12}$$

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

$$\mathcal{E}^x(\rho) = \mathrm{Tr}_X\Big((\mathbb{1} \otimes |x\rangle\langle x|)\; U(\rho \otimes \tau)U^\dagger\Big), \tag{4.13}$$

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. (4.12) 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.

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.

$$\frac{\mathcal{E}(\rho)}{\mathrm{Tr}(\mathcal{E}(\rho))} = \mathcal{V}(\rho), \tag{4.14}$$

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

Remark 4.8. 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 this chapter 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. (4.12) 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. (4.12) and Eq. (4.13) as a solid foundation as we progress to our results section.

4.3 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 4.1.

We will proceed by considering channels of the form $\mathcal{E}(\rho) = \mathrm{Tr}_X(U(\rho\otimes\tau)U^\dagger)$ as in Eq. (4.12), and we will compare these to the channel $\rho \mapsto H^{\otimes n}\rho H^{\otimes n}$. As per the discussion above in Section 4.2, 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 4.2 for a detailed summary of our findings.

The following subsection introduces some simple facts and supporting results.

	$0 \mapsto n$		$k \mapsto n$	
Exact & Deterministic	✗	(Theorem 4.18)	✗	(Theorem 4.23)
Exact & Probabilistic	✗	(Theorem 4.18)	?	
Approximate & Deterministic	$\mathcal{D} \geq \frac{1}{2}\Big(1-2^{-n}\Big)$	(Theorem 4.20)	?	
Approximate & Probabilistic	$\mathcal{D} \geq \frac{1}{2}\Big(1-2^{-n}\Big)$	(Theorem 4.20)	?	

Table 4.2: 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 4.7. A question mark (?) indicates that we have not considered this case in this chapter. 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 4.21.

4.3.1 Preliminaries

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

Lemma 4.9. The family of controlled unitaries $\mathcal{C}(\mathcal{U})$ are incoherent if and only if $\mathcal{U}$ are incoherent.

Proof. Recall from Definition 4.6 that the controlled unitaries are of the form

$$V = \sum_{x \in S} |x\rangle\langle x| \otimes U + \sum_{y \in S^c} |y\rangle\langle y| \otimes \mathbb{1} \tag{4.15}$$

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 $V |c_1 c_2\rangle = |c_1 c_2\rangle$. Now consider $c_1 \in S$. For $U = \sum_z e^{i\theta_z} |\pi(z)\rangle\langle z|$ incoherent, we have

$$V |c_1 c_2\rangle = \sum_{x \in S} |x\rangle\langle x| \otimes U |c_1 c_2\rangle \tag{4.16}$$

$$= \sum_{x \in S} |x\rangle\langle x| \otimes \left(\sum_z e^{i\theta_z} |\pi(z)\rangle\langle z| \right) |c_1 c_2\rangle \tag{4.17}$$

$$= e^{i\theta_{c_2}} |c_1\rangle |\pi(c_2)\rangle . \tag{4.18}$$

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 $|c_1 c_2\rangle$ 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 4.7, 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 4.7 to be on the ancillary subsystem, i.e.

$$\mathcal{E}^x(\rho) = \mathrm{Tr}_2\Big(U(\rho \otimes \tau)U^\dagger\Big). \tag{4.19}$$

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

$$U = U_k V_k \dots U_1 V_1 U_0, \tag{4.20}$$

for U_i incoherent unitaries and V_i controlled-Hadamards ("controlled" in the general sense of Definition 4.6).

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

Definition 4.10. The *coherence rank* [34, 157] 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 4.11. 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. Then we have for any state $|\psi\rangle$, the coherence rank satisfies

$$\frac{\chi(|\psi\rangle)}{2^k} \leq \chi\left(U|\psi\rangle\right) \leq 2^k \chi(|\psi\rangle). \tag{4.21}$$

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 4.6), 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 $\chi(V|\psi\rangle) \leq 2\chi(|\psi\rangle)$ for all $|\psi\rangle$, which also implies that $\chi(|\psi\rangle) \leq 2\chi(V^\dagger|\psi\rangle) = 2\chi(V|\psi\rangle)$, as V is self-inverse. Combining these shows that

$$\frac{\chi(|\psi\rangle)}{2} \leq \chi\left(V|\psi\rangle\right) \leq 2\chi(|\psi\rangle). \tag{4.22}$$

Now we can use induction. The base case of $U = U_1V_1$ follows immediately from the above. Now suppose that

$$\frac{\chi(|\psi\rangle)}{2^k} \leq \chi\left(U_kV_k \ldots U_1V_1U_0|\psi\rangle\right) \leq 2^k\chi(|\psi\rangle). \tag{4.23}$$

Define $|\phi\rangle = U_kV_k \ldots U_1V_1U_0|\psi\rangle$, and we then get

$$\frac{\chi(|\phi\rangle)}{2} \leq \chi\left(U_{k+1}V_{k+1}|\phi\rangle\right) = \chi\left(V_{k+1}|\phi\rangle\right) \leq 2\chi(|\phi\rangle). \tag{4.24}$$

□

We will use these upper and lower bounds on the coherence rank as a key ingredient in Theorem 4.23, one of our no-go results.

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

Lemma 4.12. For the induced trace distance, it is sufficient to take the maximum over pure states, i.e. for any channels $\mathcal{E}$, $\mathcal{V}$

$$\mathcal{D}(\mathcal{E},\mathcal{V}) := \max_{\rho}\ D\Big(\mathcal{E}(\rho),\mathcal{V}(\rho)\Big) = \max_{|\phi\rangle}\ D\Big(\mathcal{E}(|\phi\rangle\langle\phi|),\mathcal{V}(|\phi\rangle\langle\phi|)\Big). \tag{4.25}$$

Proof.

$$\begin{aligned}
\max_{\rho} D(\mathcal{E}(\rho),\mathcal{V}(\rho)) &= \max_{p_i,\psi_i} D\Big(\sum p_i\mathcal{E}(\psi_i), \sum p_i\mathcal{V}(\psi_i)\Big) && (4.26)\\
&\leq \max_{p_i,\psi_i} \sum p_i D(\mathcal{E}(\psi_i),\mathcal{V}(\psi_i)) && (4.27)\\
&\leq \max_{p_i,\psi_i} \sum p_i \left(\max_{\phi} D(\mathcal{E}(\phi),\mathcal{V}(\phi))\right) && (4.28)\\
&= \max_{\phi} D(\mathcal{E}(\phi),\mathcal{V}(\phi)) && (4.29)\\
&\leq \max_{\rho} D(\mathcal{E}(\rho),\mathcal{V}(\rho)) && (4.30)
\end{aligned}$$

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 [20]. □

For pure states we also have that [21]

$$D\Big(|\psi\rangle\langle\psi|\,,|\phi\rangle\langle\phi|\Big) = \sqrt{1-|\langle\psi|\phi\rangle|^2}. \tag{4.31}$$

Combining this with Lemma 4.12 leads to the following corollary:

Corollary 4.13. The induced trace distance between unitary channels is given by

$$\mathcal{D}(U,V) = \max_{|\psi\rangle} \sqrt{1 - |\langle\psi| U^\dagger V |\psi\rangle|^2}. \tag{4.32}$$

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 4.14. 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

$$\mathcal{D}(U, H^{\otimes n}) \geq \sqrt{1 - 2^{k-n}}. \tag{4.33}$$

Proof. Using Corollary 4.13 we have that

$$\mathcal{D}(U, H^{\otimes n}) = \max_{|\psi\rangle} \sqrt{1 - |\langle\psi| H^{\otimes n} U |\psi\rangle|^2} \tag{4.34}$$

$$\geq \sqrt{1 - |\langle 0^n| H^{\otimes n} U |0^n\rangle|^2} \tag{4.35}$$

$$\geq \sqrt{1 - |\langle +^n| U |0^n\rangle|^2}. \tag{4.36}$$

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 4.11). 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

$$|\langle +^n| U |0^n\rangle|^2 = \left| \frac{\sum_{x=0}^{2^k-1} \alpha_x}{2^{\frac{n}{2}}} \right|^2 \leq \frac{2^k \sum_{x=0}^{2^k-1} |\alpha_x|^2}{2^n} = 2^{k-n}, \tag{4.37}$$

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

$$\mathcal{D}(U, H^{\otimes n}) \geq \sqrt{1 - |\langle +^n| U |0^n\rangle|^2} \tag{4.38}$$

$$\geq \sqrt{1 - 2^{k-n}}. \tag{4.39}$$

□

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.

4.3.2 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 4.15 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 4.16 that channels that only use incoherent resources supplemented with an arbitrary ancilla state (see Section 4.2) 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 [136] (an erratum to [137] – see Example 4.1 for more context here).

Lemma 4.15. 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

$$\Delta \circ \mathcal{E} \circ \Delta = \Delta \circ \mathcal{E}, \tag{4.40}$$

where Δ is the dephasing map defined in Eq. (1.88). 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 4.15. 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 (4.40) is met. This condition implies that

$$\Delta\Big(\mathcal{E}(\Delta(\rho \otimes \tau))\Big) = \Delta\Big(U\rho U^\dagger\Big), \qquad \forall \rho. \tag{4.41}$$

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

$$U|x\rangle = \sum_y U_{yx}|y\rangle \qquad\qquad U^\dagger|x\rangle = \sum_y U^*_{xy}|y\rangle \tag{4.42}$$

$$\langle x| U = \sum_y U_{xy}\langle y| \qquad\qquad \langle x| U^\dagger = \sum_y U^*_{yx}\langle y|\,, \tag{4.43}$$

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. (4.41) to obtain

$$\Delta\Big(\mathcal{E}(|x\rangle\!\langle x| \otimes \Delta(\tau))\Big) = \Delta\left(\sum_{y,z} U_{yx}U^*_{zx}|y\rangle\!\langle z|\right) \tag{4.44}$$

$$= \sum_y |U_{yx}|^2 |y\rangle\!\langle y| \tag{4.45}$$

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

$$\sum_x |U_{zx}|^2 \Delta\Big(\mathcal{E}(|x\rangle\!\langle x| \otimes \Delta(\tau))\Big) = \sum_{x,y} |U_{zx}|^2 |U_{yx}|^2 |y\rangle\!\langle y|\,. \tag{4.46}$$

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. (4.41) then implies that

$$\sum_x |U_{zx}|^2 \Delta \circ \mathcal{E}\Big(|x\rangle\!\langle x| \otimes \Delta(\tau)\Big) = |z\rangle\!\langle z| \,. \tag{4.47}$$

Comparing (4.46) with (4.47), as the left-hand sides are equal we see that

$$\sum_{x,y} |U_{zx}|^2 |U_{yx}|^2 \, |y\rangle\!\langle y| = |z\rangle\!\langle z| \,. \tag{4.48}$$

This can only be true if

$$\sum_x |U_{zx}|^2 |U_{yx}|^2 = 0 \quad \text{for } y \neq z. \tag{4.49}$$

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

$$|U_{zx}||U_{yx}| = 0 \quad \text{for } y \neq z,\, \forall x. \tag{4.50}$$

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,

$$U|x\rangle = \sum_y U_{yx} |y\rangle = U_{y'x} |y'\rangle \,, \tag{4.51}$$

for some y' (depending on x). Thus in summary, Eq. (4.41) 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 4.7 satisfy the condition in Lemma 4.15, and thus an arbitrary ancilla is not sufficient to elevate incoherent resources to computational universality.

Lemma 4.16. For any incoherent unitary U, the map $\rho \mapsto \mathrm{Tr}_2\Big(U\rho U^\dagger\Big)$ commutes with the dephasing map Δ.

See Eq. (1.86) for the definition of incoherent unitaries, and Eq. (1.88) 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. (1.86)).

Then for any state ρ we have

$$U\Delta(\rho)U^\dagger = \left(\sum_y e^{i\theta_y} |\pi(y)\rangle\langle y|\right) \sum_x |x\rangle\langle x| \,\rho\, |x\rangle\langle x| \left(\sum_z e^{-i\theta_z} |z\rangle\langle \pi(z)|\right) \tag{4.52}$$

$$= \sum_{x,y,z} e^{i\theta_y} e^{-i\theta_z} \;\; |\pi(y)\rangle \langle y|x\rangle \langle x| \,\rho\, |x\rangle \langle x|z\rangle \langle \pi(z)| \tag{4.53}$$

$$= \sum_x \;\; |\pi(x)\rangle\langle x| \,\rho\, |x\rangle\langle \pi(x)| \,. \tag{4.54}$$

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

$$\Delta(U\rho U^\dagger) = \sum_x |\pi(x)\rangle\langle\pi(x)| \left(\sum_y e^{i\theta_y} |\pi(y)\rangle\langle y| \,\rho \sum_z e^{-i\theta_z} |z\rangle\langle\pi(z)|\right) |\pi(x)\rangle\langle\pi(x)| \tag{4.55}$$

$$= \sum_{x,y,z} e^{i\theta_y} e^{-i\theta_z} \, |\pi(x)\rangle \langle \pi(x)|\pi(y)\rangle \langle y| \,\rho\, |z\rangle \langle \pi(z)|\pi(x)\rangle \langle \pi(x)| \tag{4.56}$$

$$= \sum_x \;\; |\pi(x)\rangle\langle x| \,\rho\, |x\rangle\langle \pi(x)| \,. \tag{4.57}$$

Hence the equality of Eq. (4.54) and Eq. (4.57) (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 4.15.

Hence Lemma 4.16 and Lemma 4.15 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 4.2), 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 4.7 (and surrounding text) that we represent these by convex combinations of normalised sub-channels

$$\mathcal{E}^x(\rho) = \alpha \mathrm{Tr}_X\Big(\mathbb{1} \otimes |x\rangle\langle x| \, U \rho \otimes \tau U^\dagger\Big). \tag{4.58}$$

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

Lemma 4.17. 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 4.16, and we give a more concise proof as follows.

Proof.

$$(\Delta \circ \mathcal{E}^x)(\rho) = \sum_i |i\rangle\langle i| \operatorname{Tr}_X \Big(\mathbb{1} \otimes |x\rangle\langle x| \, U\rho U^\dagger \Big) \, |i\rangle\langle i| \tag{4.59}$$

$$= \sum_j \operatorname{Tr}_X \Big(\, |j\rangle\langle j| \, \mathbb{1} \otimes |x\rangle\langle x| \, U\rho U^\dagger \, |j\rangle\langle j| \, \Big) \tag{4.60}$$

$$= \operatorname{Tr}_X \Big(\mathbb{1} \otimes |x\rangle\langle x| \sum_j |j\rangle\langle j| \, U\rho U^\dagger \, |j\rangle\langle j| \, \Big) \tag{4.61}$$

$$= \operatorname{Tr}_X \Big(\mathbb{1} \otimes |x\rangle\langle x| \, U \sum_j |j\rangle\langle j| \, \rho \, |j\rangle\langle j| \, U^\dagger \Big) \tag{4.62}$$

$$= (\mathcal{E}^x \circ \Delta)(\rho) \tag{4.63}$$

□

As any convex combination of such channels will also commute with the dephasing map, by Lemma 4.15 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 4.18. 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 4.2, 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 4.16 and Lemma 4.17, these maps commute with the dephasing map Δ. Hence we can apply Lemma 4.15 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 4.7 and n Hadamard gates. Our second main technical result achieves this goal as follows.

Lemma 4.19. 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.

$$\mathcal{E} \circ \Delta = \Delta \circ \mathcal{E}, \tag{4.64}$$

where Δ is the dephasing map defined in Eq. (1.88). 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

$$\mathcal{D}\Big(\mathcal{E}_\tau \ , \ H^{\otimes n}\Big) \geq 1 - \frac{1}{2^n}. \tag{4.65}$$

Proof of Lemma 4.19.. 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

$$\begin{aligned}
\mathcal{D}\Big(\mathcal{E}_\tau \ , \ H^{\otimes n}\Big) &:= \max_\rho D\Big(\mathcal{E}(\rho \otimes \tau) \ , \ H^{\otimes n}\rho H^{\otimes n}\Big) && (4.66)\\
&\geq \max_\rho D\Big(\Delta \circ \mathcal{E}(\rho \otimes \tau) \ , \ \Delta(H^{\otimes n}\rho H^{\otimes n})\Big) && (4.67)\\
&= \max_\rho D\Big(\mathcal{E}(\Delta(\rho) \otimes \Delta(\tau)) \ , \ \Delta(H^{\otimes n}\rho H^{\otimes n})\Big) && (4.68)\\
&\geq \max_{|\phi\rangle \in B_n} D\Big(\mathcal{E}(\Delta(|\phi\rangle\!\langle\phi|) \otimes \Delta(\tau)) \ , \ \Delta(H^{\otimes n}\,|\phi\rangle\!\langle\phi|\,H^{\otimes n})\Big) && (4.69)\\
&= \max_{|\psi\rangle \in C_n} D\Big(\mathcal{E}(\frac{\mathbb{1}}{2^n} \otimes \Delta(\tau)) \ , \ |\psi\rangle\!\langle\psi|)\Big), && (4.70)
\end{aligned}$$

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

$$\begin{aligned}
\mathcal{D}\Big(\mathcal{E}_\tau \ , \ H^{\otimes n}\Big) &\geq \max_{|\psi\rangle \in C_n} D\Big(\sigma \ , \ |\psi\rangle\!\langle\psi|)\Big) && (4.71)\\
&\geq \max_{|\psi\rangle \in C_n} D\Big(\Delta(\sigma) \ , \ \Delta(|\psi\rangle\!\langle\psi|))\Big) && (4.72)\\
&= \max_{|\psi\rangle \in C_n} D\Big(\Delta(\sigma) \ , \ |\psi\rangle\!\langle\psi|)\Big) && (4.73)\\
&\geq \max_{|\psi\rangle \in C_n} \Big(1 - \langle\psi|\,\Delta(\sigma)\,|\psi\rangle\Big) && (4.74)\\
&\geq 1 - \frac{1}{2^n} && (4.75)
\end{aligned}$$

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 4.2, 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 [22], 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 (4.13) commutes with Δ (Lemma 4.17) we see that Lemma 4.19 also applies. The conclusion is that even approximate, probabilistic implementation of Hadamards is not possible, which is our second main result. Recall (see Eq. (1.44) and subsequent paragraph) 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 4.20. Given the ability to perform incoherent unitaries, computational basis measurements and classical control, it is impossible 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 4.18. 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 4.2). These maps commute with the dephasing map Δ by Lemma 4.16 and Lemma 4.17. Then Lemma 4.19 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 $1 - 2^{-n}$. □

4.3.3 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 4.6. 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. 4.3, 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.

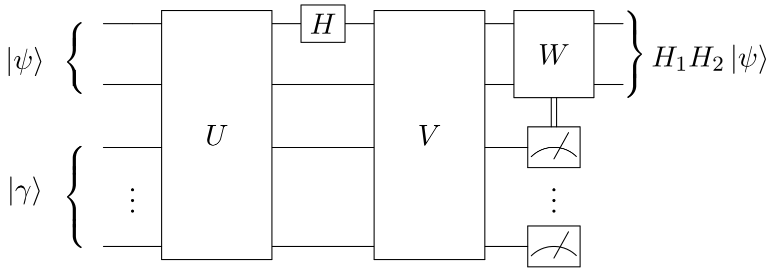


Figure 4.3: A possible circuit for using a single Hadamard gate and incoherent unitaries U, V and W to implement two Hadamard gates. We rule out the existence of such a circuit in this chapter.

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:

$$H_1 H_2 |\psi\rangle |\gamma_\psi\rangle = V H_1 U |\psi\rangle |\gamma\rangle , \tag{4.76}$$

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 4.2 that we can replace the last gate W by its quantum controlled version (which will be incoherent by Lemma 4.9) 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

$$H_1 H_2 |\psi\rangle |\gamma_\psi\rangle = \sum_x \alpha_x V H_1 U |x\rangle |\gamma\rangle = \sum_x \alpha_x H_1 H_2 |x\rangle |\gamma_x\rangle . \tag{4.77}$$

Tracing out the first register then gives

$$|\gamma_\psi\rangle\langle\gamma_\psi| = \sum_x |\alpha_x|^2 |\gamma_x\rangle\langle\gamma_x| \,, \tag{4.78}$$

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

$$VH_1U|\psi\rangle|\gamma\rangle = H_1H_2|\psi\rangle|\gamma'\rangle \tag{4.79}$$

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. (4.79) implies the following two equations

$$VH_1U|00\rangle|\gamma\rangle = |{+}{+}\rangle|\gamma'\rangle \tag{4.80}$$

$$VH_1U|{+}{+}\rangle|\gamma\rangle = |00\rangle|\gamma'\rangle \,. \tag{4.81}$$

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

$$4r' \in [\frac{r}{2}, 2r] \tag{4.82}$$

$$r' \in [2r, 8r] \quad \implies 4r' \in [8r, 32r], \tag{4.83}$$

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

$$\mathrm{Tr}_2\left(U\rho\otimes|\gamma\rangle\langle\gamma|\,U^\dagger\right) = V\rho V^\dagger. \tag{4.84}$$

Then

$$\mathrm{Tr}_1\left(U\rho\otimes|\gamma\rangle\langle\gamma|\,U^\dagger\right) = |\gamma'\rangle\langle\gamma'| \tag{4.85}$$

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. (4.84) becomes

$$\mathrm{Tr}_2\left(U\,|\psi\rangle\langle\psi| \otimes |\gamma\rangle\langle\gamma|\,U^\dagger\right) = V\,|\psi\rangle\langle\psi|\,V^\dagger. \tag{4.86}$$

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

$$U\Big(\,|\psi\rangle\,|\gamma\rangle\,\Big) = V\otimes\mathbb{1}\Big(\,|\psi\rangle\,|\gamma_\psi\rangle\,\Big) \tag{4.87}$$

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

$$V\otimes\mathbb{1}\,|\psi\rangle\,|\gamma_\psi\rangle = \sum_x \alpha_x\; U\,|x\rangle\,|\gamma\rangle = \sum_x \alpha_x\; V\otimes\mathbb{1}\,|x\rangle\,|\gamma_x\rangle \tag{4.88}$$

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

$$\sum_x \alpha_x\,|x\rangle\,|\gamma_\psi\rangle = \sum_x \alpha_x\;\;|x\rangle\,|\gamma_x\rangle\,. \tag{4.89}$$

Tracing out the first system gives

$$|\gamma_\psi\rangle\langle\gamma_\psi| = \sum_x |\alpha_x|^2\,|\gamma_x\rangle\langle\gamma_x|\,, \tag{4.90}$$

which in turn implies

$$|\gamma_\psi\rangle\langle\gamma_\psi| = |\gamma_x\rangle\langle\gamma_x| = |\gamma_{x'}\rangle\langle\gamma_{x'}| \qquad \forall x, x', \psi \tag{4.91}$$

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

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

$$\mathrm{Tr}_1\left(U\,|\psi\rangle\langle\psi| \otimes |\gamma\rangle\langle\gamma|\,U^\dagger\right) = |\gamma'\rangle\langle\gamma'| \tag{4.92}$$

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

$$\begin{aligned}\mathrm{Tr}_1\left(U\rho\otimes|\gamma\rangle\langle\gamma|\,U^\dagger\right) &= \sum_k p_k \mathrm{Tr}_1\left(U\,|\psi_k\rangle\langle\psi_k|\otimes|\gamma\rangle\langle\gamma|\,U^\dagger\right) && (4.93)\\ &= \sum_k p_k\,|\gamma'\rangle\langle\gamma'| && (4.94)\\ &= |\gamma'\rangle\langle\gamma'| && (4.95)\end{aligned}$$

□

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:

$$U = U_k V_k \dots U_1 V_1 U_0, \tag{4.96}$$

where U_i are incoherent unitaries and V_i are Hadamards or controlled Hadamards (in the general sense of Definition 4.6). As discussed in Section 4.2, this describes any operation involving incoherent unitaries, classical control and k Hadamard gates – see Eq. (4.20) and surrounding text. We can now state our next result.

Lemma 4.22. 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

$$\mathrm{Tr}_2\left(U\rho \otimes |\gamma\rangle\!\langle\gamma|\, U^\dagger\right) = H^{\otimes n}\rho H^{\otimes n} \qquad \forall\rho, \tag{4.97}$$

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

Proof. Consider the case where $\rho = |\psi\rangle\!\langle\psi|$ is a pure state. Using Lemma 4.21, we can then write Eq. (4.97) as

$$U\,|\psi\rangle\,|\gamma\rangle = H^{\otimes n} \otimes \mathbb{1}\,|\psi\rangle \otimes |\gamma'\rangle \tag{4.98}$$

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

Let $|\gamma\rangle$ and $|\gamma'\rangle$ have coherence ranks r and r' respectively (recall Definition 4.10 for the definition of the coherence rank χ), and consider the cases of $|\psi\rangle$ being equal to $|0^n\rangle$ and $|+^n\rangle$:

$$U\,|0^n\rangle\,|\gamma\rangle = |+^n\rangle\,|\gamma'\rangle \tag{4.99}$$

$$U\,|+^n\rangle\,|\gamma\rangle = |0^n\rangle\,|\gamma'\rangle\,. \tag{4.100}$$

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

$$\frac{\chi(U\,|0^n\rangle\,|\gamma\rangle)}{2^n} = \chi(U\,|+^n\rangle\,|\gamma\rangle). \tag{4.101}$$

We now directly apply Lemma 4.11, 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

$$\chi(U\,|0^n\rangle\,|\gamma\rangle) \leq 2^k \chi(|0^n\rangle\,|\gamma\rangle) = 2^k r \tag{4.102}$$

$$\chi(U\,|+^n\rangle\,|\gamma\rangle) \geq 2^{-k} \chi(|+^n\rangle\,|\gamma\rangle) = 2^{n-k} r. \tag{4.103}$$

Combining these with Eq. (4.101) leads to

$$2^{n-k} r \leq 2^{k-n} r, \tag{4.104}$$

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

$$n \leq k \tag{4.105}$$

as claimed. □

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

Theorem 4.23. 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 4.2, any operation involving incoherent incoherent unitaries, k Hadamards, computational basis measurements, classical control and access to some ancillary state $|\gamma\rangle$ can be written as $\rho \mapsto \mathrm{Tr}_2(U\rho \otimes |\gamma\rangle\langle\gamma| U^\dagger)$, where $U = U_k V_k \ldots U_1 V_1 U_0$ alternates between incoherent unitaries U_i and controlled Hadamards V_i (controlled in the general sense of Definition 4.6). Lemma 4.22 then directly yields the result. □

4.4 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. There are many interesting future avenues to explore.

4.4.1 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. (4.13). We leave these questions to ongoing and future work, in order to complete the picture as presented in Table 4.2.

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 4.19) compared to not using an ancilla at all (Lemma 4.21), perhaps there is still some advantage to be had here. In this chapter, 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 chapter, and find lower bounds on implementing n Hadamards using k Hadamards, incoherent unitaries, classical control, computational basis measurements, and an arbitrary ancilla.*

4.4.2 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 [134, 147], taking LOCC as the free operations. In particular, in [134] 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 [147].

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 chapter. 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 [158, 159], hence this approach is highly impractical and more refined ideas would be needed.

One could extend the definitions in [134, 147] 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 aforementioned works.

Definition 4.24. 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 [147]. 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 [135], 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 [135], 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 [32, 33]. 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] [32].

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 [73, 149, 150], 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.

4.4.3 General resource theories

Finally, our analysis raises some interesting questions for general resource theories [35], see Section 1.4.7 for some background. 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 4. *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

$$\mathcal{E}(\rho) = \mathrm{Tr}_2\left(U\rho\otimes\tau U^\dagger\right) \tag{4.106}$$

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 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 [160] 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.

Problem 5. *Is there a trade-off between unitarity and resource generating power?*

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

In light of this, we note that the style of channels considered in this chapter 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.

4.4.4 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.

4.5 Acknowledgements and contributions

This work began around September 2021 with my two supervisors, Paul Skrzypczyk and Noah Linden. We started by talking about the resource theory of magic in quantum computation, and over the next few months discussed a variety of surrounding topics and literature. This lead us to ask a natural question of where else it might be possible to put the "cut" between gates and states in the Clifford + T gate set. We pondered the existence of a Hadamard gadget using only computational basis measurements and incoherent unitaries, and after some time were able to prove our main no-go result. We then wanted to extend this to show that k Hadamards could not be used to implement $n > k$ Hadamards, and this result followed shortly afterwards.

I undertook the technical calculations under guidance from my two supervisors. After some discussion we decided to write a paper with a relatively comprehensive introduction, with the aim of providing sufficient background to place our work in context, and also serving as a useful summary of various bodies of literature. I wrote the paper, and we posted the paper to the arXiv after a few rounds of editing. The paper was recently accepted at the journal *Quantum*.

I would like to thank my co-authors and supervisors Paul Skrzypczyk and Noah Linden for their guidance, insights, and good humour during this project.

We are also extremely grateful to Andreas Winter for pointing out a way to improve Lemma 4.19, and for kindly letting us use the new version of the Lemma and his proof.

CHAPTER 5

Testing multipartite productness is easier than testing bipartite productness

Chapter Summary

We prove a lower bound on the number of copies needed to test the property of a multipartite quantum state being product across some bipartition (i.e. not genuinely multipartite entangled), given the promise that the input state either has this property or is ϵ-far in trace distance from any state with this property. We show that $\Omega(n/\log n)$ copies are required (for fixed $\epsilon \leq \frac{1}{2}$), complementing a previous result that $O(n/\epsilon^2)$ copies are sufficient. Our proof technique proceeds by considering uniformly random ensembles over such states, and showing that the trace distance between these ensembles becomes arbitrarily small for sufficiently large n unless $k = \Omega(n/\log n)$. We discuss implications for testing graph states and computing the generalised geometric measure of entanglement.

This chapter is based on unpublished work with Ashley Montanaro.

Relevant background: multipartite entanglement and Schmidt decomposition (Section 1.4.2), Haar integration and the symmetric subspace (Section 1.4.8).

Contents

5.1 Introduction

Quantum entanglement [29, 76, 161] is celebrated as a ubiquitous resource across the whole landscape of quantum information and technology. In measurement based approaches to quantum computation [37, 38, 138], one seeks to generate entanglement between multiple sites, for example via the creation of graph states [162, 163], and an important practical task is to be able to certify the presence (or lack of) such entanglement [164, 165]. Multipartite entanglement [166, 167] is also a fundamental component of quantum networks [61, 168] and plays a significant role in quantum error correction [169, 170].

In classical computer science, the domain of property testing [171, 172] seeks to ascertain if a given object has some property P, or is far away from having that property. An ϵ-*tester* takes as input either $x \in P$ or x ϵ-far from P, and in the former case it accepts with probability at least $\frac{2}{3}$, whereas in the latter case it accepts with probability at most $\frac{1}{3}$. A tester is deemed *efficient* if the number of queries made (e.g. number of bits of the object read) is much less than the size n of the object. Quantum property testing applies these notions to the quantum world, where one can take either the tester or the object to be tested (or both) to be quantum mechanical in some aspect – see [36] for a comprehensive review. When testing properties of quantum states, one typically seeks algorithms that minimise the number of copies required to test the desired property. In particular, it is highly desirable to prove lower bounds on the number of copies required, to understand the optimality of various approaches and the fundamental limits on extracting information from quantum states.

In this chapter we will study the property of a multipartite quantum state being product across some (unknown) bipartition, or equivalently the property of not being *genuinely multipartite entangled*, through the lens of property testing. Let us formalise some definitions.

Definition 5.1. Consider a state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ consisting of n parties, each of local dimension d. We say that it is

- *Genuinely multipartite entangled* (GME) if it is entangled across any bipartition of the n parties.
- *Bipartite product* (BP) if it is not GME, that is, there exists some non-trivial partition $S \subset [n]$ such that the state is product across this bipartition.
- *Multipartite product* (MP) if the state is product across every bipartition, i.e. the state can be written as the tensor product of n local states.

In [173], it is shown that given an n-partite state $|\psi\rangle$ that is either multipartite product, or is at least ϵ far from any multipartite product state, there exists a tester using two copies of the input state $|\psi\rangle$, and accepts with certainty if $|\psi\rangle$ is MP and accepts with probability at most $1 - \Theta(\epsilon^2)$ otherwise. Repeating this procedure k times (using $2k$ copies) reduces this latter probability to $(1 - \Theta(\epsilon^2))^k \leq e^{-\Theta(k\epsilon^2)}$, and hence the property of multipartite productness can be tested using $O(1/\epsilon^2)$ copies, for any n. The proof strategy uses the product test [174], which in turn consists of applying the swap test [175] (a simple test for equality of two states) across corresponding pairs of subsystems of two copies of the input state (also see [36] for a proof sketch).

Furthermore, a general result is derived in [176] for testing multiple properties of a quantum state simultaneously. More specifically, given a set of measurement operators M_i (POVM elements satisfying $0 \leq M_i \leq \mathbb{1}$, corresponding to different measurements $\{M_i\ ,\ \mathbb{1} - M_i\}$) and an input state ρ with the promise that either $\mathrm{Tr}(M_i\rho)$ is small for all i, or there exists at least one i with $\mathrm{Tr}(M_i\rho)$ large, the authors construct a procedure that distinguishes between these cases using one copy of the input state ρ. In the same paper this result is applied to testing bipartite productness: building upon the result from [173] they derive a tester using $O(n/\epsilon^2)$ copies of the state.

In this chapter, we show that this is close to optimal – at least $\Omega(n/\log n)$ copies are needed to test bipartite productness, for any fixed constant $0 < \epsilon \leq \frac{1}{2}$. Our main result can be stated formally as follows.

Theorem 5.2. An ϵ-tester for testing the property of a multipartite state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ being bipartite product requires at least $\Omega\left(\frac{n}{\log n}\right)$ copies of the input state $|\psi\rangle$, for any $0 < \epsilon \leq \frac{1}{2}$.

So testing bipartite productness across an unknown bipartition is harder than testing both multipartite productness or productness across a known partition (both can be done with $O(1/\epsilon^2)$ copies), hence it appears that the uncertainty regarding which partition the state is product across is responsible for the increase in hardness. We now comment on two initial applications of our result.

Recall that *graph states* [162, 163] are defined by associating a qubit initialised in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ state for every node, and applying a controlled-Z gate for every corresponding edge. Given a graph state, one can consider testing classical properties of the underlying graph [177] using few copies of the state [178, 179]. In particular, our work here relates to the property of the underlying graph being *connected*: if there exists a path from any vertex to any other vertex. The underlying graph is not connected if and only if the associated state is bipartite product. Therefore our results imply that any attempt to test non-connectivity of the underlying graph by testing if the state is bipartite product must use $\Omega(n/\log n)$ copies. However, it is not ruled out that one could test for non-connectivity using fewer copies, taking advantage of the information that the given state is promised to be a graph state.

Secondly, consider the following quantifier of multipartite entanglement

$$E_G(|\psi\rangle) := 1 - \max_{|\phi\rangle \text{ is BP}} |\langle\psi|\phi\rangle|^2 \tag{5.1}$$

$$= \min_{|\phi\rangle \text{ is BP}} D\left(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|\right)^2 \tag{5.2}$$

for D the trace distance. This is known as the *generalised geometric measure of entanglement* – see [180–182] and references therein. Thus we can reinterpret our main result as showing that to determine if either $E_G(|\psi\rangle) = 0$ or $E_G(|\psi\rangle) \geq \epsilon^2$ (given the promise that one of them holds), you need $\Omega(n/\log n)$ copies of $|\psi\rangle$, for any $0 < \epsilon \leq \frac{1}{2}$. So in general one can expect computing E_G to require at least this many copies.

Our proof of Theorem 5.2 proceeds in several steps:

(i) We first show in Lemma 5.3 that if a tester exists, then this places a lower bound on the trace distance of certain quantum states. These quantum states are respectively close to distributions over BP and ϵ-far from BP states.

(ii) We then give an upper bound on the trace distance between these states as a function of n (the number of parties), k (the number of copies) and d (the local dimension) – this is Lemma 5.4.

(iii) Finally, we see that unless $k = \Omega(n/\log n)$, then this upper bound goes to zero, which contradicts the existence of a tester.

The bulk of the technical work is in proving point (ii), which requires calculations involving the Haar measure, symmetric subspace and permutation matrices – see e.g. [81, 183, 184] for relevant literature.

5.1.1 Summary of results

Main conceptual contributions:

- We show that testing bipartite productness of a multipartite state requires $\Omega(n/\log n)$ copies of the state.
- This also gives a lower bound on the number of copies required to compute the generalised geometric measure of entanglement, and on testing for non-connectivity in graph states using this method.

Main technical calculations:

Lemma 5.4. Consider the following states

$$\rho = \frac{\Pi^k_{d^n}}{\binom{d^n+k-1}{k}}, \qquad \sigma = \mathop{\mathbb{E}}_{S\subseteq[n]}\left[\frac{\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{n-|S|}}}{\binom{d^{|S|}+k-1}{k}\binom{d^{n-|S|}+k-1}{k}}\right], \tag{5.3}$$

where Π^k_d denotes the projector onto the symmetric subspace of k systems of local dimension d. Then their squared trace-distance is upper bounded by the following expression:

$$D(\rho,\sigma)^2 \leq \frac{k!}{4}\left(1 + (k!)^3\left(\frac{1+d}{2d}\right)^n - e^{-k^2/d^n}\right). \tag{5.4}$$

Lemma 5.5. Let $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ be drawn uniformly at random from the Haar measure, and let $\Gamma_{\max}$ denote the maximum Schmidt coefficient over all non-trivial bipartitions.

Let $\frac{\sqrt{3}}{2} \leq \gamma < 1$ be a constant. Then there exist positive constants c_1, c_2 and N (in terms of γ, d) such that for all $n > N$

$$\mathbb{P}\left(\Gamma_{\max} > \gamma\right) \leq c_1 2^n e^{-c_2 d^n}. \tag{5.5}$$

Open questions:

- Can our lower bound be improved to $\Omega(n)$ to tightly match the known upper bound?
- How many copies of the input state are required to test the complementary property of being maximally multipartite entangled (according to some particular measure)?

Prior work and concepts:

- Montanaro and de Wolf give an excellent overview to quantum property testing in general [36], and there exist several excellent reviews of entanglement [28, 29], which cover the multipartite setting. In addition, [162] gives an overview of graph states and their applications.
- In [173], the authors discuss testing the property of being a product state.
- The main upper bound of $O(n)$ for testing the property of being not genuinely multipartite product comes from [176] – this paper motivates our work as we seek to determine how optimal this approach is.

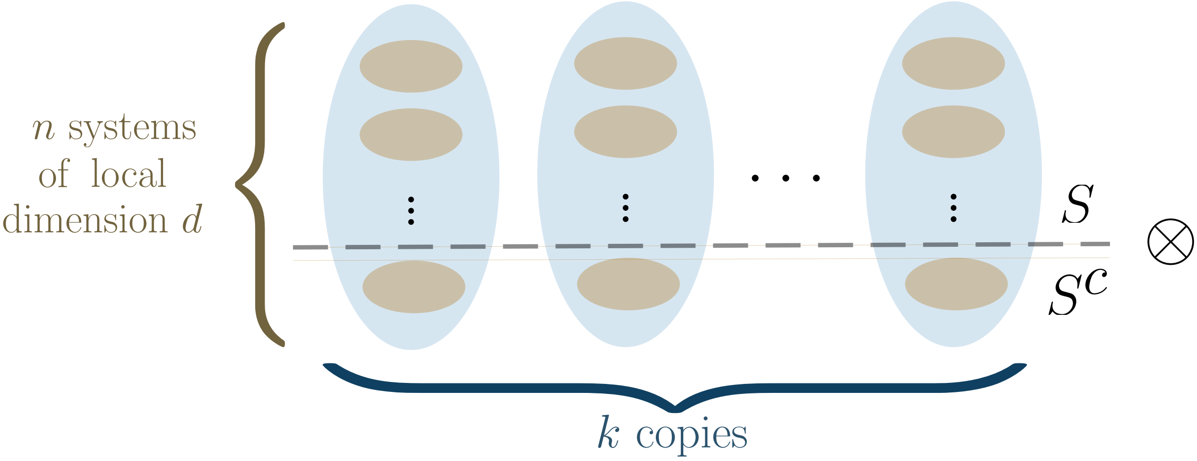


Figure 5.1: Illustration of the property considered in this chapter. The input is given by a quantum state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$, which is either product across some bipartiton $S : S^c$, or ϵ-far from being product. We are interested in algorithms for distinguishing these cases that use a small number of copies k of the input state $|\psi\rangle$. Some of the technical aspects of this chapter (see Lemma 5.4) involve unitaries U_α that permute the k systems according to a permutation $\alpha \in \mathcal{S}_k$. Note that in the context of this diagram, these permutations U_α permute the k 'columns', and not the n 'rows', and hence given some bipartion $S \subset [n]$ we can write $U'_\alpha = U_\alpha \otimes_S U_\alpha$ for U'_α acting on the whole space – see also Eq. (5.6).

5.1.2 Mathematical preliminaries

We use $D(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1$ to denote trace distance, $\binom{n}{k} := \frac{n!}{(n-k)!k!}$ the binomial coefficients, and $[n] := \{0, \dots, n-1\}$ the set of numbers from 0 to $n-1$ inclusive. We write 'ln' for the natural logarithm and 'log' for the logarithm to base 2. Recall the definitions of the symmetric subspace from Section 1.4.8.

We use S^c to denote the complement of a subset $S \subseteq [n]$, and $|S|$ to denote the size of the set S, so for example $|S| + |S^c| = n$. We denote the empty set by $\emptyset$.

For a multipartite quantum state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ that is product across some bipartition $S \subset [n]$, we may use labels on the states and tensor product symbol for clarity. For example, if the state $|\psi\rangle$ is product across the bipartition $S : S^c$ with respective states $|\phi\rangle$ and $|\tau\rangle$, for k copies we may write (see also Fig. 5.1)

$$|\psi\rangle^{\otimes k} = \left|\phi^S\right\rangle^{\otimes k} \otimes_S \left|\tau^{S^c}\right\rangle^{\otimes k}, \tag{5.6}$$

and similarly for operators.

Finally, recall that Schmidt decomposition allows us to write any bipartite state $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ as

$$|\psi\rangle = \sum_i \gamma_i \left|v_i\right\rangle \left|w_i\right\rangle, \tag{5.7}$$

where the Schmidt coefficients γ_i are non-negative, the sets $|v_i\rangle$ and $|w_i\rangle$ are respectively orthonormal, and the number of terms in the expansion is minimal and is referred to as the Schmidt rank – see also Definition 1.19.

5.2 Results

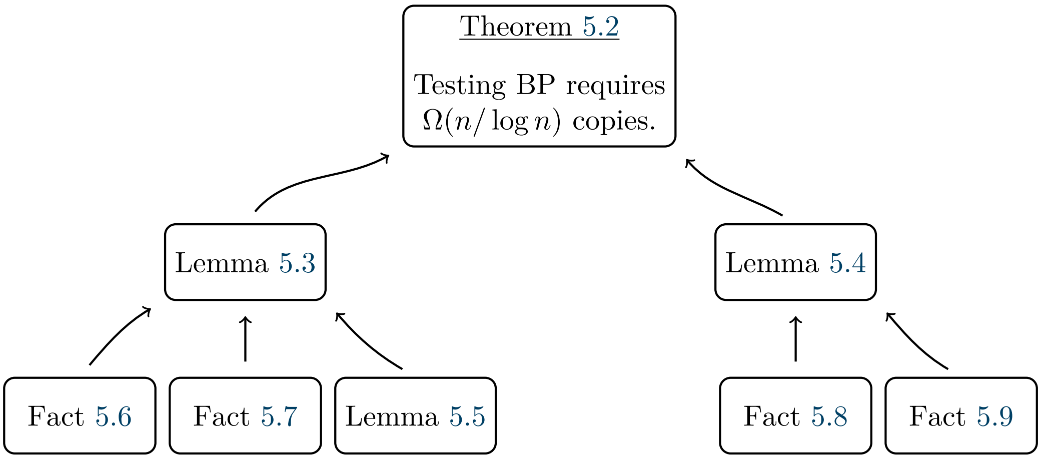


Figure 5.2: Proof structure of the main theorem in this chapter and supporting results.

We first state the two main ingredients used in the proof of our main result.

Lemma 5.3. For $0 < \epsilon \leq \frac{1}{2}$, the existence of an ϵ-tester for the property of a multipartite state being bipartite product using k copies implies that

$$D(\rho, \sigma) \ \geq \ \frac{1}{3} - O(2^{-n}), \tag{5.8}$$

for D the trace distance, and where

$$\rho = \frac{\Pi^k_{d^n}}{\binom{d^n+k-1}{k}}, \qquad \sigma = \mathop{\mathbb{E}}_{S\subseteq[n]}\left[\frac{\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{n-|S|}}}{\binom{d^{|S|}+k-1}{k}\binom{d^{n-|S|}+k-1}{k}}\right], \tag{5.9}$$

for Π^k_d the projector onto the symmetric subspace of k systems of local dimension d.

Lemma 5.4. Consider the following states

$$\rho = \frac{\Pi^k_{d^n}}{\binom{d^n+k-1}{k}}, \qquad \sigma = \mathop{\mathbb{E}}_{S\subseteq[n]}\left[\frac{\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{n-|S|}}}{\binom{d^{|S|}+k-1}{k}\binom{d^{n-|S|}+k-1}{k}}\right], \tag{5.10}$$

where Π^k_d denotes the projector onto the symmetric subspace of k systems of local dimension d. Then their squared trace-distance is upper bounded by the following expression:

$$D(\rho,\sigma)^2 \leq \frac{k!}{4}\left(1 + (k!)^3\left(\frac{1+d}{2d}\right)^n - e^{-k^2/d^n}\right). \tag{5.11}$$

Using these two ingredients we can prove our main theorem.

5.2.1 Proof of Main Result

Theorem 5.2. An ϵ-tester for testing the property of a multipartite state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ being bipartite product requires at least $\Omega\left(\frac{n}{\log n}\right)$ copies of the input state $|\psi\rangle$, for any $0 < \epsilon \leq \frac{1}{2}$.

Proof of Theorem 5.2. If a tester exists, by Lemma 5.3 we have that

$$\frac{1}{3} \leq O(2^{-n}) + D(\rho, \sigma) \tag{5.12}$$

for the states ρ, σ as stated. Lemma 5.4 then gives us

$$
\begin{aligned}
D(\rho,\sigma)^2 &\leq \frac{k!}{4}\left(1+(k!)^3\left(\frac{1+d}{2d}\right)^n - e^{-k^2/d^n}\right) && (5.13)\\
&\leq \frac{k!}{4}\left((k!)^3\left(\frac{1+d}{2d}\right)^n + O(k^2/d^n)\right) && (5.14)\\
&\leq \frac{k^{4k}}{4}2^{-n}\left(1+\frac{1}{d}\right)^n + O(k^{2+k}d^{-n}), && (5.15)
\end{aligned}
$$

where we used $k! \leq k^k$ and $1 - e^{-k^2/d^n} = O(k^2/d^n)$ (assuming $k^2/d^n < 1\ \forall n$). The latter can be seen from the fact that $1 - e^{-f(n)} \leq e^{-1}f(n)$ for all functions $f(n) \leq 1$.

As the local dimension $d \geq 2$, we have $1 + \frac{1}{d} \leq \frac{3}{2}$, and so

$$
\begin{aligned}
D^2 &\leq \frac{k^{4k}}{4}2^{-n}\left(\tfrac{3}{2}\right)^n + O(k^{2+k}d^{-n}) && (5.16)\\
&\leq O\left(k^{4k}\left(\tfrac{3}{4}\right)^n\right) + O(k^{2+k}2^{-n}) && (5.17)\\
&\leq O\left(k^{4k}\left(\tfrac{3}{4}\right)^n\right) && (5.18)\\
&= O\left(2^{4k\log k - n\log 4/3}\right). && (5.19)
\end{aligned}
$$

Thus after taking the square root we have

$$
D \leq O\left(2^{2k\log k - an}\right), \tag{5.20}
$$

where $a = \frac{1}{2}\log 4/3 \approx 0.208$. Now take $k < \frac{cn}{\log n}$, with $0 < c < \frac{a}{2}$. Then observe that

$$
\begin{aligned}
2k\log k - an &< \frac{2cn}{\log n}\left(\log c + \log n - \log\log n\right) - an && (5.21)\\
&= (2c-a)n + (c\log c)\left(\frac{n}{\log n}\right) - c\left(\frac{n\log\log n}{\log n}\right) && (5.22)\\
&< 0 \quad \text{for sufficiently large } n\text{, as } 2c < a. && (5.23)
\end{aligned}
$$

This means that $O(2^{2k\log k - an})$ would tend to zero as n goes to infinity. This contradicts the assertion that a tester must satisfy

$$
\frac{1}{3} \leq O(2^{-n}) + D(\rho,\sigma), \tag{5.24}
$$

as the right hand side of the inequality would tend to zero as n tends to infinity. Hence no tester exists unless $k \in \Omega(\frac{n}{\log n})$.

□

We also state and prove the following result on the distribution of the maximum Schmidt coefficient under the Haar measure. Aside from potentially being of independent interest, it primarily serves as a crucial ingredient in Lemma 5.3 where it is needed to show that the Haar distribution is close to the same distribution conditioned on states with bounded maximum Schmidt coefficient.

Lemma 5.5. Let $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ be drawn uniformly at random from the Haar measure, and let $\Gamma_{\max}$ denote the maximum Schmidt coefficient over all non-trivial bipartitions.

Let $\frac{\sqrt{3}}{2} \leq \gamma < 1$ be a constant. Then there exist positive constants c_1, c_2 and N (in terms of γ and d, expressions given below) such that for all $n > N$

$$\mathbb{P}\left(\Gamma_{\max} > \gamma\right) \leq c_1 2^n e^{-c_2 d^n}. \tag{5.25}$$

Here c_1, c_2, N are given by

$$c_1 = \tfrac{1}{2}\left(\frac{30}{\gamma^2}\right)^{2d}, \tag{5.26}$$

$$c_2 = \frac{d\gamma^4}{126\ln 2}, \tag{5.27}$$

$$N = \frac{1}{\ln d}\ln\left(\frac{252\ln 2\ln\left(\frac{30}{\gamma^2}\right)}{\gamma^4}\right). \tag{5.28}$$

Proof. From [183, 185] we have for $\lambda_{\max}$ the max eigenvalue of either reduced density matrix of a Haar random state:

$$\mathbb{P}\left(\lambda_{\max} > \frac{1}{d_A} + \frac{\delta}{d_A}\right) \leq \left(\frac{10d_A}{\delta}\right)^{2d_A} \exp\left(-d_B\frac{\delta^2}{14\ln 2}\right), \tag{5.29}$$

where d_A and d_B are the local dimensions across a fixed bipartition. Recall that the maximum Schmidt coefficient is equal to the square root of the maximum eigenvalue. Hence using the relabelling $\frac{1+\delta}{d_A} = \gamma^2 \iff \delta = d_A\gamma^2 - 1$, we can write the above as

$$\mathbb{P}\left(\lambda_{\max} > \gamma^2\right) = \mathbb{P}\left(\gamma_{\max} > \gamma\right) \tag{5.30}$$

$$\leq \left(\frac{10d_A}{d_A\gamma^2 - 1}\right)^{2d_A} \exp\left(-d_B\frac{(d_A\gamma^2-1)^2}{14\ln 2}\right), \tag{5.31}$$

for $\gamma_{\max}$ the maximum Schmidt coefficient across this bipartition.

As we are considering n parties each with local dimension d, set $d_A = d^x$, where $x \leq \frac{n}{2}$, and $d_B = d^{n-x}$. Note also that for $\gamma \geq \frac{\sqrt{3}}{2}$ and $d_A \geq 2$, we have

$$d_A\gamma^2 \geq \frac{3}{2} \qquad \iff \qquad d_A\gamma^2 - 1 \geq \frac{d_A\gamma^2}{3}. \tag{5.32}$$

Hence we can write

$$\mathbb{P}\left(\gamma_{\max} > \gamma\right) \leq \left(\frac{30}{\gamma^2}\right)^{2\cdot d^x} \exp\left(-\frac{d^{n+x}\gamma^4}{126\ln 2}\right) \tag{5.33}$$

$$= \exp(d^x(a - bd^n)), \tag{5.34}$$

for positive constants

$$a = 2\ln\left(\frac{30}{\gamma^2}\right), \qquad b = \frac{\gamma^4}{126\ln 2}. \tag{5.35}$$

For $a - bd^n \leq 0$, the worst case is for $x = 1$ (when d^x is smallest, and $d^x(a - bd^n)$ is largest). So for n sufficiently large we have that

$$\exp(d^x(a - bd^n)) \leq \exp(d(a - bd^n)). \tag{5.36}$$

Taking the union bound over all $2^{n-1} - 1$ nontrivial bipartitions then gives

$$\mathbb{P}\left(\Gamma_{\max} > \gamma\right) \leq 2^{n-1}\exp(d(a - bd^n)) \tag{5.37}$$

$$\equiv c_1 2^n e^{-c_2 d^n}, \tag{5.38}$$

for $\Gamma_{\max}$ the maximum Schmidt coefficient over all bipartitions, and where

$$c_1 = \tfrac{1}{2}e^{da} = \tfrac{1}{2}\left(\frac{30}{\gamma^2}\right)^{2d}, \qquad c_2 = db = \frac{d\gamma^4}{126\ln 2}. \tag{5.39}$$

Finally, observe that we can rewrite the condition $a - bd^n \leq 0$ as

$$n \geq \frac{\ln\left(\frac{a}{b}\right)}{\ln(d)} = \frac{\ln\left(\frac{\ln 2c_1}{c_2}\right)}{\ln(d)} = \frac{1}{\ln d}\ln\left(\frac{252\ln 2\ln\left(\frac{30}{\gamma^2}\right)}{\gamma^4}\right). \tag{5.40}$$

□

5.2.2 Proof of Lemma 5.3

Lemma 5.3. For $0 < \epsilon \leq \frac{1}{2}$, the existence of an ϵ-tester for the property of a multipartite state being bipartite product using k copies implies that

$$D(\rho, \sigma) \;\geq\; \frac{1}{3} - O(2^{-n}), \tag{5.8}$$

for D the trace distance, and where

$$\rho = \frac{\Pi^k_{d^n}}{\binom{d^n+k-1}{k}}, \qquad \sigma = \mathop{\mathbb{E}}_{S\subseteq[n]}\left[\frac{\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{n-|S|}}}{\binom{d^{|S|}+k-1}{k}\binom{d^{n-|S|}+k-1}{k}}\right], \tag{5.9}$$

for Π^k_d the projector onto the symmetric subspace of k systems of local dimension d.

Proof. Suppose there is a tester for the property of being bipartite product (BP) using k copies of the input state. This means that there exists an operator (a POVM element) $M : (\mathbb{C}^d)^{\otimes kn} \rightarrow (\mathbb{C}^d)^{\otimes kn}$ with $0 \leq M \leq \mathbb{1}$, such that for all inputs $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ we have the following.

- If $|\psi\rangle$ is BP then $\mathrm{Tr}(M\ \ |\psi\rangle\langle\psi|^{\otimes k}) \geq \frac{2}{3}$.
- If $|\psi\rangle$ is ϵ-far from being BP then $\mathrm{Tr}(M\ \ |\psi\rangle\langle\psi|^{\otimes k}) \leq \frac{1}{3}$.

This implies that for any $|\psi\rangle$ that is BP, and any $|\phi\rangle$ that is ϵ far from being BP we have

$$\mathrm{Tr}\left(M\left(|\psi\rangle\langle\psi|^{\otimes k} - |\phi\rangle\langle\phi|^{\otimes k}\right)\right) \geq \frac{1}{3}. \tag{5.41}$$

By linearity, this must also hold if we replace the states with averages, respectively according to any distribution $\mathcal{D}_{BP}$ on BP states, and any distribution $\mathcal{D}_F$ on states ϵ-far from being BP. The variational characterisation of the trace distance then also allows us to write

$$\frac{1}{3} \leq \mathrm{Tr}\left(M\left(\mathbb{E}_{\psi\sim\mathcal{D}_{BP}}(|\psi\rangle\langle\psi|^{\otimes k}) - \mathbb{E}_{\phi\sim\mathcal{D}_F}(|\phi\rangle\langle\phi|^{\otimes k})\right)\right), \tag{5.42}$$

$$\leq D\Bigg(\mathbb{E}_{\psi\sim\mathcal{D}_{BP}}(|\psi\rangle\langle\psi|^{\otimes k})\ ,\ \mathbb{E}_{\phi\sim\mathcal{D}_F}(|\phi\rangle\langle\phi|^{\otimes k})\Bigg). \tag{5.43}$$

We will take $\mathcal{D}_{BP}$ as the distribution defined by taking a random non-trivial bipartition of the n parties, and then randomising over pure states on each subsystem using the Haar measure. More concretely, for some subset $S \subseteq [n]$ denote the normalised states

$$\tau_S = \left(\int d\theta\, |\theta\rangle\langle\theta|^{\otimes k}\right) \otimes_S \left(\int d\omega\, |\omega\rangle\langle\omega|^{\otimes k}\right) \tag{5.44}$$

$$= \frac{\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{n-|S|}}}{\binom{d^{|S|}+k-1}{k}\binom{d^{n-|S|}+k-1}{k}}, \tag{5.45}$$

where Π_d^k is the projector onto the symmetric subspace – see Eq. (1.92) and Eq. (1.93).

Define $\sigma := \mathbb{E}_{S\subseteq[n]}\Big[\tau_S\Big]$, and as a distribution over BP states we will take

$$\sigma' := \mathbb{E}_{\psi\sim\mathcal{D}_{BP}}(|\psi\rangle\langle\psi|^{\otimes k}) = \mathop{\mathbb{E}}_{\substack{S\subseteq[n]\\ S\neq\emptyset,[n]}}\Big[\tau_S\Big]. \tag{5.46}$$

These states are $O(2^{-n})$ close in trace distance, as seen by the following calculation (using the triangle inequality).

$$\left\|\mathop{\mathbb{E}}_{S\subseteq[n]}\Big[\tau_S\Big] - \mathop{\mathbb{E}}_{\substack{S\subseteq[n]\\ S\neq\emptyset,[n]}}\Big[\tau_S\Big]\right\|_1 = \left\|\frac{1}{2^n}\left(\tau_\emptyset + \tau_{[n]}\right) + \left(\frac{1}{2^n} - \frac{1}{2^n-2}\right)\sum_{\substack{S\subseteq[n]\\ S\neq\emptyset,[n]}} \tau_S\right\|_1 \tag{5.47}$$

$$\leq \frac{1}{2^n}\left(\|\tau_\emptyset\|_1 + \left\|\tau_{[n]}\right\|_1\right) + \left|\frac{1}{2^n} - \frac{1}{2^n-2}\right| \sum_{\substack{S\subseteq[n]\\ S\neq\emptyset,[n]}} \|\tau_S\|_1 \tag{5.48}$$

$$= \frac{1}{2^{n-1}} + (2^n-2)\left|\frac{1}{2^n} - \frac{1}{2^n-2}\right| \tag{5.49}$$

$$= \frac{1}{2^{n-2}}. \tag{5.50}$$

Now define $\mathcal{D}_F$ to be the Haar measure conditioned on the maximum Schmidt coefficient over all bipartitions being at most $\gamma = \sqrt{1-\epsilon^2}$. This guarantees that the output is at least ϵ-far in trace distance from being BP by the following facts, with proof in Section 5.4.1.

Fact 5.6.

(i) The maximum Schmidt coefficient $\gamma_{\max}$ of a bipartite state $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is equal to

$$\max_{\substack{|\alpha\rangle \in \mathbb{C}^{d_1} \\ |\beta\rangle \in \mathbb{C}^{d_2}}} |\langle\psi| \ |\alpha\rangle\,|\beta\rangle|. \tag{5.51}$$

(ii) If a multipartite state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ has max Schmidt coefficient at most γ across any nontrivial bipartition, then it must be at least ϵ-far in trace distance from any bipartite product state, for $\epsilon = \sqrt{1-\gamma^2}$.

We also require the following fact, which intuitively states that if two distributions only disagree on a subset that occurs with small probability, then the distributions themselves will be close. We give proof in Section 5.4.2.

Fact 5.7. Let H denote the Haar distribution, and H_s be the Haar distribution conditioned on states belonging to some measurable set S. Let p be the probability that a Haar random state does not belong to S, i.e. $p = 1 - \int_S d\psi$. Define the states

$$\rho = \mathbb{E}_{\psi\sim H}(|\psi\rangle\!\langle\psi|^{\otimes k}), \tag{5.52}$$

$$\rho' = \mathbb{E}_{\phi\sim H_S}(|\phi\rangle\!\langle\phi|^{\otimes k}). \tag{5.53}$$

Then the trace distance between these states is at most p:

$$D(\rho,\rho') \leq p. \tag{5.54}$$

Now take S as the set of states with maximum Schmidt coefficient at most γ. By Lemma 5.5, for $\frac{\sqrt{3}}{2} \leq \gamma \leq 1$ the probability that a Haar random state has maximum Schmidt coefficient greater than γ is at most $c_1 2^n e^{-c_2 d^n}$, where c_1 and c_2 are given in Lemma 5.5. Hence by Fact 5.7 the trace distance between the following states

$$\rho = \mathbb{E}_{\psi\sim H}(|\psi\rangle\!\langle\psi|^{\otimes k}) \tag{5.55}$$

$$\rho' = \mathbb{E}_{\phi\sim H_S}(|\phi\rangle\!\langle\phi|^{\otimes k}) \tag{5.56}$$

is at most $c_1 2^n e^{-c_2 2^n}$. Finally, Fact 5.6 tells us that if $|\psi\rangle$ has maximum Schmidt coefficient at most γ across any bipartition, then it is $\epsilon = \sqrt{1-\gamma^2}$ far in trace distance from any BP state. The condition $\frac{\sqrt{3}}{2} \leq \gamma \leq 1$ is equivalent to $0 \leq \epsilon \leq \frac{1}{2}$.

Thus in summary, by two applications of the triangle inequality the existence of an ϵ-tester for bipartite productness, for $0 < \epsilon \leq \frac{1}{2}$, implies that

$$\begin{aligned} \frac{1}{3} &\leq D(\rho', \sigma') && (5.57)\\ &\leq D(\sigma, \sigma') + D(\rho, \rho') + D(\rho, \sigma) && (5.58)\\ &\leq O(2^{-n}) + O(2^n e^{-cd^n}) + D(\rho, \sigma) && (5.59)\\ &\leq O(2^{-n}) + D(\rho, \sigma), && (5.60)\end{aligned}$$

for $c > 0$ a constant and where

$$\rho = \frac{\Pi^k_{d^n}}{\binom{d^n+k-1}{k}}, \qquad \sigma = \mathop{\mathbb{E}}_{S\subseteq[n]} \left[\frac{\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{n-|S|}}}{\binom{d^{|S|}+k-1}{k}\binom{d^{n-|S|}+k-1}{k}} \right]. \tag{5.61}$$

□

5.2.3 Proof of Lemma 5.4

Lemma 5.4. Consider the following states

$$\rho = \frac{\Pi^k_{d^n}}{\binom{d^n+k-1}{k}}, \qquad \sigma = \mathop{\mathbb{E}}_{S\subseteq[n]} \left[\frac{\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{n-|S|}}}{\binom{d^{|S|}+k-1}{k}\binom{d^{n-|S|}+k-1}{k}} \right], \tag{5.10}$$

where Π^k_d denotes the projector onto the symmetric subspace of k systems of local dimension d. Then their squared trace-distance is upper bounded by the following expression:

$$D(\rho, \sigma)^2 \leq \frac{k!}{4}\left(1 + (k!)^3 \left(\frac{1+d}{2d}\right)^n - e^{-k^2/d^n}\right). \tag{5.11}$$

Proof. First, we can use the following standard inequality to replace the 1-norm with the 2-norm, for any matrix $A \in \mathbb{C}^{d\times d}$

$$\|A\|_1 \leq \sqrt{d}\|A\|_2, \tag{5.62}$$

where $\|A\|_p := \mathrm{Tr}\left(|A|^p\right)^{\frac{1}{p}}$. So we have

$$\begin{aligned} D(\rho, \sigma)^2 &= \frac{1}{4}\|\rho - \sigma\|_1^2 && (5.63)\\ &\leq \frac{d^{nk}}{4}\|\rho - \sigma\|_2^2 = \frac{d^{nk}}{4}\mathrm{Tr}\left((\rho-\sigma)^2\right) && (5.64)\\ &= \frac{d^{nk}}{4}\Big(\mathrm{Tr}(\rho^2) + \mathrm{Tr}(\sigma^2) - 2\mathrm{Tr}(\rho\sigma)\Big). && (5.65)\end{aligned}$$

To calculate $\mathrm{Tr}(\rho\sigma)$, we will now use the fact that

$$\mathrm{Sym}^k_{d_1} \otimes \mathrm{Sym}^k_{d_2} \subseteq \mathrm{Sym}^k_{d_1 d_2}. \tag{5.66}$$

To see this, take a state $|\psi\rangle \in \mathrm{Sym}^k_{d_1} \otimes \mathrm{Sym}^k_{d_2}$. Then by definition it is preserved under $U_\alpha \otimes U_\beta$ $\forall \alpha, \beta \in \mathcal{S}_k$. In particular, it is preserved when $\alpha = \beta$, and we have $U_\alpha \otimes U_\alpha = U'_\alpha$, where U'_α acts on the whole space. So $|\psi\rangle$ is in $\mathrm{Sym}^k_{d_1 d_2}$ – see also Fig. 5.1 for a visual aid. This implies the following relationship between the projectors onto these spaces

$$\Pi^k_{d_1 d_2} \cdot \left(\Pi^k_{d_1} \otimes \Pi^k_{d_2}\right) = \Pi^k_{d_1} \otimes \Pi^k_{d_2}. \tag{5.67}$$

Hence we have

$$\begin{aligned}
\mathrm{Tr}(\rho\sigma) &= \mathop{\mathbb{E}}_{S}\left[\frac{\mathrm{Tr}\left(\Pi^k_{d^n} \cdot \Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{n-|S|}}\right)}{\binom{d^n+k-1}{k}\binom{d^{|S|}+k-1}{k}\binom{d^{n-|S|}+k-1}{k}}\right] && (5.68)\\
&= \frac{1}{\binom{d^n+k-1}{k}} \mathop{\mathbb{E}}_{S}\left[\frac{\mathrm{Tr}\left(\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{n-|S|}}\right)}{\binom{d^{|S|}+k-1}{k}\binom{d^{n-|S|}+k-1}{k}}\right] && (5.69)\\
&= \frac{1}{\binom{d^n+k-1}{k}} = \mathrm{Tr}(\rho^2). && (5.70)
\end{aligned}$$

So altogether at this stage we have

$$\begin{aligned}
D^2 &\leq \frac{d^{nk}}{4}\Big(\mathrm{Tr}(\rho^2) + \mathrm{Tr}(\sigma^2) - 2\mathrm{Tr}(\rho\sigma)\Big) && (5.71)\\
&= \frac{d^{nk}}{4}\Big(\mathrm{Tr}(\sigma^2) - \mathrm{Tr}(\rho^2)\Big). && (5.72)
\end{aligned}$$

We will now use the following fact to bound $\mathrm{Tr}(\rho^2)$ and $\mathrm{Tr}(\sigma^2)$, deferring the proof to Section 5.4.3.

Fact 5.8. For all $a, b \in \mathbb{N}$ we have

$$\frac{a^b}{b!} \leq \binom{a+b-1}{b} \leq \frac{a^b}{b!}\, e^{b^2/a}. \tag{5.73}$$

We can use this to bound $\mathrm{Tr}(\rho^2)$ as follows.

$$\mathrm{Tr}(\rho^2) = \frac{1}{\binom{d^n+k-1}{k}} \geq \frac{k!}{e^{k^2/d^n} d^{nk}}. \tag{5.74}$$

To bound $\mathrm{Tr}(\sigma^2)$, we can again employ Fact 5.8 to obtain

$$\frac{1}{\binom{d^{|S|}+k-1}{k}} \leq \frac{k!}{d^{|S|k}}, \tag{5.75}$$

so that

$$\begin{aligned}
\mathrm{Tr}(\sigma^2) &= \mathrm{Tr}\left(\underset{S,T\subseteq[n]}{\mathbb{E}} \left[\frac{\left(\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{|S^c|}}\right) \left(\Pi^k_{d^{|T|}} \otimes_T \Pi^k_{d^{|T^c|}}\right)}{\binom{d^{|S|}+k-1}{k}\binom{d^{|S^c|}+k-1}{k}\binom{d^{|T|}+k-1}{k}\binom{d^{|T^c|}+k-1}{k}} \right] \right) && (5.76)\\
&\leq \frac{(k!)^4}{d^{2nk}}\ F(k,n,d), && (5.77)
\end{aligned}$$

using $|S| + |S^c| + |T| + |T^c| = 2n$ and where we define

$$F \equiv F(k,n,d) = \mathrm{Tr}\left(\underset{S,T\subseteq[n]}{\mathbb{E}} \left[\left(\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{|S^c|}}\right) \left(\Pi^k_{d^{|T|}} \otimes_T \Pi^k_{d^{|T^c|}}\right)\right] \right). \qquad (5.78)$$

Hence at this stage we have

$$\begin{aligned}
D^2 &\leq \frac{d^{nk}}{4}\Big(\mathrm{Tr}(\sigma^2) - \mathrm{Tr}(\rho^2)\Big) && (5.79)\\
&\leq \frac{d^{nk}}{4}\left(F\cdot\frac{(k!)^4}{d^{2nk}} - \frac{k!}{e^{k^2/d^n}d^{nk}}\right) && (5.80)\\
&= \frac{k!}{4}\left(F\cdot\frac{(k!)^3}{d^{nk}} - e^{-k^2/d^n}\right). && (5.81)
\end{aligned}$$

We now seek an upper bound on F. Recall that

$$\Pi^k_d = \underset{\alpha\in\mathcal{S}_k}{\mathbb{E}}\left[U_\alpha\right], \qquad (5.82)$$

where

$$U_\alpha = \sum_{\mathbf{x}\in[d]^k} \left|x_{\alpha^{-1}(1)}, ..., x_{\alpha^{-1}(k)}\middle\rangle\!\middle\langle x_1, ..., x_k\right|. \qquad (5.83)$$

We can thus write

$$\begin{aligned}
F &= \mathrm{Tr}\Big(\underset{S,T}{\mathbb{E}} \Big[\left(\Pi^k_{d^{|S|}} \otimes_S \Pi^k_{d^{|S^c|}}\right) \left(\Pi^k_{d^{|T|}} \otimes_T \Pi^k_{d^{|T^c|}}\right)\Big]\Big) && (5.84)\\
&= \underset{\substack{S,T\subseteq[n]\\ \alpha,\beta,\gamma,\delta\in\mathcal{S}_k}}{\mathbb{E}} \left[\mathrm{Tr}\left(\left(U^S_\alpha \otimes_S U^{S^c}_\beta\right)\left(U^T_\gamma \otimes_T U^{T^c}_\delta\right)\right)\right] && (5.85)\\
&= \underset{\substack{S,T\\ \alpha,\beta,\gamma,\delta}}{\mathbb{E}} \left[\mathrm{Tr}\Big(U^{S\cap T}_{\alpha\gamma} \otimes U^{S\cap T^c}_{\alpha\delta} \ \otimes\ U^{S^c\cap T}_{\beta\gamma} \ \otimes\ U^{S^c\cap T^c}_{\beta\delta}\Big)\right] && (5.86)\\
&= \underset{\substack{S,T\\ \alpha,\beta,\gamma,\delta}}{\mathbb{E}} \left[\mathrm{Tr}\Big(U^{S\cap T}_{\alpha\gamma}\Big)\ \mathrm{Tr}\Big(U^{S\cap T^c}_{\alpha\delta}\Big)\ \mathrm{Tr}\Big(U^{S^c\cap T}_{\beta\gamma}\Big)\ \mathrm{Tr}\Big(U^{S^c\cap T^c}_{\beta\delta}\Big)\right], && (5.87)
\end{aligned}$$

where the superscripts denote the systems that the unitaries act on.

We now use the following fact, giving proof in Section 5.4.4.

Fact 5.9. For some permutation $\alpha \in \mathcal{S}_k$, consider the unitary

$$U_\alpha = \sum_{\mathbf{x}\in[d]^k} \left|x_{\alpha^{-1}(1)}, \dots, x_{\alpha^{-1}(k)}\middle\rangle\!\middle\langle x_1, \dots, x_k\right|. \tag{5.88}$$

Let $c(\alpha)$ be the number of cycles in the permutation α. Then we have

$$\operatorname{Tr}(U_\alpha) = d^{c(\alpha)}. \tag{5.89}$$

Hence we can write

$$\begin{aligned} F &= \mathop{\mathbb{E}}_{\substack{S,T\\ \alpha,\beta,\gamma,\delta}} \left[\operatorname{Tr}\left(U_{\alpha\gamma}^{S\cap T}\right) \operatorname{Tr}\left(U_{\alpha\delta}^{S\cap T^c}\right) \operatorname{Tr}\left(U_{\beta\gamma}^{S^c\cap T}\right) \operatorname{Tr}\left(U_{\beta\delta}^{S^c\cap T^c}\right)\right] && (5.90)\\ &= \mathop{\mathbb{E}}_{\substack{S,T\\ \alpha,\beta,\gamma,\delta}} \left[d^{|S\cap T|c(\alpha\gamma)+|S\cap T^c|c(\alpha\delta)+|S^c\cap T|c(\beta\gamma)+|S^c\cap T^c|c(\beta\delta)}\right]. && (5.91) \end{aligned}$$

We can simply this expression slightly and eliminate one of the sums over $\mathcal{S}_k$ as follows. First we use the substitutions relabelling $\delta' = \beta\delta$ and $\gamma' = \beta\gamma$:

$$F = \mathop{\mathbb{E}}_{\substack{S,T\\ \alpha,\beta,\gamma',\delta'}} \left[d^{|S\cap T|c(\alpha\beta^{-1}\gamma')+|S\cap T^c|c(\alpha\beta^{-1}\delta')+|S^c\cap T|c(\gamma')+|S^c\cap T^c|c(\delta')}\right]. \tag{5.92}$$

Next we can define $\alpha' = \alpha\beta^{-1}\delta'$, followed by $\delta'' = \delta^{-1}$ to get

$$\begin{aligned} F &= \mathop{\mathbb{E}}_{\substack{S,T\\ \alpha',\beta,\gamma',\delta'}} \left[d^{|S\cap T|c(\alpha\delta'^{-1}\gamma')+|S\cap T^c|c(\alpha')+|S^c\cap T|c(\gamma')+|S^c\cap T^c|c(\delta')}\right] && (5.93)\\ &= \mathop{\mathbb{E}}_{\substack{S,T\\ \alpha',\gamma',\delta''}} \left[d^{|S\cap T|c(\alpha\delta''\gamma')+|S\cap T^c|c(\alpha')+|S^c\cap T|c(\gamma')+|S^c\cap T^c|c(\delta''^{-1})}\right]. && (5.94) \end{aligned}$$

Finally, we can use the fact that the cycle number is preserved under inverses, i.e. $c(\delta^{-1}) = c(\delta)$, and perform a global relabelling to arrive at

$$F = \mathop{\mathbb{E}}_{\substack{S,T\\ \alpha,\gamma,\delta}} \left[d^{|S\cap T|c(\alpha\delta\gamma)+|S\cap T^c|c(\alpha)+|S^c\cap T|c(\gamma)+|S^c\cap T^c|c(\delta)}\right]. \tag{5.95}$$

We can now separate out the case where α, δ, γ are all the identity permutation $e \in \mathcal{S}_k$, so here the cycle length is k.

$$\begin{aligned}
F &= \mathop{\mathbb{E}}_{\substack{S,T\\ \alpha,\gamma,\delta}} \left[d^{|S\cap T|c(\alpha\delta\gamma)+|S\cap T^c|c(\alpha)+|S^c\cap T|c(\gamma)+|S^c\cap T^c|c(\delta)} \right] && (5.96)\\
&= \tfrac{1}{(k!)^3} \mathop{\mathbb{E}}_{S,T} \left[d^{k(|S\cap T|+|S\cap T^c|+|S^c\cap T|+|S^c\cap T^c|)} \right] && (5.97)\\
&\quad + \tfrac{(k!)^3-1}{(k!)^3} \mathop{\mathbb{E}}_{\substack{S,T\\ \alpha,\delta,\gamma\in\mathcal{S}_k\\ (\alpha,\delta,\gamma)\neq(e,e,e)}} \left[d^{|S\cap T|c(\alpha\delta\gamma)+|S\cap T^c|c(\alpha)+|S^c\cap T|c(\gamma)+|S^c\cap T^c|c(\delta)} \right] && (5.98)\\
&\leq \frac{d^{nk}}{(k!)^3} + \mathop{\mathbb{E}}_{\substack{S,T\\ \alpha,\delta,\gamma\in\mathcal{S}_k\\ (\alpha,\delta,\gamma)\neq(e,e,e)}} \left[d^{|S\cap T|c(\alpha\delta\gamma)+|S\cap T^c|c(\alpha)+|S^c\cap T|c(\gamma)+|S^c\cap T^c|c(\delta)} \right]. && (5.99)
\end{aligned}$$

Now the next biggest term within the expectation (after the case of α, δ, γ all equal to the identity) will be when exactly one of α, δ, γ is equal to a single SWAP and identity on the rest. In this case, we can take without loss of generality $c(\alpha) = k - 1$, $c(\delta) = c(\gamma) = k$ and $c(\alpha\delta\gamma) = k - 1$. Thus

$$\begin{aligned}
F &\leq \frac{d^{nk}}{(k!)^3} + \mathop{\mathbb{E}}_{S,T} \left[d^{|S\cap T|(k-1)+|S\cap T^c|(k-1)+|S^c\cap T|k+|S^c\cap T^c|k} \right] && (5.100)\\
&= \frac{d^{nk}}{(k!)^3} + d^{(k-1)n} \mathop{\mathbb{E}}_{S,T} \left[d^{|S^c\cap T|+|S^c\cap T^c|} \right]. && (5.101)
\end{aligned}$$

Now observe that

$$\begin{aligned}
\mathop{\mathbb{E}}_{S,T} \left[d^{|S^c\cap T|+|S^c\cap T^c|} \right] &= \mathop{\mathbb{E}}_{S} \left[d^{|S^c|} \right] = \mathop{\mathbb{E}}_{S} \left[d^{|S|} \right] && (5.102)\\
&= \frac{1}{2^n} \sum_{s=0}^{n} \binom{n}{s} d^s && (5.103)\\
&= \left(\frac{1+d}{2} \right)^n. && (5.104)
\end{aligned}$$

So we have shown that

$$\begin{aligned}
F &\leq \frac{d^{nk}}{(k!)^3} + d^{(k-1)n} \left(\frac{1+d}{2} \right)^n && (5.105)\\
&= \frac{d^{nk}}{(k!)^3} + d^{nk} \left(\frac{1+d}{2d} \right)^n. && (5.106)
\end{aligned}$$

Bringing this all together and plugging in our bound on F into Eq. (5.81), we have

$$\begin{aligned}
D^2 &\leq \frac{k!}{4} \left(F \cdot \frac{(k!)^3}{d^{nk}} - e^{-k^2/d^n} \right) && (5.107)\\
&\leq \frac{k!}{4} \left(1 + (k!)^3 \left(\frac{1+d}{2d} \right)^n - e^{-k^2/d^n} \right), && (5.108)
\end{aligned}$$

as claimed.

□

5.3 Concluding remarks

We have demonstrated that testing bipartite productness requires at least $\Omega(n/\log n)$ copies, which matches the upper bound of $O(n)$ from [176] up to a logarithmic factor. As discussed in the introduction, this also implies that computing the generalised geometric measure of entanglement for multipartite states requires $\Omega(n/\log n)$ copies in general. Another implication is that if one wishes to test the property of some graph state corresponding to a non-connected graph using less than $\Omega(n/\log n)$ copies, one would need a different approach to that of simply testing for bipartite productness.

In would be interesting to see if our bound could be further tightened to $\Omega(n)$ to match the known upper bound more closely, although we believe alternative proof techniques would be needed. One could also study the dependence on ϵ in more depth – in our techniques this dependence appears via Lemma 5.5 and Fact 5.6 in combination, however as we take n to infinity the relevant term in Lemma 5.3 tends to zero for all ϵ.

Another compelling avenue would be to examine the complementary property of being genuine multipartite entangled, which to the best of our knowledge has not yet been studied. Clearly one cannot directly test for this in the property testing framework, as any bipartite product state can be arbitrarily close to a GME state in trace distance, e.g by slight perturbations of the state. However, one could consider the property of being maximally multipartite entangled according to some measure, such as the generalised geometric measure discussed in this chapter.

5.4 Proofs of supporting facts

5.4.1 Proof of Fact 5.6

Fact 5.6.

(i) The maximum Schmidt coefficient $\gamma_{\max}$ of a bipartite state $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is equal to

$$\max_{\substack{|\alpha\rangle\in\mathbb{C}^{d_1}\\ |\beta\rangle\in\mathbb{C}^{d_2}}} |\langle\psi| \; |\alpha\rangle\,|\beta\rangle|. \tag{5.51}$$

(ii) If a multipartite state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ has max Schmidt coefficient at most γ across any nontrivial bipartition, then it must be at least ϵ-far in trace distance from any bipartite product state, for $\epsilon = \sqrt{1-\gamma^2}$.

Proof.

(i) Write $|\psi\rangle = \sum_i \gamma_i |u_i\rangle |v_i\rangle$ in Schmidt decomposition, with $|u_i\rangle$ and $|v_i\rangle$ respectively orthonormal sets and γ_i non-negative and non-increasing with i. Denote $\gamma_{\max} \equiv \gamma_0$ as the maximum Schmidt coefficient. Clearly taking $|\alpha\rangle = |u_0\rangle$ and $|\beta\rangle = |v_0\rangle$ shows that

$$\gamma_{\max} \leq \max_{\alpha,\beta} |\langle\psi| \ |\alpha\rangle |\beta\rangle|. \tag{5.109}$$

We also have that

$$\begin{aligned} \max_{\alpha,\beta} |\langle\psi| \ |\alpha\rangle |\beta\rangle| &\leq \sum \gamma_i |\langle\alpha|u_i\rangle \langle\beta|v_i\rangle| && (5.110) \\ &\leq \gamma_{\max} \sum |\langle\alpha|u_i\rangle \langle\beta|v_i\rangle| && (5.111) \\ &\leq \gamma_{\max} \sqrt{\sum_i |\langle\alpha|u_i\rangle|^2 \sum_j |\langle\beta|v_j\rangle|^2} && (5.112) \\ &= \gamma_{\max}, && (5.113) \end{aligned}$$

where we used the Triangle and Cauchy-Schwarz inequalities.

(ii) Recall the well known relation between trace distance and fidelity for pure states

$$\tfrac{1}{2} \| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_1 = \sqrt{1 - |\langle\psi|\phi\rangle|^2}. \tag{5.114}$$

Now let $|\phi\rangle = |\alpha\rangle |\beta\rangle$ be a BP state (written across some bipartition). Then

$$\tfrac{1}{2} \| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_1 = \sqrt{1 - |\langle\psi| \ |\alpha\rangle |\beta\rangle|^2} \geq \sqrt{1 - \gamma^2}, \tag{5.115}$$

where the last inequality follows from part (i).

□

5.4.2 Proof of Fact 5.7

Fact 5.7. Let H denote the Haar distribution, and H_s be the Haar distribution conditioned on states belonging to some measurable set S. Let p be the probability that a Haar random state does not belong to S, i.e. $p = 1 - \int_S d\psi$. Define the states

$$\begin{aligned} \rho &= \mathbb{E}_{\psi\sim H}(|\psi\rangle\langle\psi|^{\otimes k}), && (5.52) \\ \rho' &= \mathbb{E}_{\phi\sim H_S}(|\phi\rangle\langle\phi|^{\otimes k}). && (5.53) \end{aligned}$$

Then the trace distance between these states is at most p:

$$D(\rho, \rho') \leq p. \tag{5.54}$$

Proof. We can write

$$\rho' = \frac{1}{1-p}\int d\phi \;\; |\phi\rangle\langle\phi|^{\otimes k}\,\mathbf{1}_S(\phi), \tag{5.116}$$

where $\mathbf{1}_S(\phi) = 1$ if $|\phi\rangle \in S$ and 0 otherwise (the indicator function), and p is a normalisation factor enforcing $\mathrm{Tr}(\rho) = 1$. Then we have

$$\begin{aligned}
\|\rho - \rho'\|_1 &= \left\|\int d\psi \;\; |\psi\rangle\langle\psi|^{\otimes k}\left(\mathbb{1} - \frac{1}{1-p}\mathbf{1}_S\right)\right\|_1 && (5.117)\\
&\leq \int d\psi \;\left\||\psi\rangle\langle\psi|^{\otimes k}\right\|_1\left|1 - \frac{1}{1-p}\mathbf{1}_S\right| && (5.118)\\
&= \int d\psi \;\left|1 - \frac{1}{1-p}\mathbf{1}_S\right| && (5.119)\\
&= \int_S d\psi \;\left(\frac{1}{1-p} - 1\right) + \int_{S^c} d\psi && (5.120)\\
&= (1-p)\left(\frac{1}{1-p} - 1\right) + p && (5.121)\\
&= 2p. && (5.122)
\end{aligned}$$

□

5.4.3 Proof of Fact 5.8

Fact 5.8. For all $a, b \in \mathbb{N}$ we have

$$\frac{a^b}{b!} \leq \binom{a+b-1}{b} \leq \frac{a^b}{b!}\; e^{b^2/a}. \tag{5.73}$$

Proof. Firstly, we have

$$\begin{aligned}
\binom{a+b-1}{b} &= \frac{(a+b-1)!}{b!(a-1)!} && (5.123)\\
&= \frac{(a+b-1)\;\ldots\;(a)}{b!} && (5.124)\\
&\geq \frac{a^b}{b!}. && (5.125)
\end{aligned}$$

For the upper bound, observe that

$$\begin{aligned}\binom{a+b-1}{b} &= \frac{(a+b-1)!}{b!(a-1)!} && (5.126)\\ &= \frac{(a+b-1)\ \dots\ (a)}{b!} && (5.127)\\ &\leq \frac{(a+b-1)^b}{b!} && (5.128)\\ &\leq \frac{a^b}{b!}(1+\frac{b}{a})^b && (5.129)\\ &\leq \frac{a^b}{b!}e^{b^2/a}, && (5.130)\end{aligned}$$

where in the last line we used that $1 + x \leq e^x$ for all real x. □

5.4.4 Proof of Fact 5.9

Fact 5.9. For some permutation $\alpha \in \mathcal{S}_k$, consider the unitary

$$U_\alpha = \sum_{\mathbf{x}\in[d]^k} \left|x_{\alpha^{-1}(1)}, ..., x_{\alpha^{-1}(k)}\middle\rangle\middle\langle x_1, ..., x_k\right|. \tag{5.88}$$

Let $c(\alpha)$ be the number of cycles in the permutation α. Then we have

$$\mathrm{Tr}\left(U_\alpha\right) = d^{c(\alpha)}. \tag{5.89}$$

Proof. The trace of a permutation matrix is the number of fixed points. First consider if there is only one cycle. Then there are d fixed points, occurring exactly when $x_1 = \cdots = x_k$. Now suppose α has m cycles, and write it in cycle decomposition as

$$\alpha = c_1 \dots c_m. \tag{5.131}$$

As these cycles act on independent copies of the system, we can write

$$U_\alpha = U_{c_1} \otimes \cdots \otimes U_{c_m}, \tag{5.132}$$

from which it follows that

$$\begin{aligned}\mathrm{Tr}(U_\alpha) &= \mathrm{Tr}(U_{c_1})\dots\mathrm{Tr}(U_{c_m}) && (5.133)\\ &= d \times \cdots \times d && (5.134)\\ &= d^m. && (5.135)\end{aligned}$$

□

5.5 Acknowledgements and contributions

This work began around May 2023. Myself and Ashley Montanaro first became interested in studying graph states, and how one could test properties of the underlying graph whilst only using a few copies of a given graph state. This lead us to consider multipartite entanglement more generally, and Ashley suggested a route to proving a lower bound on testing bipartite productness. After several weeks at the whiteboard working through the details, we became convinced of the correctness of our result, and I am now in the process of finalising the paper.

I would like to thank Ashley for undertaking this project with me and for all I that I have learnt throughout the process.

Chapter 6

Conclusions

In this thesis, we have considered several quantum resources, including quantum steering, measurement incompatibility, coherence, and entanglement. We have introduced and explored a number of novel ideas, such as steering in networks, high-dimensional measurement incompatibility, coherence in gadget-based quantum computation, and property testing of non genuinely multipartite entangled states.

Before detailing some concrete research questions that came out of these works, we first briefly comment on the field of quantum information in general. As alluded to in the introduction, two driving questions can be posed as:

(1) Why is quantum mechanics *weird*?

(2) How can this weirdness be *useful*?

Firstly, it is of high value to continue deepening our understanding of quantum properties and resources, and exactly where the quantum-classical boundary lies. When are we witnessing genuinely quantum behaviour? How can we be convinced that some phenomena cannot be explained classically? For which tasks can we expect a quantum advantage? Continued work in the foundational aspects of this field is required to reach a more complete answer to these questions. For example, deepening our understanding of fundamental properties of entanglement and nonlocality, understanding the relationship between quantum and classical complexity classes, or exploring operational interpretations of information theoretic quantities. One of the most exciting aspects of the field of quantum information is that it is a combination of many different ideas and concepts. There is surely much to be gained by combining seemingly distinct notions and exploring novel fundamental concepts: indeed the intersection of ideas from computer science and quantum mechanics is at the heart of the whole field.

Secondly, there is a great push presently to find relevant applications of quantum technologies in society, and several startup companies now exist with venture capital funding. The development of quantum computers would provide huge benefits both for continued fundamental research, as well as their potential to provide computational insights to genuinely useful problems, such as in material modelling. With the advent of several recent quantum computational supremacy claims, it is an exciting time as quantum computers are now reaching the point of being able to genuinely outperform classical computers for certain tasks. It is important for us to be seriously exploring how these new technologies can provide benefit to industry, whilst being responsible regarding the dangers of over-hype.

Let us now summarise the key ideas and questions appearing in each chapter.

Chapter 2: Network quantum steering

Main contributions

- We introduced a new definition of quantum steering for networks.
- We provided no-go results of when network steering is not possible, in terms of properties of the sources in the network.
- We gave concrete examples of network steering, including a form of activation using unsteerable states.

Open questions

Measurement incompatibility in quantum networks.

As discussed in Chapter 2, it is possible to exhibit quantum nonlocality (and steering) in networks even when the parties perform fixed measurements. It is well understood that in the standard Bell nonlocality setting, measurement incompatibility is necessary in order to observe nonlocal correlations. So how does this property manifest itself when only a single measurement is performed? Conceptually one can imagine that a set of incompatible measurements is being performed, conditioned on the value of one of the sources. However we have shown that network steering is achievable when the parties perform fixed Bell-type measurements, in which case it is not at all clear how measurement incompatibility might be at play here – perhaps there is a completely different measurement resource that is the relevant one.

Classifying NLHS models.

Another research question that emerged from the project on network steering is that of determining when properties of the sources (e.g. separable, unsteerable, local) can allow us to immediately conclude a local hidden state model exists. We examined several basic cases, however there are several cases left unknown, for example the case of five parties sharing respective sources that are separable, local, local, and separable. It would be interesting to either show that in such a case one always arrives at a NLHS model, or find an example for which quantum steering can arise – in either case the goal would be to find a tight characterisation of such scenarios.

Chapter 3: High dimensional measurement incompatibility

Main contributions

- We introduced a new definition of high-dimensional measurement incompatibility for a set of measurement, which can also be seen as a form of compression.
- We showed that this definition is mathematically equivalent to high-dimensional quantum steering.
- We introduced n-partially incompatibility breaking channels and characterised their Choi states.

Open questions

Characterisation of quantum channels with Choi state possessing FDI-SN n.

There exists a concrete correspondence via channel state duality between states of Schmidt number n and n-partially entanglement breaking channels. In our work we also discussed a correspondence between n-partially incompatibility breaking channels, and states for which one can certify a Schmidt number of n in a semi-device independent (steering) scenario. A natural question is then to consider states for which one can certify a Schmidt number of n in a fully-device independent (nonlocality) scenario, and ask if there is some intuitive or operational characterisation of the channels.

Chapter 4: The Hadamard gate cannot be replaced by a resource state in universal quantum computation

Main contributions

- We provided a unified framework from which to consider models of quantum computation that involve free operations acting on some fixed resourceful state.
- We showed 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.

Open questions

Resource theoretic results and quantum computation.

There are several interesting results involving the resources of magic and entanglement:

- It has been shown that in measurement based quantum computation, having too much entanglement renders the overall computation classically simulable [186, 187], and a similar result has been shown for the resource of magic in [188]
- The axiomatic and operational approaches to the resource theory often do not coincide, e.g. for entanglement [189] and magic [190].
- Simulation algorithms that scale with a resource quantifier, e.g. for magic [77].

I have wondered about if these results can be extended to other resources, or even proved in general. For example, several parallels have been made in [139, 140] between the resource theory of magic and that of matchgates. In general, it would be interesting to see how much of the machinery developed for magic also could be applied to matchgates, and also if perhaps there is a more fundamental underlying structure.

Measurement Incompatibility in MBQC

In a similar vein, studying the role of measurement incompatibility in measurement based quantum computation would be an exciting avenue to explore. Specifically, one could consider a general set up in which some entangled resource state $|\Psi\rangle$ is provided, and one can perform adaptive measurements at each site according to some set of measurements $M_{a|x}$. If these measurements are compatible, one would expect that any computation could be simulated classically, as one could instead perform the fixed measurement of the parent POVM at each site. However we know that universal quantum computation is possible even when this set $M_{a|x}$ is simply X and Z measurements [135]. Hence it would be interesting to see if one can quantify the simulability of some measurement based computation in terms of the incompatibility of the allowed measurements $M_{a|x}$. One could try to achieve an analogous result to that in the case of magic introduced in [77].

Tighter bounds and more complete analysis.

Another natural question would be to improve or show optimality of the bounds presented in Chapter 4, and find lower bounds on implementing n Hadamards using k Hadamards, incoherent unitaries, classical control, computational basis measurements, and an arbitrary ancilla.

Quantum control of free operations.

As also discussed in Chapter 4, the resource of coherence has the property that the quantum control of free operations remains free. This is not true for entanglement, as for example a CNOT gate (controlled-X) gate is capable of generating entanglement, and so is not free. Nor is it the case for magic, as a controlled-S gate is non-Clifford despite S being a Clifford gate. Finding another resource theory whose free operations are preserved under quantum control could lead to analogous results as presented in Chapter 4, but with this alternative resource as opposed to coherence.

Trade-offs between unitarity and resource content.

It could also be possible to generalise some of the underlying machinery in Chapter 4 in the following way. If some channel $\rho \mapsto \mathrm{Tr}_2(U\ \rho \otimes \tau\ U^\dagger)$ is close in induced trace distance to a unitary channel $\rho \mapsto V\rho V^\dagger$ for some fixed ancillary state τ and unitaries U and V, then the resource content of V cannot be much higher than that of U.

To gain some intuition for this idea, suppose that the resource content of U is much lower than that of V. Suppose also that the channel $\rho \mapsto \mathrm{Tr}_2(U\ \rho \otimes \tau\ U^\dagger)$ and $\rho \mapsto V\rho V^\dagger$ are close in induced trace distance, which should imply that the resource content of the two channels are similar, for any continuous resource quantifier. As the resource content of U is much less than that of V, the channel $\Lambda(\rho) = \mathrm{Tr}_2(U\ \rho \otimes \tau\ U^\dagger)$ must be using the ancillary state in some way, and hence the unitary U cannot be in product form – one extreme possibility is that the unitary U is simply swapping in the resourceful ancillary state. But then the overall channel would be far from unitary (for example, if U was a swap, then the resultant channel would simply be the constant channel that always prepares τ). However if Λ is far from being unitary, then in particular it cannot be close to V, which would be a contradiction. Hence, this hints at a general trade-off between unitarity and resource content in this scenario. See [160] for some work in this direction.

Relationship between coherence and measurement incompatibility.

Again as raised in Chapter 4, could it be the case that *either* coherence or measurement incompatibility must be present in the operations in order to perform universal quantum computation? Clearly in the circuit model, coherence is the relevant resource here as measurements are typically always taken in the computational basis. However in measurement based quantum computation, the only operations performed are adaptive local measurements, and universal measurement based quantum computation is possible with only X and Z measurements. One could think of the ability to perform the Hadamard gate as being equivalent in some sense to the ability to perform X and Z measurements, in which case perhaps a more helpful perspective is to consider these as two sides of the same underlying resource, which is necessary for computational universality.

Chapter 5: Testing multipartite productness is easier

than testing bipartite productness

Main contributions

- We proved a lower bound on the number of copies required to test the property of not being genuinely multipartite entangled.
- We showed that this also provides a lower bound for a particular method of testing non-connectiveness of a graph underlying a graph state, and on the complexity of computing the geometric measure of entanglement.

Open questions

Testing genuine multipartite entanglement

As highlighted in Chapter 5, studying the complementary property to bipartite productness of genuine multipartite entanglement would be a natural future avenue. For example, how many copies of a state are required to determine if it is locally equivalent to a multipartite GHZ state, or ϵ-far from any such states, given the promise that is one of these cases? It would also be worthwhile attempting to better understand any practical significance of testing multipartite entanglement, for example of it could be of use in characterising graph states experimentally.

6.1 Final remarks

In any kind of explorative research, there are two crucial tasks. The first is of being able to ask the right kind of questions, opening up a novel direction and uncovering a rich landscape of further research directions. The second is of solving and answering such questions. Academia as a whole surely needs both the question-askers and the problem-solvers.

The majority of this thesis arguably falls into the former: Chapters 2, 3 and 4 are primarily introducing novel research directions, whereas Chapter 5 is more focused on performing the technical work of answering a well-defined question (that is, proving a lower bound).

It is my hope that in the field of quantum information in general, the art of posing interesting questions will continue to be celebrated in equal amount to the discovery of solutions to existing problems. There is highly fertile ground in the subfields of quantum foundations, resource theories, quantum measurements, and quantum computation left to explore, and I am confident that future enquiries in these domains will continue to lead to exciting and fruitful discoveries, and ultimately provide technological benefit to society at large.

We thank the reader for their attention. Any comments or questions can be directed to *bdmjones ⟨at⟩ hotmail ⟨dot⟩ co ⟨dot⟩ uk.*

Bibliography

[1] Roland Omnes.
The Interpretation of Quantum Mechanics.
Princeton University Press, 1994.

[2] David Wallace.
The emergent multiverse: Quantum theory according to the Everett interpretation.
Oxford University Press, USA, 2012.

[3] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner.
Bell nonlocality.
Rev. Mod. Phys., 86(2):419–478, Apr 2014.

[4] Claude Elwood Shannon.
A mathematical theory of communication.
The Bell system technical journal, 27(3):379–423, 1948.

[5] John Von Neumann.
Mathematical foundations of quantum mechanics: New edition, volume 53.
Princeton University Press, 2018.

[6] Alexander S Holevo.
Quantum coding theorems.
Russian Mathematical Surveys, 53(6):1295, 1998.

[7] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al.
Advances in quantum cryptography.
Advances in optics and photonics, 12(4):1012–1236, 2020.

[8] William K Wootters and Wojciech H Zurek.
A single quantum cannot be cloned.
Nature, 299(5886):802–803, 1982.

[9] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acin.
Quantum cloning.
Reviews of Modern Physics, 77(4):1225, 2005.

[10] Ashley Montanaro.
Quantum algorithms: an overview.
npj Quantum Information, 2(1):1–8, 2016.

[11] Alexander M Dalzell, Sam McArdle, Mario Berta, Przemyslaw Bienias, Chi-Fang Chen, András Gilyén, Connor T Hann, Michael J Kastoryano, Emil T Khabiboulline, Aleksander Kubica, et al.
Quantum algorithms: A survey of applications and end-to-end complexities.
arXiv preprint arXiv:2310.03011, 2023.

[12] Sam McArdle, Suguru Endo, Alán Aspuru-Guzik, Simon C Benjamin, and Xiao Yuan.
Quantum computational chemistry.
Reviews of Modern Physics, 92(1):015003, 2020.

[13] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al.
Quantum supremacy using a programmable superconducting processor.
Nature, 574(7779):505–510, 2019.

[14] Lars S Madsen, Fabian Laudenbach, Mohsen Falamarzi Askarani, Fabien Rortais, Trevor Vincent, Jacob FF Bulmer, Filippo M Miatto, Leonhard Neuhaus, Lukas G Helt, Matthew J Collins, et al.
Quantum computational advantage with a programmable photonic processor.
Nature, 606(7912):75–81, 2022.

[15] Michelle Mosca and Marco Piani.
Quantum Threat Timeline Report 2023.
Technical report, EvolutionQ Inc, Global Risk Institute, 2022.
Available here.

[16] Benjamin DM Jones, Ivan Šupić, Roope Uola, Nicolas Brunner, and Paul Skrzypczyk.
Network Quantum Steering.
Physical Review Letters, 127(17):170405, 2021.

[17] Benjamin DM Jones, Roope Uola, Thomas Cope, Marie Ioannou, Sébastien Designolle, Pavel Sekatski, and Nicolas Brunner.
Equivalence between simulability of high-dimensional measurements and high-dimensional steering.
Physical Review A, 107(5):052425, 2023.

[18] Marie Ioannou, Pavel Sekatski, Sébastien Designolle, Benjamin DM Jones, Roope Uola, and Nicolas Brunner.
Simulability of high-dimensional quantum measurements.
Physical Review Letters, 129(19):190401, 2022.

[19] Benjamin DM Jones, Paul Skrzypczyk, and Noah Linden.

The Hadamard gate cannot be replaced by a resource state in universal quantum computation.
arXiv preprint arXiv:2312.03515, 2023.

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

[21] Mark M Wilde.
Quantum information theory.
Cambridge University Press, 2013.

[22] John Watrous.
The Theory of Quantum Information.
Cambridge University Press, 2018.

[23] Ronald De Wolf.
Quantum computing: Lecture notes.
arXiv preprint arXiv:1907.09415, 2019.

[24] Michael Walter.
Symmetry and Quantum Information Lecture Notes.
2018.
Available at https://qi.rub.de/qit18/.

[25] Marco Tomamichel.
Quantum information processing with finite resources: mathematical foundations.
Springer, 2015.

[26] Teiko Heinosaari and Mário Ziman.
The mathematical language of quantum theory: from uncertainty to entanglement.
Cambridge University Press, 2011.

[27] Scott Aaronson.
Quantum computing since Democritus.
Cambridge University Press, 2013.

[28] Michael Horodecki, Peter W Shor, and Mary Beth Ruskai.
Entanglement breaking channels.
Reviews in Mathematical Physics, 15(06):629–641, 2003.

[29] Otfried Gühne and Géza Tóth.
Entanglement detection.
Physics Reports, 474(1-6):1–75, 2009.

[30] D Cavalcanti and P Skrzypczyk.
Quantum steering: a review with focus on semidefinite programming.
Rep. Prog. Phys., 80(2):024001, dec 2016.

[31] Roope Uola, Ana C. S. Costa, H. Chau Nguyen, and Otfried Gühne.
Quantum steering.
Rev. Mod. Phys., 92(1):015001, Mar 2020.

[32] 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.

[33] Teiko Heinosaari, Takayuki Miyadera, and Mário Ziman.
An invitation to quantum incompatibility.
Journal of Physics A: Mathematical and Theoretical, 49(12):123001, 2016.

[34] Alexander Streltsov, Gerardo Adesso, and Martin B Plenio.
Colloquium: Quantum coherence as a resource.
Reviews of Modern Physics, 89(4):041003, 2017.

[35] Eric Chitambar and Gilad Gour.
Quantum resource theories.
Reviews of Modern Physics, 91(2):025001, 2019.

[36] Ashley Montanaro and Ronald de Wolf.
A survey of quantum property testing.
arXiv preprint arXiv:1310.2035, 2013.

[37] 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.

[38] 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.

[39] Campbell, Earl T and Terhal, Barbara M and Vuillot, Christophe.
Roads towards fault-tolerant universal quantum computation.
Nature, 549(7671):172–179, 2017.

[40] Reg Allenby.

Linear algebra.
Elsevier, 1995.

[41] Werner H Greub.
Linear algebra, volume 23.
Springer Science & Business Media, 2012.

[42] Gilbert Strang.
Introduction to linear algebra.
SIAM, 2022.

[43] Erwin Schrödinger.
Die gegenwärtige situation in der quantenmechanik.
Naturwissenschaften, 23(50):844–849, 1935.

[44] W Forrest Stinespring.
Positive functions on c*-algebras.
Proceedings of the American Mathematical Society, 6(2):211–216, 1955.

[45] Göran Lindblad.
Completely positive maps and entropy inequalities.
Communications in Mathematical Physics, 40:147–151, 1975.

[46] Man-Duen Choi.
Completely positive linear maps on complex matrices.
Linear algebra and its applications, 10(3):285–290, 1975.

[47] MA Neumark.
On a representation of additive operator set functions.
In *CR (Doklady) Acad. Sci. URSS (NS)*, volume 41, pages 359–361, 1943.

[48] Reinhard F Werner.
Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model.
Physical Review A, 40(8):4277, 1989.

[49] David J Griffiths and Darrell F Schroeter.
Introduction to quantum mechanics.
Cambridge university press, 2018.

[50] Alistair IM Rae and Jim Napolitano.
Quantum mechanics.
CRC Press LLC, 2018.

[51] J. Kiukas, C. Budroni, R. Uola, and J.-P. Pellonpää.
Continuous-variable steering and incompatibility via state-channel duality.
Phys. Rev. A, 96:042331, 2017.

[52] Min Jiang, Shunlong Luo, and Shuangshuang Fu.
Channel-state duality.
Phys. Rev. A, 87:022310, Feb 2013.

[53] Barbara M Terhal and Paweł Horodecki.
Schmidt number for density matrices.
Physical Review A, 61(4):040301, 2000.

[54] Teiko Heinosaari, Jukka Kiukas, Daniel Reitzner, and Jussi Schultz.
Incompatibility breaking quantum channels.
Journal of Physics A: Mathematical and Theoretical, 48(43):435301, 2015.

[55] Valerio Scarani.
Bell nonlocality.
Oxford University Press, 2019.

[56] J. S. Bell.
On the Einstein Podolsky Rosen paradox.
Physics, 1:195–200, Nov 1964.

[57] Boris S Tsirel'son.
Quantum analogues of the bell inequalities. the case of two spatially separated domains.
Journal of Soviet mathematics, 36:557–570, 1987.

[58] Boris S Tsirelson.
Some results and problems on quantum bell-type inequalities.
Hadronic Journal Supplement, 8(4):329–345, 1993.

[59] Boris S Cirel'son.
Quantum generalizations of bell's inequality.
Letters in Mathematical Physics, 4:93–100, 1980.

[60] Valerio Scarani.
The device-independent outlook on quantum physics.
Acta Physica Slovaca, 62(4):347–409, 2012.

[61] Armin Tavakoli, Alejandro Pozas-Kerstjens, Ming-Xing Luo, and Marc-Olivier Renou.
Bell nonlocality in networks, 2021.

[62] Tristan Kraft, Sébastien Designolle, Christina Ritz, Nicolas Brunner, Otfried Gühne, and Marcus Huber.
Quantum entanglement in the triangle network, 2020.

[63] Marc-Olivier Renou, Elisa Bäumer, Sadra Boreiri, Nicolas Brunner, Nicolas Gisin, and Salman Beigi.
Genuine Quantum Nonlocality in the Triangle Network.
Phys. Rev. Lett., 123:140401, Sep 2019.

[64] Matthew F. Pusey.
Negativity and steering: A stronger Peres conjecture.
Phys. Rev. A, 88:032313, Sep 2013.

[65] H. M. Wiseman, S. J. Jones, and A. C. Doherty.
Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox.
Phys. Rev. Lett., 98:140402, Apr 2007.

[66] Joseph Bowles, Tamás Vértesi, Marco Túlio Quintino, and Nicolas Brunner.
One-way Einstein-Podolsky-Rosen Steering.
Phys. Rev. Lett., 112:200402, May 2014.

[67] Erwin Schrödinger.
Discussion of probability relations between separated systems.
In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 31, pages 555–563. Cambridge University Press, 1935.

[68] Yu Xiang, Shuming Cheng, Qihuang Gong, Zbigniew Ficek, and Qiongyi He.
Quantum steering: practical challenges and future directions.
PRX Quantum, 3(3):030102, 2022.

[69] 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.

[70] Jeroen Dehaene and Bart De Moor.
Clifford group, stabilizer states, and linear and quadratic operations over GF(2).
Physical Review A, 68(4):042318, 2003.

[71] Daniel Gottesman.
Stabilizer codes and quantum error correction.
California Institute of Technology, 1997.

[72] Scott Aaronson and Daniel Gottesman.

Improved simulation of stabilizer circuits.
Physical Review A, 70(5):052328, 2004.

[73] Richard Jozsa and Marten Van Den Nest.
Classical simulation complexity of extended Clifford circuits.
Quantum Info. Comput., 14:633–648, may 2014.

[74] Sergey Bravyi and Alexei Kitaev.
Universal quantum computation with ideal Clifford gates and noisy ancillas.
Physical Review A, 71(2):022316, 2005.

[75] Daniel Litinski.
Magic state distillation: Not as costly as you think.
Quantum, 3:205, 2019.

[76] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki.
Quantum entanglement.
Reviews of Modern Physics, 81(2):865, 2009.

[77] 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.

[78] James R Seddon and Earl T Campbell.
Quantifying magic for multi-qubit operations.
Proceedings of the Royal Society A, 475(2227):20190251, 2019.

[79] Eric Chitambar and Gilad Gour.
Comparison of incoherent operations and measures of coherence.
Physical Review A, 94(5):052336, 2016.

[80] 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.

[81] Aram W Harrow.
The church of the symmetric subspace.
arXiv preprint arXiv:1308.6595, 2013.

[82] Reinhard F. Werner.
Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model.
Phys. Rev. A, 40:4277–4281, Oct 1989.

[83] Stephanie Wehner, David Elkouss, and Ronald Hanson.
Quantum internet: A vision for the road ahead.
Science, 362(6412):–, 2018.

[84] C. Branciard, N. Gisin, and S. Pironio.
Characterizing the nonlocal correlations created via entanglement swapping.
Phys. Rev. Lett., 104:170401, Apr 2010.

[85] Cyril Branciard, Denis Rosset, Nicolas Gisin, and Stefano Pironio.
Bilocal versus nonbilocal correlations in entanglement-swapping experiments.
Phys. Rev. A, 85:032119, Mar 2012.

[86] Tobias Fritz.
Beyond Bell's theorem: correlation scenarios.
New J. Phys., 14(10):103001, oct 2012.

[87] Rafael Chaves and Tobias Fritz.
Entropic approach to local realism and noncontextuality.
Phys. Rev. A, 85(3):–, Mar 2012.

[88] Armin Tavakoli, Paul Skrzypczyk, Daniel Cavalcanti, and Antonio Acín.
Nonlocal correlations in the star-network configuration.
Phys. Rev. A, 90:062109, Dec 2014.

[89] Rafael Chaves.
Polynomial Bell Inequalities.
Phys. Rev. Lett., 116:010402, Jan 2016.

[90] Denis Rosset, Cyril Branciard, Tomer Jack Barnea, Gilles Pütz, Nicolas Brunner, and Nicolas Gisin.
Nonlinear bell inequalities tailored for quantum networks.
Phys. Rev. Lett., 116:010403, Jan 2016.

[91] Mirjam Weilenmann and Roger Colbeck.
Non-Shannon inequalities in the entropy vector approach to causal structures.
Quantum, 2:57, Mar 2018.

[92] Elie Wolfe, Robert W. Spekkens, and Tobias Fritz.
The inflation technique for causal inference with latent variables.
J. Causal Inference, 7(2):–, Jul 2019.

[93] Nicolas Gisin, Jean-Daniel Bancal, Yu Cai, Patrick Remy, Armin Tavakoli, Emmanuel Zambrini Cruzeiro, Sandu Popescu, and Nicolas Brunner.

Constraints on nonlocality in networks from no-signaling and independence.
Nature communications, 11(1):1–6, 2020.

[94] Johan Åberg, Ranieri Nery, Cristhiano Duarte, and Rafael Chaves.
Semidefinite tests for quantum network topologies.
Phys. Rev. Lett., 125(11):–, Sep 2020.

[95] Elie Wolfe, Alejandro Pozas-Kerstjens, Matan Grinberg, Denis Rosset, Antonio Acín, and Miguel Navascués.
Quantum inflation: A general approach to quantum causal compatibility.
Phys. Rev. X, 11:021043, May 2021.

[96] Tamás Kriváchy, Yu Cai, Daniel Cavalcanti, Arash Tavakoli, Nicolas Gisin, and Nicolas Brunner.
A neural network oracle for quantum nonlocality problems in networks.
npj Quantum Information, 6(1):1–7, 2020.

[97] Thomas C. Fraser and Elie Wolfe.
Causal compatibility inequalities admitting quantum violations in the triangle structure.
Phys. Rev. A, 98:022113, Aug 2018.

[98] Marc-Olivier Renou and Salman Beigi.
Network nonlocality via rigidity of token-counting and color-matching, 2020.

[99] Ivan Šupić, Jean-Daniel Bancal, Yu Cai, and Nicolas Brunner.
Genuine network quantum nonlocality and self-testing, 2021.

[100] Miguel Navascués, Elie Wolfe, Denis Rosset, and Alejandro Pozas-Kerstjens.
Genuine network multipartite entanglement.
Phys. Rev. Lett., 125:240505, Dec 2020.

[101] Ming-Xing Luo.
New genuine multipartite entanglement.
arXiv e-prints, page arXiv:2003.07153, March 2020.

[102] Tristan Kraft, Cornelia Spee, Xiao-Dong Yu, and Otfried Gühne.
Characterizing quantum networks: Insights from coherence theory.
Phys. Rev. A, 103(5), May 2021.

[103] Daniel Cavalcanti, Paul Skrzypczyk, GH Aguilar, RV Nery, PH Souto Ribeiro, and SP Walborn.
Detection of entanglement in asymmetric quantum networks and multipartite quantum steering.
Nature communications, 6(1):1–6, 2015.

[104] Q. Y. He and M. D. Reid.
Genuine multipartite Einstein-Podolsky-Rosen steering.
Phys. Rev. Lett., 111:250403, Dec 2013.

[105] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert.
"Event-ready-detectors" Bell experiment via entanglement swapping.
Phys. Rev. Lett., 71:4287–4290, Dec 1993.

[106] Marco Túlio Quintino, Nicolas Brunner, and Marcus Huber.
Superactivation of quantum steering.
Phys. Rev. A, 94:062123, Dec 2016.

[107] Nora Tischler, Farzad Ghafari, Travis J. Baker, Sergei Slussarenko, Raj B. Patel, Morgan M. Weston, Sabine Wollmann, Lynden K. Shalm, Varun B. Verma, Sae Woo Nam, H. Chau Nguyen, Howard M. Wiseman, and Geoff J. Pryde.
Conclusive experimental demonstration of one-Way Einstein-Podolsky-Rosen steering.
Phys. Rev. Lett., 121:100401, Sep 2018.

[108] Marco Túlio Quintino, Tamás Vértesi, Daniel Cavalcanti, Remigiusz Augusiak, Maciej Demianowicz, Antonio Acín, and Nicolas Brunner.
Inequivalence of entanglement, steering, and Bell nonlocality for general measurements.
Phys. Rev. A, 92(3):032107, Sep 2015.

[109] Ana Belén Sainz, Nicolas Brunner, Daniel Cavalcanti, Paul Skrzypczyk, and Tamás Vértesi.
Postquantum steering.
Phys. Rev. Lett., 115:190403, Nov 2015.

[110] Feng Zhu, Max Tyler, Natalia Herrera Valencia, Mehul Malik, and Jonathan Leach.
Is high-dimensional photonic entanglement robust to noise?
AVS Quantum Science, 3(1):011401, 2021.

[111] Sebastian Ecker, Frédéric Bouchard, Lukas Bulla, Florian Brandt, Oskar Kohout, Fabian Steinlechner, Robert Fickler, Mehul Malik, Yelena Guryanova, Rupert Ursin, et al.
Overcoming noise in entanglement distribution.
Physical Review X, 9(4):041042, 2019.

[112] Sébastien Designolle, Vatshal Srivastav, Roope Uola, Natalia Herrera Valencia, Will McCutcheon, Mehul Malik, and Nicolas Brunner.
Genuine high-dimensional quantum steering.
Physical Review Letters, 126(20):200404, 2021.

[113] M. D. Reid.
Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification.
Phys. Rev. A, 40:913–923, Jul 1989.

[114] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng.
Realization of the Einstein-Podolsky-Rosen paradox for continuous variables.
Phys. Rev. Lett., 68:3663–3666, Jun 1992.

[115] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid.
Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox.
Phys. Rev. A, 80:032112, Sep 2009.

[116] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde.
Experimental EPR-steering using Bell-local states.
Nature Physics, 6(11):845–849, sep 2010.

[117] Howard M Wiseman, Steve James Jones, and Andrew C Doherty.
Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox.
Physical review letters, 98(14):140402, 2007.

[118] Marco Túlio Quintino, Tamás Vértesi, and Nicolas Brunner.
Joint measurability, Einstein-Podolsky-Rosen steering, and bell nonlocality.
Phys. Rev. Lett., 113:160402, 2014.

[119] Roope Uola, Tobias Moroder, and Otfried Gühne.
Joint measurability of generalized measurements implies classicality.
Phys. Rev. Lett., 113:160403, 2014.

[120] Roope Uola, Costantino Budroni, Otfried Gühne, and Juha-Pekka Pellonpää.
One-to-one mapping between steering and joint measurability problems.
Phys. Rev. Lett., 115(23):230402, 2015.

[121] Dariusz Chruściński and Andrzej Kossakowski.
On partially entanglement breaking channels.
Open Systems & Information Dynamics, 13(1):17–26, 2006.

[122] Andreas Bluhm, Lukas Rauber, and Michael M Wolf.
Quantum compression relative to a set of measurements.
In *Annales Henri Poincare*, volume 19, pages 1891–1937. Springer, 2018.

[123] Andreas Bluhm, Leevi Leppäjärvi, and Ion Nechita.
On the simulation of quantum multimeters.
arXiv preprint arXiv:2402.18333, 2024.

[124] Andreas Bluhm.
Compression and measurements in quantum information theory.
PhD thesis, Technische Universität München, 2019.

[125] Ioannis Kogias, Paul Skrzypczyk, Daniel Cavalcanti, Antonio Acín, and Gerardo Adesso.
Hierarchy of steering criteria based on moments for all bipartite quantum systems.
Physical Review Letters, 115(21), Nov 2015.

[126] Tobias Moroder, Oleg Gittsovich, Marcus Huber, Roope Uola, and Otfried Gühne.
Steering Maps and Their Application to Dimension-Bounded Steering.
Physical Review Letters, 116(9), Mar 2016.

[127] Otfried Gühne, Erkka Haapasalo, Tristan Kraft, Juha-Pekka Pellonpää, and Roope Uola.
Incompatible measurements in quantum information science.
arXiv:2112.06784, 2021.

[128] Paul Skrzypczyk, Miguel Navascués, and Daniel Cavalcanti.
Quantifying Einstein-Podolsky-Rosen steering.
Phys. Rev. Lett., 112:180404, May 2014.

[129] Roope Uola, Tristan Kraft, Jiangwei Shang, Xiao-Dong Yu, and Otfried Gühne.
Quantifying quantum resources with conic programming.
Physical review letters, 122(13):130404, 2019.

[130] Nicolas Brunner, Stefano Pironio, Antonio Acin, Nicolas Gisin, André Allan Méthot, and Valerio Scarani.
Testing the Dimension of Hilbert Spaces.
Phys. Rev. Lett., 100:210503, May 2008.

[131] Pauli Jokinen, Sophie Egelhaaf, Juha-Pekka Pellonpää, and Roope Uola.
Compressing continuous variable quantum measurements.
arXiv preprint arXiv:2312.13814, 2023.

[132] Tameem Albash and Daniel A Lidar.
Adiabatic quantum computation.
Reviews of Modern Physics, 90(1):015002, 2018.

[133] Samuel L Braunstein and Peter Van Loock.
Quantum information with continuous variables.
Reviews of Modern Physics, 77(2):513, 2005.

[134] 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.

[135] 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.

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

[137] Khaled Ben Dana, María García Díaz, Mohamed Mejatty, and Andreas Winter.
Resource theory of coherence: Beyond states.
Physical Review A, 95(6):062327, 2017.

[138] Robert Raussendorf and Hans J Briegel.
A one-way quantum computer.
Physical Review Letters, 86(22):5188, 2001.

[139] 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.

[140] Martin Hebenstreit, Richard Jozsa, Barbara Kraus, and Sergii Strelchuk.
Computational power of matchgates with supplementary resources.
Physical Review A, 102(5):052604, 2020.

[141] 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.

[142] Barbara M Terhal and David P DiVincenzo.
Classical simulation of noninteracting-fermion quantum circuits.
Physical Review A, 65(3):032325, 2002.

[143] Michael A Nielsen.
Cluster-state quantum computation.
Reports on Mathematical Physics, 57(1):147–161, 2006.

[144] Daniel Gottesman and Isaac L Chuang.
Quantum teleportation is a universal computational primitive.
arXiv preprint quant-ph/9908010, 1999.

[145] M Nest.
Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond.
arXiv preprint arXiv:0811.0898, 2008.

[146] 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.

[147] 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.

[148] Aram W Harrow and Ashley Montanaro.
Quantum computational supremacy.
Nature, 549(7671):203–209, 2017.

[149] Luke E Heyfron and Earl T Campbell.
An efficient quantum compiler that reduces T count.
Quantum Science and Technology, 4(1):015004, 2018.

[150] 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.

[151] 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.

[152] Matteo Rossi, Marcus Huber, Dagmar Bruß, and Chiara Macchiavello.
Quantum hypergraph states.
New Journal of Physics, 15(11):113022, 2013.

[153] Yaoyun Shi.
Both toffoli and controlled-NOT need little help to do universal quantum computing.
Quantum Info. Comput., 3(1):84–92, 2003.

[154] Dorit Aharonov.
A simple proof that Toffoli and Hadamard are quantum universal.

arXiv preprint quant-ph/0301040, 2003.

[155] Sergey Bravyi, Graeme Smith, and John A Smolin.
Trading classical and quantum computational resources.
Physical Review X, 6(2):021043, 2016.

[156] 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.

[157] Nathan Killoran, Frank ES Steinhoff, and Martin B Plenio.
Converting nonclassicality into entanglement.
Physical Review Letters, 116(8):080402, 2016.

[158] Patrick Hayden, Debbie Leung, Peter W Shor, and Andreas Winter.
Randomizing quantum states: Constructions and applications.
Communications in Mathematical Physics, 250:371–391, 2004.

[159] Ashley Montanaro.
Quantum states cannot be transmitted efficiently classically.
Quantum, 3:154, 2019.

[160] Ryuji Takagi and Hiroyasu Tajima.
Universal limitations on implementing resourceful unitary evolutions.
Physical Review A, 101(2):022315, 2020.

[161] Ingemar Bengtsson and Karol Życzkowski.
Geometry of quantum states: an introduction to quantum entanglement.
Cambridge university press, 2017.

[162] Marc Hein, Wolfgang Dür, Jens Eisert, Robert Raussendorf, M Nest, and H-J Briegel.
Entanglement in graph states and its applications.
arXiv preprint quant-ph/0602096, 2006.

[163] Marc Hein, Jens Eisert, and Hans J Briegel.
Multiparty entanglement in graph states.
Physical Review A, 69(6):062311, 2004.

[164] Damian Markham and Alexandra Krause.
A simple protocol for certifying graph states and applications in quantum networks.
Cryptography, 4(1):3, 2020.

[165] Bastian Jungnitsch, Tobias Moroder, and Otfried Gühne.
Taming multiparticle entanglement.
Physical review letters, 106(19):190502, 2011.

[166] Michael Walter, David Gross, and Jens Eisert.
Multipartite entanglement.
Quantum Information: From Foundations to Quantum Technology Applications, pages 293–330, 2016.

[167] Ingemar Bengtsson and Karol Zyczkowski.
A brief introduction to multipartite entanglement.
arXiv preprint arXiv:1612.07747, 2016.

[168] H Jeff Kimble.
The quantum internet.
Nature, 453(7198):1023–1030, 2008.

[169] Andrew J Scott.
Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions.
Physical Review A, 69(5):052330, 2004.

[170] Wolfgang Dür and Hans J Briegel.
Entanglement purification and quantum error correction.
Reports on Progress in Physics, 70(8):1381, 2007.

[171] Oded Goldreich, Shari Goldwasser, and Dana Ron.
Property testing and its connection to learning and approximation.
Journal of the ACM (JACM), 45(4):653–750, 1998.

[172] Eldar Fischer.
The art of uninformed decisions: A primer to property testing.
In *Current Trends in Theoretical Computer Science: The Challenge of the New Century Vol 1: Algorithms and Complexity Vol 2: Formal Models and Semantics*, pages 229–263. World Scientific, 2004.

[173] Aram W Harrow and Ashley Montanaro.
Testing product states, quantum Merlin-Arthur games and tensor optimization.
Journal of the ACM (JACM), 60(1):1–43, 2013.

[174] Florian Mintert, Marek Kuś, and Andreas Buchleitner.
Concurrence of mixed multipartite quantum states.
Physical review letters, 95(26):260502, 2005.

[175] Harry Buhrman, Richard Cleve, John Watrous, and Ronald De Wolf.
Quantum fingerprinting.
Physical review letters, 87(16):167902, 2001.

[176] Aram W Harrow, Cedric Yen-Yu Lin, and Ashley Montanaro.
Sequential measurements, disturbance and property testing.
In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1598–1611. SIAM, 2017.

[177] Oded Goldreich.
Introduction to testing graph properties.
Property testing: current research and surveys, pages 105–141, 2010.

[178] Ashley Montanaro and Changpeng Shao.
Quantum algorithms for learning a hidden graph.
In *17th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2022)*. Schloss-Dagstuhl-Leibniz Zentrum für Informatik, 2022.

[179] Liming Zhao, Carlos A Pérez-Delgado, and Joseph F Fitzsimons.
Fast graph operations in quantum computation.
Physical Review A, 93(3):032314, 2016.

[180] Aditi Sen(De) and Ujjwal Sen.
Channel capacities versus entanglement measures in multiparty quantum states.
Physical Review A, 81(1):012308, 2010.

[181] Tamoghna Das, Sudipto Singha Roy, Shrobona Bagchi, Avijit Misra, Aditi Sen, Ujjwal Sen, et al.
Generalized geometric measure of entanglement for multiparty mixed states.
Physical Review A, 94(2):022336, 2016.

[182] Mengru Ma, Yinfei Li, and Jiangwei Shang.
Multipartite entanglement measures: a review.
arXiv preprint arXiv:2309.09459, 2023.

[183] Patrick Hayden, Debbie W Leung, and Andreas Winter.
Aspects of generic entanglement.
Communications in mathematical physics, 265:95–117, 2006.

[184] Antonio Anna Mele.
Introduction to Haar Measure Tools in Quantum Information: A Beginner's Tutorial.
arXiv preprint arXiv:2307.08956, 2023.

[185] Aram Harrow, Patrick Hayden, and Debbie Leung.
Superdense coding of quantum states.
Physical review letters, 92(18):187901, 2004.

[186] David Gross, Steve T Flammia, and Jens Eisert.
Most quantum states are too entangled to be useful as computational resources.
Physical Review Letters, 102(19):190501, 2009.

[187] Michael J Bremner, Caterina Mora, and Andreas Winter.
Are random pure states useful for quantum computation?
Physical Review Letters, 102(19):190502, 2009.

[188] Zi-Wen Liu and Andreas Winter.
Many-Body Quantum Magic.
PRX Quantum, 3:020333, May 2022.

[189] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter.
Everything you always wanted to know about LOCC (but were afraid to ask).
Communications in Mathematical Physics, 328:303–326, 2014.

[190] Arne Heimendahl, Markus Heinrich, and David Gross.
The axiomatic and the operational approaches to resource theories of magic do not coincide.
Journal of Mathematical Physics, 63(11):112201, 2022.