Sequential measurement in quantum learning

Hector Spencer-Wood

Submitted for the
degree of Doctor of Philosophy

School of Physics and Astronomy
College of Science and Engineering
University of Glasgow

May 2024

Abstract

In an increasingly quantum world with more and more quantum technologies nearing practical use, the importance of interacting directly with quantum data is becoming clear. Although doing so often leads to advantages, it also presents us with some uniquely quantum challenges: for example, information about a quantum system cannot, in general, be extracted without disturbing the state of the system. In this thesis, we primarily focus on how performing a learning task on quantum data disturbs it, and affects one's ability to learn about it again in the future. In particular, we focus on the learning task of unsupervised binary classification, and how it affects quantum data when it is performed on a subset of it. In such a binary classification task, we are given a dataset that is made up of qubits that are each in one of two unknown pure states, and our aim is to cluster, with optimal probability of success, the data points into two groups based on their state. To investigate how well we can perform this task sequentially, we first consider a base case of a three-qubit dataset, made up of qubits that are each in one of two unknown states, and investigate how an intermediate classification on a two-qubit subset affects our ability to subsequently classify the whole dataset. We analytically derive and plot the tradeoff between the success rates of the two classifications and find that, although the intermediate classification does indeed affect the subsequent one in a non-trivial way, there is a remarkably large region where the first classification does not force the second away from its optimal probability of success. We then describe this scenario as a quantum circuit and simulate the tradeoff using Qiskit's AerSimulator. Following on from this, we go on to investigate whether an intermediate measurement can leave a subsequent one unaffected in the more general setting of an n-qubit dataset, again made up of qubits that are each in one of two unknown states. We see that numerics hint that nothing about the order of the qubits in a $(n-1)$-qubit dataset can be learnt without affecting a subsequent classification on the full dataset. We make steps to prove that this is indeed the case and show that an immediate consequence of this is that, for some $m > 1$, a non-trivial intermediate classification on $n-m$ qubits will always negatively affect a subsequent one on all n qubits. We conclude this line of work by deriving two bounds to how successful an intermediate classification of $n-1$ qubits can be without affecting the following n-qubit one, hypothesising that one of these is optimal.

We then shift our focus to the field of indefinite causal order (ICO). Motivated by ICO's connection to non-commutivity, we explore the idea of implementing quantum key distribution (QKD) in an indefinite causal regime. After showing that it is possible to share a key in an ICO, we find that, unlike other QKD protocols in the literature, eavesdroppers can be detected without publicly discussing a subset of the shared key. Indeed, we show that this is true for any individual attack in which the eavesdroppers abide by the causal structure chosen by the sharing parties. Further, we prove the security of this protocol for a subclass of these individual attacks. We then ask whether this "private detection" is a truly consequence of ICO and show that there is a definite causal ordered strategy that appears to yield the same phenomenon. Although we note that there are hints of some more subtle differences between the definite and indefinite causal cases, we conclude that carrying out QKD in an ICO is unlikely to offer any advantage, at least when considered in the form that we did. Finally, we close this thesis by summarising what we have found and noting some possible directions for future study.

Acknowledgements

First and foremost, I can't thank my main supervisor Sarah Croke enough for my PhD experience. The level of support, advice, independence and tolerance to ridiculous questions that I received from you has allowed me to genuinely have fun working on physics problems. Being surprised that this is possible, I am forever grateful. I would also like to thank John Jeffers for all the support and useful discussions, especially in the earlier years of my Ph.D. - I can only apologise for the horrendous notations I subjected you and Sarah to. Thanks too to Fiona Speirits for always being willing to offer advice and guidance, but more importantly, for having the best chat at our group meetings.

Thanks to the rest of the Quantum Theory group at the University of Glasgow. I'm certain I'm not over-exaggerating when I say that it is the world's friendliest research group. The kindness and inclusively that everyone in the group showed since day one was a key factor in making my time doing this Ph.D. such a positive experience. Everyone in the group deserves thanks: Steve, Rob, Jim, Jörg, Nic, Giulio, Claire, Dom and Francis. But a particularly large one goes to the other Ph.D. students (past and present): Ben, Maddie, Nico, Tom, Romek, Neel, Scarlett, Annette, Fergus, Zhujun, Roselyn, Lizzie, Mairi, Billy. Finally from the physics part of my life, thanks to my new office-mates, from the strange world of gravitational waves: Ardiana (thanks for the motivation), Alex, Shashwat, Jen and Xiaofei - I'll finally stop hogging the whiteboard.

To my friends outside of physics, thank you, I couldn't have done this without the change of scenery you provided. Rob (Bertrand) and Gav (Addy): you are the best flatmates I could ask for, there are too many memories and inside jokes to mention here, but I appreciate every one of them. Ryan (Ryzie), Lauren (Enzo), Lewis (Lewsis), Kyrie (Keeks), Ben (Carbi B), Maddie (Modo), I love living in Glasgow because of you, thank you for so much for all the *good times* over the years. An additional shout out to Nico (Coco) too, you're pretty much Glasgow. Zander, Katie and everyone from back home, thanks for being so unrelentingly silly. To the BMX world: Jake, Rory, David, Alex, John, Chaz, Dave, Grant, Fraz and everyone at BSD, (and everyone else I ride bikes with) thank you for all the fun and motivation to not be a one-sided coin. Thank you also to everyone from my undergraduate years. In particular, Alex, Camilla, Albus and Lucius - you're my favourite Danish people, and Ruaraidh - thanks for all the physics nightmares **CCWZ** and jams we had. To the squash players: Thejas, Amy and many of the people mentioned above, the stress of thesis writing was sustainable thanks to you.

Finally I'd like to thank my family. To my parents: Ettie and Jonathan, I'm so grateful for everything you've done for me. The unconditional support you've offered in every weird phase of my life has allowed me to pursue things purely for the sake of interest and enjoyment. Special thanks also to Lydia, Scott, Noah, Stan, Bill and Freya, as I feel like I've bored you more than anyone else with my physics chat. Of course, thanks to all my other siblings: Holly, Tom (plus respective families), and also my extended family - I can make it to the next family holiday now that this is done.

Author's Declaration

I certify that the thesis presented here for examination for a PhD degree of the University of Glasgow is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it) and that the thesis has not been edited by a third party beyond what is permitted by the University's PGR Code of Practice.

I declare that the thesis does not include work forming part of a thesis presented successfully for another degree.

I declare that this thesis has been produced in accordance with the University of Glasgow's Code of Good Practice in Research. I acknowledge that if any issues are raised regarding good research practice based on review of the thesis, the examination may be postponed pending the outcome of any investigation of the issues.

Parts of this work either have been, or will be, published in:

- H. Spencer-Wood, J. Jeffers, and S. Croke. "Measurement disturbance tradeoffs in three-qubit unsupervised quantum classification". *Phys. Rev. A* 105 (2022);
- H. Spencer-Wood. "Indefinite causal key distribution". *arXiv preprint arXiv:2303.03893* (2023);
- H. Spencer-Wood, J. Jeffers, and S. Croke. "Sequential unsupervised classification of quantum data". *In preparation*;

Hector Spencer-Wood
May 2024

Contents

Chapter 1

Introduction and summary

The interface between the classical and quantum worlds has been an endless source of intrigue since the earliest days of quantum mechanics. That the universe at the smallest scales behaves so differently when compared with what we're familiar with at our everyday, classical scales, has led to countless foundational questions about it. Ranging from whether classical physics emerges from quantum, to what resources make the quantum world intrinsically different from the classical one [1], one line of inquiry in particular has also received a great deal of attention from a practical viewpoint. Namely: by what processes, and to what extent, can we, living in a classical system, interact with the information in a quantum system? The practical significance of this question came into sharp focus thanks to a series of discoveries showing differences, and often advantages, to working with quantum information over its classical counterpart [2–8]. Indeed, the hints of possible *quantum advantages*, along with our relatively recent ability to work, experimentally, with individual quantum systems has catalysed a quantum revolution [9]. However, there is another side to the story: the limitations of working with quantum information. For example, unknown quantum states famously cannot be cloned [2, 3], and it is not possible to extract information about a quantum system without inducing disturbance [10][1]. Understanding such limitations is important, not only for understanding how the world works, but also for knowing what we can hope for from such a quantum revolution. It is in relation to this side of the story that is the main theme of this thesis. That is, the limits of our interaction with, and information extraction from, quantum systems. To investigate this, we focus on the field of quantum learning, in particular, the problem of learning about unknown quantum data. One of the chief aims of this work is to understand something about how quantum data is affected by the process of learning, and how this affects the reusabilty of such data.

In Chapter 2 we introduce the background theory required for the understanding of this work. By introducing the postulates of quantum mechanics, we are able to cover many of the concepts and notations used, including that of quantum systems and states, along with quantum measurements in the form of POVMs and, more generally, quantum instruments. We then take time to introduce the mathematical necessities of this thesis, focusing largely on various aspects of representation theory.

In Chapter 3, we take our first steps in understanding the effects of an unsupervised quantum learning task on a set of quantum data. To do this, we consider a simple scenario of a quantum dataset made up of three quantum bits (qubits), where each qubit occupies one of two possible unknown states, and the learning task we will focus on (throughout this thesis) is a binary classification. As mentioned earlier, we are interested in how such a classification would affect the dataset. Therefore, our contribution to this problem is to consider how an intermediate classification on a subset of the first two qubits would affect one's ability to subsequently classify the entire dataset. As we will see, these classifications are realised as quantum measurements, so the non-triviality of this problem has its roots in the quantum phenomenon of measurement disturbance. This work culminates in a full, analytical tradeoff between the success rate of the intermediate classification, with that of the subsequent one. We end this chapter with the construction of a quantum circuit that carries out this protocol. With this, we are able to use a simulation of a quantum processor to recreate the tradeoff we derived.

[1] Which could both be desirable properties, or the contrary, depending on who you ask. For example, quantum cryptographers might be grateful for them whereas quantum cryptanalysts might disagree [4].

Moving on, in Chapter 4, we make steps to generalise the results of Chapter 3 to the case of an n-qubit dataset. As we will see, in the $2 \to 3$-qubit case of Chapter 3, although the intermediate, two-qubit classification has a non-trivial effect on the success rate of the subsequent three-qubit classification, there is a notable region where, despite allowing us to learn something, the first classification does not affect the success rate of the second one. So, in Chapter 4, we explore the generalisation of this phenomenon to an n-qubit dataset and ask how strong an initial classification on a subset of $n-1$ qubits can be *without* affecting the overall success rate of a subsequent classification on the entire dataset. We find that we seem to be limited in what we can learn about the $(n-1)$-qubit subset in this scenario. We make steps in showing that, although we can deduce something about how many of each type of state there is, we are not able to learn anything about how they are ordered without negatively impacting the classification on the entire dataset. We show that it follows immediately from this that, if true, a classification on $n-m$ qubits (for $m > 1$) cannot even tell us anything about the numbers of each type of qubit without affecting a subsequent n-qubit classification. Following on from this, we construct an intermediate measurement [corresponding the $(n-1)$-qubit classification] that realises an analytical, closed form lower bound to the optimal success rate achievable in the first step that does not affect the second. Finally, we write down an algorithm to construct a measurement that gives an improved lower bound. We hypothesise that this strategy is an optimal one.

In Chapter 5, we move away from quantum learning to look at something quite different: a study of quantum key distribution in an indefinite causal setting. Indefinite causal order is, yet another, counterintuitive quantum phenomenon. Whereas in our classical world, we are used to events happening in a well defined order: A before B or vice versa, in quantum mechanics, these events can happen in a controlled superposition of orders. It it this that has been coined indefinite causal order [11–13]. The other component to this part of the thesis is quantum key distribution. In the original protocol [4], two parties, Alice and Bob, use quantum states, and mutually unbiased bases to a share a key whilst monitoring for eavesdroppers. Motivated by the non-commutativity of measurements in these mutually unbiased bases, we explore whether anything can be gained by placing Alice and Bob in an indefinite causal order. We should note that although it is not related to quantum learning, this chapter is not completely distinct from the others: a common thread is that of sequential measurements, in this case, sequential measurements in an indefinite causal order.

We conclude with Chapter 6 where we summarise what has been covered in this thesis. Here, we also look to the future and discuss open questions as well as possible directions for further research.

Chapter 2

Theoretical and mathematical background

2.1 Elements of linear algebra

In this section we highlight, briefly, the main linear algebra requirements to understand this work. We primarily follow Ref. [14], often taking definitions directly, and call on Refs. [15–17] when necessary. We refer the reader to these references for a more complete guide. We assume the reader is familiar with basic set theory, vector spaces, subspaces, their dimensionality and bases, as well as linear combinations and linear independence. Unless stated otherwise, we will be taking our vector spaces to be complex[1] and finite-dimensional throughout.

2.1.1 Linear operators

We begin with linear transformations.

Definition 2.1.1. *Let V, W be finite-dimensional vector spaces over a field $\mathbb{F}$. A function $T : V \to W$ is a linear transformation if, for all $\mathbf{u}, \mathbf{v} \in V,\ \alpha, \beta \in F$,*

$$T(\alpha\mathbf{u} + \beta\mathbf{v}) = \alpha T(\mathbf{u}) + \beta T(\mathbf{v}).$$

We will often call T a linear transformation on V.

Another term for a linear transformation is a *vector space homomorphism*. It turns out that, since we are taking our vector spaces to be finite dimensional, every linear transformation T can be represented by a matrix, with respect to bases of the input and output spaces of T. It will often be the case that we have a particular basis in mind, so we usually think of our linear transformations as matrices.

Definition 2.1.2. *For two vector spaces V, W, if a linear transformation $T : V \to W$ is bijective, we call T a vector space isomorphism (or just an isomorphism if the context is clear). If such an isomorphism exists between V and W, we say V and W are isomorphic, written as $V \cong W$.*

Definition 2.1.3. *A linear operator is a linear transformation $T : V \to V$. We call $\mathcal{L}(V)$ the set of linear operators on V.*

The linear transformations we consider will usually be linear operators, and these can be considered as $d \times d$ matrices, where $d = \dim V$. We define $M_d(\mathbb{C})$ to be the set of $d \times d$ matrices with complex entries. All the operators (and transformations) we consider will be linear, and so we will refer to linear operators just as *operators*, with linearity implicitly assumed. We will use the terms operator and matrix interchangeably.

Let's consider some important examples and classes of operators. First, the identity operator $\mathbb{I}$ on a vector space V leaves every vector $\mathbf{v}$ unaffected: $\mathbb{I}\mathbf{v} = \mathbf{v},\ \forall \mathbf{v} \in V$. The set of *invertible operators* $A : V \to V$

[1] That is, a vector space over the field of the complex numbers $\mathbb{C}$.

is denoted by $\mathrm{GL}(V)$. Alternatively, thinking in terms of $d \times d$ matrices (where $d = \dim V$) with elements in the field $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, we define[2]

$$\mathrm{GL}(d, \mathbb{F}) = \{A \in M_d(\mathbb{F}) \ : \ \det A \neq 0\}, \tag{2.1}$$

such that $\det A$ denotes the determinant of A.

Another class of operators are Hermitian operators. An operator H is Hermitian if

$$H^\dagger = H, \tag{2.2}$$

where $H^\dagger$ denotes the *Hermitian conjugate* or *conjugate transpose*. Unitary operators are another class of useful operators. An operator U is unitary if

$$U^\dagger U = \mathbb{I} = U U^\dagger. \tag{2.3}$$

We will often call these *unitaries*, and supposing they act on some d-dimensional space V, we define the set of unitaries as $\mathrm{U}(V)$, or alternatively, $\mathrm{U}(d, \mathbb{F})$ when considering $d \times d$ matrices. An important example of both unitary and Hermitian operators are the Pauli operators, also known as the Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.4a}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{2.4b}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.4c}$$

where we have written these with respect to the *z-eigenbasis*, which will be made clearer later. The final class of operators we mention here make up a subset of the unitaries. Writing in terms of $d \times d$ matrices

$$\mathrm{SU}(d, \mathbb{F}) = \{U \in \mathrm{U}(d, \mathbb{F}) \ : \ \det U = 1\}. \tag{2.5}$$

Matrices in this set are called *special unitary*.

2.1.2 Hilbert spaces

Let us begin with inner products and inner product spaces.

Definition 2.1.4. *An inner product on a complex vector space V is a map $(,) : V \times V \to \mathbb{C}$ satisfying the following properties:*

1. *For all $\mathbf{v} \in V$,*
$$(\mathbf{v}, \mathbf{v}) \geq 0 \text{ and } (\mathbf{v}, \mathbf{v}) = 0 \iff \mathbf{v} = \mathbf{0}.$$
2. *For all $\mathbf{u}, \mathbf{v} \in V$,*
$$(\mathbf{u}, \mathbf{v}) = (\mathbf{v}, \mathbf{u})^*, \tag{2.6}$$
where α^* denotes complex the conjugation of $\alpha \in \mathbb{C}$.
3. *For all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, $\alpha, \beta \in \mathbb{C}$,*
$$(\alpha \mathbf{u} + \beta \mathbf{v}, \mathbf{w}) = \alpha(\mathbf{u}, \mathbf{w}) + \beta(\mathbf{v}, \mathbf{w}).$$

If two vectors $\mathbf{u}, \mathbf{v} \in V$ have the property: $(\mathbf{u}, \mathbf{v}) = 0$, we will say they are orthogonal with respect to the inner product $(,)$, or if it is unambiguous, just *orthogonal*. Also, if $(\mathbf{v}, \mathbf{v}) = 1$, we say $\mathbf{v}$ is *normalised*, or a *unit vector*. Vectors that are orthogonal *and* normalised are called *orthonormal*.

Definition 2.1.5. *A complex inner product space is a complex vector space V together with an inner product.*

[2]Since we always take $\mathbb{F} = \mathbb{C}$, we often omit mention of it and simply write $\mathrm{GL}(d)$.

We will rarely refer to inner product spaces in this work, opting instead for the term *Hilbert space*. A Hilbert space is an inner product space with the additional condition that it be *complete* under the metric induced by the inner product. However, since finite dimensional complex inner product spaces are automatically complete [18], they are finite dimensional Hilbert spaces. We will normally denote a Hilbert space using $\mathcal{H}$, and write its vectors as *"kets"*: $|v\rangle \in \mathcal{H}$. Indeed, for the remainder of this thesis, whether considering a Hilbert space or not, we will write our vectors in this ket notation. Further, if $|u\rangle, |v\rangle \in \mathcal{H}$, the notation we will use for the inner product $(,) : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ is

$$(|u\rangle, |v\rangle) =: \langle u|v\rangle. \tag{2.7}$$

The object $\langle v| \in \mathcal{H}^*$, that is often called a *"bra"*, is the *dual vector* to $|v\rangle \in \mathcal{H}$. A dual vector $\langle v|$ is a linear transformation $\langle v| : \mathcal{H} \to \mathbb{C}$, and the dual space $\mathcal{H}^*$ is the vector space made up of these dual vectors. For our purposes, a vector $|v\rangle$ and its dual $\langle v|$ are related via the Hermitian conjugate:

$$|v\rangle^\dagger = \langle v|. \tag{2.8}$$

We will often write vectors $|v\rangle \in \mathcal{H}$ in terms of some orthonormal basis $\mathcal{B} = \{|i\rangle\}$ for $\mathcal{H}$[3]:

$$|v\rangle = \sum_i v_i |i\rangle, \tag{2.9}$$

where we will sometimes call v_i amplitudes (due to their role in quantum states, which we will come to later). An orthonomal basis of $\mathcal{H}$ is a basis $\mathcal{B}$ made up of orthonormal vectors. That is, $\langle i|j\rangle = \delta_{ij},\ \forall |i\rangle, |j\rangle \in \mathcal{B}$. Indeed, we will often be interested in unit vectors, so in order for $|v\rangle$ to be a unit vector in the above example, $\sum_i |v_i|^2 = 1$. Further, we can access any (basis dependent) amplitude using $v_i = \langle i|v\rangle$, from which it follows that $\big(\sum_i |i\rangle\langle i|\big)|v\rangle = |v\rangle$. Since this true for any $|v\rangle \in \mathcal{H}$, we can write the following, very useful identity:

$$\sum_i |i\rangle\langle i| = \mathbb{I}, \tag{2.10}$$

for any orthonormal basis $\{|i\rangle\}$ of $\mathcal{H}$, where we call $|a\rangle\langle b|$ an outer product operator. We call this identity the completeness relation[4], and it allows us to write any linear transformation in a similar, outer product form. Suppose $A : \mathcal{H}_1 \to \mathcal{H}_2$ is a linear transformation and $\{|i\rangle\}_{i=0}^{n-1}$, $\{|j\rangle\}_{j=0}^{m-1}$ are orthonormal bases for $\mathcal{H}_1, \mathcal{H}_2$ respectively, then we can write

$$A = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ji} |j\rangle\langle i|, \tag{2.11}$$

such that $a_{ji} := \langle j|A|i\rangle \in \mathbb{C}$.

Direct sum

If we have two vectors $\mathbf{u} = (u_1, \ldots, u_n)^T, \mathbf{v} = (v_1, \ldots, v_m)^T$, we take the direct sum of these vectors to be

$$\mathbf{u} \oplus \mathbf{v} := (u_1, \ldots, u_n, v_1, \ldots, v_m)^T. \tag{2.12}$$

This gives rise to the direct product of vector spaces U, V:

$$U \oplus V := \{\mathbf{u} \oplus \mathbf{v} \ :\ \mathbf{u} \in U, \mathbf{v} \in V\}. \tag{2.13}$$

Given an $m \times n$ matrix A, and a $p \times q$ matrix B, the direct product of matrices is given by

$$A \oplus B := \begin{pmatrix} A & 0_{m\times q} \\ 0_{p\times n} & B \end{pmatrix}, \tag{2.14}$$

where $0_{i\times j}$ denotes an $i \times j$ matrix with a zero in every entry.

We will usually deal with square matrices in this thesis (i.e. $m = n,\ p = q$). We will call matrices that have the form given in Eq. (2.14) *block diagonal*. If the square matrices A and B are constant[5], we will call matrices of this form *block constant*.

[3] Since $\mathcal{H}$ has some finite dimension d, any set of d orthonormal unit vectors $\{|v_i\rangle\}_{i=1}^d \subset \mathcal{H}$ is an orthonomal basis.
[4] Distinct from the concept of completeness when defining Hilbert spaces.
[5] That is $A = a\mathbb{I}_m,\ B = b\mathbb{I}_p$, where $\mathbb{I}_i$ is the $i \times i$ identity matrix and $a, b \in \mathbb{C}$.

2.1.3 Equivalence relations

Equivalence relations are by no means unique to linear algebra and can be found throughout mathematics. Nevertheless, we define them in this section.

Definition 2.1.6. *Let S be a nonempty set. A relation $\sim$ on S is called an equivalence relation on S if it satisfies the following three conditions:*

1. *Reflexivity:*
$$a \sim a, \quad \forall a \in S.$$
2. *Symmetry:*
$$a \sim b \implies b \sim a, \quad \forall a, b \in S.$$
3. *Transitivity:*
$$a \sim b,\ b \sim c \implies a \sim c, \quad \forall a, b, c \in S.$$

Further, an equivalence class of $x \in S$ with respect to an equivalence relation $\sim$ is a subset $[x]$ of S such that

$$[x] = \{y \in S \ : \ y \sim x\}.$$

Sometimes the notation $[x]_\sim$ will be used to highlight the equivalence relation that the equivalence class is defined with respect to. The set of equivalence class forms a *partition* of S. Meaning that $[x] \cap [y] = \varnothing$ when $x \not\sim y$, and

$$\bigcup_{x \in S} [x] = S. \tag{2.15}$$

2.1.4 Eigenvalues and eigenvectors

Let $T \in \mathcal{L}(V)$ be a linear operator on a vector space V over a field $\mathbb{F}$ throughout.

Definition 2.1.7. *A scalar $\lambda \in \mathbb{F}$ is an eigenvalue of T if there exists a nonzero vector $|\lambda\rangle \in V$ such that*

$$T|\lambda\rangle = \lambda|\lambda\rangle.$$

Here, $|\lambda\rangle$ is called an eigenvector of T associated with λ.

Note that it is possible for more than one eigenvector to correspond to the same eigenvalue. With that, the set of linear combinations of eigenvectors $|\lambda_i\rangle$ associated with λ, together with the zero vector, forms a subspace of V, called the *eigenspace of* λ.

As we noted earlier, the Hermitian operators are an important class of operators in quantum mechanics. One property of note is that their eigenvalues are real numbers. If they are non-negative, then the corresponding operator is called *positive semidefinite*, though we will sometimes just say (somewhat inaccurately) *positive*. We indicate the positive semidefiniteness of an operator A by writing $A \geq 0$. Another property of Hermitian operators is that their eigenvectors, that correspond to distinct eigenvalues, are mutually orthogonal[6]. So if the number of distinct eigenvalues of a Hermitian operator $H \in \mathcal{L}(V)$ is the dimension of V, then the eigenvectors of H can used to form an orthonormal basis of V. We call such a basis an orthonormal *eigenbasis*. Consider the Pauli-z operator for instance given in Eq. (2.4), acting on a two-dimensional space $\mathbb{C}^2$. Its eigenvalues are distinct, and given by $\lambda_\pm = \pm 1$ which means its eigenvectors should be orthogonal, and, since there are two of them, form an orthonormal basis for $\mathcal{H}$. Indeed they do:

$$|\lambda_+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{2.16a}$$

$$|\lambda_-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.16b}$$

[6]More generally, for an arbitrary linear operator T, eigenvectors corresponding to distinct eigenvalues are linearly independent.

We call this basis the Pauli-z basis, or just the z-basis, and it was with respect to this basis that the Pauli matrices in Eq. (2.4) were written. The other Pauli operators σ_x, σ_y too have their own eigenbases, that we call the x and y-bases respectively.

Finally, we define the trace $\operatorname{Tr} A$ of a matrix A (which takes the same value as the trace of the corresponding operator) to be the sum of the elements along its main diagonal. Thinking of operators as square matrices, if a matrix is diagonalisable (i.e. if its eigenvectors are linearly independent), the elements along its diagonal correspond to its eigenvalues. So in these cases the trace is the sum of the eigenvalues. Actually, this is true more generally. As will always be the case in this work, if the elements of A are complex numbers (or any algebraically closed field), then $\operatorname{Tr} A$ is the sum of the eigenvalues of A.

To evaluate the trace, note that if $A : V \to V$ and $\{|i\rangle\}$ is an orthonormal basis for V, then we can write the trace as

$$\operatorname{Tr} A = \sum_i \langle i|A|i\rangle. \tag{2.17}$$

The trace is independent of the basis used, meaning $\{|i\rangle\}$ in the above expression can be replaced with any orthonormal basis for V. We end this section with some properties of the trace. Let A, B, C be matrices (or operators) on the same vector space over a field $\mathbb{F}$, and α be an element of $\mathbb{F}$, then the following properties hold:

$$\operatorname{Tr}(\alpha A + B) = \alpha \operatorname{Tr} A + \operatorname{Tr} B, \tag{2.18a}$$

$$\operatorname{Tr}(AB) = \operatorname{Tr}(BA). \tag{2.18b}$$

Two properties that follow from Eq. (2.18b) are

$$\operatorname{Tr}(CAC^{-1}) = \operatorname{Tr} A, \tag{2.19a}$$

$$\operatorname{Tr}(ABC) = \operatorname{Tr}(BCA) = \operatorname{Tr}(CAB) \neq \operatorname{Tr}(ACB), \tag{2.19b}$$

the last of which we call the cyclic property of the trace.

2.2 Quantum mechanics

Quantum mechanics as an axiomatic system traces its origins back to Dirac and von Neumann [19, 20]. This laid solid, mathematical foundations to do everything from *"Shut up and calculate!"*[7], to interpret and understand the theory. Luckily for us, it also provides us with a natural way to introduce a lot of the relevant background theory for this thesis. We will largely write the postulates in the form presented in Ref. [17], deviating and reordering every so often to better suit our needs. The discussion surrounding these postulates is based around elements of various standard texts [17, 18, 22–24], again deviating and expanding sometimes.

2.2.1 State spaces and states

The first postulate tells us how we describe *isolated* physical systems mathematically.

> **Postulate 1**
> Associated to any isolated physical system S is a Hilbert space $\mathcal{H}^S$, such that the system is completely described by a unit vector $|\psi\rangle^S \in \mathcal{H}^S$. We call $|\psi\rangle^S$ the state vector of the system, or just the state of the system.

We will often omit mention of the system S in our Hilbert space and vector notation, unless the ambiguity of the situation is too much without it, and conversely, sometimes we will attempt to improve clarity (e.g. to make the distinction between the system label and other indices more obvious) by writing the system in brackets, e.g. $|\psi\rangle^{(S)}$. As mentioned earlier, we will exclusively be working with finite dimensional systems, meaning that $\mathcal{H}$ need only be an inner-product space, although will usually refer to it as a Hilbert space. For any two vectors $|\psi\rangle, |\varphi\rangle \in \mathcal{H}$, the inner product $(\cdot,\cdot) : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ associated with $\mathcal{H}$ is defined and

[7] A misinterpretation of a quote attributed to N. David Mermin, who wrote it in relation to his thoughts on the Copenhagen interpretation [21].

written as $(|\psi\rangle, |\varphi\rangle) := |\psi\rangle^\dagger |\varphi\rangle \equiv \langle\psi|\varphi\rangle \in \mathbb{C}$. Being a unit vector, a quantum state $|\psi\rangle$ is required to satisfy $\langle\psi|\psi\rangle = 1$.

Although we will describe the state of a system with a unit vector $|\psi\rangle$, it should be noted that, more accurately, states are actually equivalence classes of unit vectors that give rise to the same measurement statistics [25]. These equivalence classes are called rays [26], and when it comes to quantum states, are defined with respect to the following equivalence relation:

$$|\psi'\rangle \sim |\psi\rangle \iff |\psi'\rangle = e^{i\phi}|\psi\rangle, \tag{2.20}$$

where $|\psi\rangle, |\psi'\rangle \in \mathcal{H}$ are unit vectors and $\phi \in \mathbb{R}$. In other words, vectors differing by a *global phase* are equivalent, since $|\langle\varphi|\psi\rangle| = |\langle\varphi|\psi'\rangle|$, for all $|\varphi\rangle \in \mathcal{H}$, which will make more sense when we encounter the Born rule. Having said all of this, in this work, we will follow the majority of the literature and describe states as vectors, whilst keeping in mind the equivalence of state vectors differing by a global phase.

The vector space structure associated with quantum systems means that state vectors can be put into linear combinations. That is, given two quantum states $|\psi\rangle, |\zeta\rangle \in \mathcal{H}^S$ of a system S, the vector

$$|\varphi\rangle = \alpha|\psi\rangle + \beta|\zeta\rangle, \tag{2.21}$$

such that $\alpha, \beta \in \mathbb{C}$, is also a valid state of S, as long as $\langle\varphi|\varphi\rangle = 1$. Linear combinations of vectors representing classical systems also occur, however, unlike classical physics, quantum mechanics is postulated to be a linear theory (as we will see later in this section), meaning quantum states evolve according to linear operators. Therefore, we can think of these linear combinations of vectors, as the system existing in a *superposition* of states. This is called the superposition principle.

The density operator

Define $\mathcal{L}(\mathcal{H})$ to be the vector space of linear operators $A : \mathcal{H} \to \mathcal{H}$. We can alternatively represent the quantum state of a system as an operator $\rho \in \mathcal{L}(\mathcal{H})$ (or equivalently, a matrix) satisfying the following conditions:

$$\rho \geq 0, \tag{2.22a}$$

$$\operatorname{Tr}\rho = 1, \tag{2.22b}$$

where, to reiterate from before, an operator satisfying the first condition is called positive semidefinite, and means that the eigenvalues of ρ are non-negative. This positive semidefinite condition implies that $\rho^\dagger = \rho$. The second condition comes as an analogue to requiring $\langle\psi|\psi\rangle = 1$. To see this, consider the density operator corresponding to the state vector $|\psi\rangle$: $\rho_\psi = |\psi\rangle\langle\psi|$. From this, we can see that

$$\operatorname{Tr}\rho_\psi = \sum_i \langle i|\rho_\psi|i\rangle = \sum_i \langle i|\psi\rangle\langle\psi|i\rangle = \sum_i \langle\psi|i\rangle\langle i|\psi\rangle = \langle\psi|\psi\rangle, \tag{2.23}$$

where, in the last step, we have used the completeness of $\{|i\rangle\}$.

The benefit of the density operator approach is that it provides us with a convenient way to describe more general situations than so far described. Until now, we have considered systems that occupy a known quantum state $|\psi\rangle$, which we call a *pure state*. However, what happens if, to our knowledge, there is a chance p that the system is in the pure state $|\psi\rangle$, but it's also possible (with probability $1-p$) that it is in another state $|\varphi\rangle$. This situation can be described using the density operator

$$\rho = p|\psi\rangle\langle\psi| + (1-p)|\varphi\rangle\langle\varphi|. \tag{2.24}$$

More generally, if a system is in the state ρ_i with probability $p_i \geq 0$, we can represent the state of the system as

$$\rho = \sum_i p_i \rho_i. \tag{2.25}$$

We require $\sum_i p_i = 1$, to ensure all possibilities are accounted for. If ρ can be written in the form $|\psi\rangle\langle\psi|$, we call it a *pure state*, else we say ρ is a *mixed state*.

The qubit

A quantum bit, or qubit is the fundamental unit of quantum information [27]. Defined in analogy to its classical counterpart: a binary digit, or bit, a qubit is a two-level quantum system. Its associated Hilbert space $\mathcal{H}_{\text{qubit}}$ is therefore two-dimensional, and to bring home the analogy to classical bits, which have two possible values: 0 or 1, we define the *computational basis* of $\mathcal{H}_{\text{qubit}}$ as $\{|0\rangle, |1\rangle\}$, conventionally taking $|0\rangle$ ($|1\rangle$) to be the eigenvector corresponding to the $+1$ (-1) eigenvalue of the z Pauli matrix σ_z. Due to the superposition principle, we can quickly spot a key difference between bits and qubits. That is, whereas bits can only take the value 0 *or* 1, qubits are free to be in a superposition of its basis states $|0\rangle$ and $|1\rangle$. In general, we can write a pure qubit state $|\psi\rangle \in \mathcal{H}_{\text{qubit}}$ as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.26}$$

where $\alpha, \beta \in \mathbb{C}$, satisfying $|\alpha|^2 + |\beta|^2 = 1$. Other bases that we will use frequently are the eigenbases of the other Pauli operators. Written in relation to the computational basis, the eigenvectors of σ_x are,

$$|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \tag{2.27}$$

and of σ_y,

$$|\pm i\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle). \tag{2.28}$$

We can alternatively write these in normal $\mathbb{C}^2$ vector notation as follows:

$$|0\rangle \simeq \begin{pmatrix}1\\0\end{pmatrix}, \ |1\rangle \simeq \begin{pmatrix}0\\1\end{pmatrix}, \tag{2.29a}$$

$$|\pm\rangle \simeq \frac{1}{\sqrt{2}}\begin{pmatrix}1\\\pm 1\end{pmatrix}, \tag{2.29b}$$

$$|\pm i\rangle \simeq \frac{1}{\sqrt{2}}\begin{pmatrix}1\\\pm i\end{pmatrix}. \tag{2.29c}$$

A physical example of a qubit, used throughout this work, is a spin-half particle. In this scenario, we define the computational basis in relation to the z-component of the spin m_z:

$$|0\rangle := \left|s = \frac{1}{2}, m_z = \frac{1}{2}\right\rangle, \tag{2.30a}$$

$$|1\rangle := \left|s = \frac{1}{2}, m_z = -\frac{1}{2}\right\rangle. \tag{2.30b}$$

The other bases discussed earlier correspond to the x and y-components of the spin. An alternate physical system is that of polarised light, where the computational basis can be defined as

$$|0\rangle := |H\rangle, \tag{2.31a}$$

$$|1\rangle := |V\rangle, \tag{2.31b}$$

where $|H\rangle$ and $|V\rangle$ denote horizontally and vertically polarised light, respectively. It follows that $|+/-\rangle$ correspond to diagonally/antidiagonally polarised light, and $|+i/-i\rangle$ represent left/right circularly polarised light.

For a visual way of thinking about the qubit, we can use the Bloch sphere. Any pure qubit state can be written as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \tag{2.32}$$

which corresponds to a point on a 3-dimensional unit sphere, called the Bloch sphere, with polar coordinates $\theta \in [0, \pi], \phi \in [0, 2\pi)$. Therefore, as visualised in Fig. 2.1, we can think of a pure qubit state as a point on the *surface* of the Bloch sphere. Of course, our qubit need not be in a pure state, it could be in a mixed state.

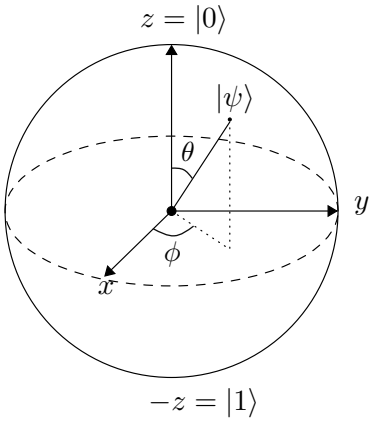

Figure 2.1: The Bloch sphere representation of the pure qubit state $|\psi\rangle$, given in Eq. (2.32). Note that antipodal points are orthogonal to one another.

Mixed (strictly not pure) states correspond to points *within* the Bloch sphere. Generally, we can represent any state ρ, mixed or pure, in terms of the identity and Pauli matrices[8] ($\mathbb{1}, \sigma_x, \sigma_y, \sigma_z$ respectively):

$$\rho = \frac{1}{2}\big(\mathbb{1} + \mathbf{a} \cdot \boldsymbol{\sigma}\big), \tag{2.33}$$

where $\boldsymbol{\sigma} := (\sigma_x, \sigma_y, \sigma_z)$, and $\mathbf{a} \in \mathbb{R}^3$ corresponds to the coordinates of a point in/on the Bloch sphere. It follows that $\mathbf{a}$ must satisfy $|\mathbf{a}| \leq 1$, with the equality occurring if and only if ρ is a pure state, which justifies that qubit states only lie on the surface of the Bloch sphere if they are pure. When this is the case, we can write $\mathbf{a} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ to recover $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle$ given in Eq. (2.32). The other extreme case occurs when $\mathbf{a} = 0$, in which case the state of the qubit is known as the maximally mixed state

$$\rho = \frac{1}{2}\mathbb{1}. \tag{2.34}$$

More generally, for a d-dimensional quantum system, the maximally mixed state is given by

$$\rho = \frac{1}{d}\mathbb{I}, \tag{2.35}$$

where $\mathbb{I}$, here, is the d-dimensional identity operator. Recalling the completeness relation in Eq. (2.10), we can interpret a system that occupies the maximally mixed state as being equally likely, as far as we can tell, to be in any state in an orthonormal basis.

Before moving on, we should note two notational points. First, we will reserve $\mathbb{1}$ to be the identity *only on qubit spaces* throughout this thesis, and secondly, we will occasionally write $[\psi] := |\psi\rangle\langle\psi|$ to describe a pure state density operator.

2.2.2 Composite systems

The second postulate tells us how we describe composite quantum systems mathematically. That is, a quantum system made up of multiple physical systems, e.g. two atoms.

> **Postulate 2**
> The state space $\mathcal{H}^S$ of a composite system $S = S_1 S_2 \dots S_n$, made up of n component systems $S_1, S_2, \dots, S_n$, is given by the tensor product of the component state spaces $\mathcal{H}^{S_1}, \mathcal{H}^{S_2}, \dots, \mathcal{H}^{S_n}$. That is, $\mathcal{H}^S = \mathcal{H}^{S_1} \otimes \mathcal{H}^{S_2} \otimes \cdots \otimes \mathcal{H}^{S_n}$.

[8] Since density operators are Hermitian, and $\{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$ form a basis for the space of 2×2 Hermitian matrices.

This provides us with the setting to write down the state of a composite system. Suppose $|\psi_i\rangle^{S_i} \in \mathcal{H}^{S_i}$ for $i \in \{1, \dots, n\}$, then the state $|\psi\rangle^S \in \mathcal{H}^S$ of the composite system S is given by

$$|\psi\rangle^S = |\psi_1\rangle^{S_1} \otimes |\psi_2\rangle^{S_2} \otimes \cdots \otimes |\psi_n\rangle^{S_n}. \tag{2.36}$$

We will regularly use the following shorthands

$$|\psi_1\rangle^{S_1} \otimes |\psi_2\rangle^{S_2} \otimes \cdots \otimes |\psi_n\rangle^{S_n} \equiv |\psi_1\rangle^{S_1}|\psi_2\rangle^{S_2} \cdots |\psi_n\rangle^{S_n} \equiv |\psi_1\psi_2 \cdots \psi_n\rangle^{S_1 S_2 \cdots S_n}, \tag{2.37}$$

often omitting mention of the systems wherever it does not confuse the matter. We can also write all of this in the density matrix formalism. If $\rho_i^{(S_i)} \in \mathcal{L}\big(\mathcal{H}^{S_i}\big)$ is the state of the system S_i, for $i \in \{1, \dots, n\}$, then the density operator $\rho^{(S)} \in \mathcal{L}\big(\mathcal{H}^S\big)$ of the composite system S is given by

$$\rho^{(S)} = \rho_1^{(S_1)} \otimes \rho_2^{(S_2)} \otimes \cdots \otimes \rho_n^{(S_n)}. \tag{2.38}$$

The states of a composite system that we have considered so far are called *separable*, in that they can be written as a tensor product of states of the component systems. Being a quantum system, S can be in a superposition of states, which leads to the possibility of states that are not separable, called *entangled states*. We will not go into the details of entanglement, but important examples of entangled states are known as the *Bell states*, representing a bipartite system S_1S_2 of two qubits with state space $\mathcal{H}_{\text{qubit}}^{S_1} \otimes \mathcal{H}_{\text{qubit}}^{S_2}$:

$$|\Phi^{\pm}\rangle^{S_1S_2} = \frac{1}{\sqrt{2}}\Big(|00\rangle^{S_1S_2} \pm |11\rangle^{S_1S_2}\Big), \tag{2.39a}$$

$$|\Psi^{\pm}\rangle^{S_1S_2} = \frac{1}{\sqrt{2}}\Big(|01\rangle^{S_1S_2} \pm |10\rangle^{S_1S_2}\Big), \tag{2.39b}$$

where we have used the computational basis of each component system, as defined previously. Note that since these states are orthonormal and there are four of them, they form an orthonormal basis for the four-dimensional state space $\mathcal{H}_{\text{qubit}}^{S_1} \otimes \mathcal{H}_{\text{qubit}}^{S_2}$. Likewise, in the density operator formalism, in general, $\rho^{(S)}$ can be written in the form

$$\rho^{(S)} = \sum_{|i\rangle, |j\rangle \in \mathcal{B}^S} r_{ji} |j\rangle\langle i| \tag{2.40}$$

(as long as $\rho^{(S)} \geq 0$, $\operatorname{Tr} \rho^{(S)} = 1$), where $\mathcal{B}^S$ is some basis for $\mathcal{H}^S$ and $r_{ji} \in \mathbb{C}$, meaning that the density matrix need not take the separable form of Eq. (2.38)[9]. Note that this form accounts for both pure and mixed states.

Given a composite system $S = S_1 \dots S_n$, we can also consider the state of any combination of the component systems using a *reduced density operator*. For simplicity, consider a bipartite system S_1S_2 in the state $\rho^{S_1S_2}$, then we write the state of the system S_1 using the reduced density operator

$$\rho^{S_1} = \operatorname{Tr}_{S_2} \rho^{S_1S_2} = \sum_{|i\rangle \in \mathcal{B}^{S_2}} \langle i|^{S_2} \rho^{S_1S_2} |i\rangle^{S_2}, \tag{2.41}$$

where Tr_{S_2} denotes the partial trace over system S_2, and $\mathcal{B}^{S_2} = \big\{|i\rangle^{S_2}\big\}$ is some orthonormal basis for $\mathcal{H}^{S_2}$. We could similarly find ρ^{S_2} by *"tracing out"* system S_1. It turns out that this partial trace operation is the unique choice to obtain the reduced density operator that correctly describes the corresponding component system.

This reduced density operator allows us to gain some more understanding of mixed states. That is, a mixed state of a system S can always be thought of as the reduced density operator of some pure state on a larger space $S' \supset S$. Take the maximally mixed state of a qubit S_1 described earlier: $\rho = \mathbb{1}/2$. This can

[9] This feature is perhaps obscured by how we wrote down our separable density operator in Eq. (2.38): that is, in the form of an element of $\mathcal{L}\big(\mathcal{H}^{S_1}\big) \otimes \cdots \otimes \mathcal{L}\big(\mathcal{H}^{S_n}\big)$, rather than $\mathcal{L}\big(\mathcal{H}^S\big) = \mathcal{L}\big(\mathcal{H}^{S_1} \otimes \cdots \otimes \mathcal{H}^{S_n}\big)$. It was okay to do this since $\mathcal{L}\big(\mathcal{H}^{S_1} \otimes \cdots \otimes \mathcal{H}^{S_n}\big) = \mathcal{L}\big(\mathcal{H}^{S_1}\big) \otimes \cdots \otimes \mathcal{L}\big(\mathcal{H}^{S_n}\big)$ for finite dimensional $\mathcal{H}^{S_i}$.

be written as the reduced density operator of a two-qubit system S_1S_2 in a Bell state $\Phi^+ = |\Phi^+\rangle\langle\Phi^+|^{(S_1S_2)}$, given in Eq. (2.39). Explicitly,

$$\begin{aligned}\mathrm{Tr}_{S_2}\,\Phi^+ &= \sum_{m=0}^{1} \langle m|^{(S_2)} \Big[|\Phi^+\rangle\langle\Phi^+|^{(S_1S_2)} \Big] |m\rangle^{(S_2)} \\ &= \frac{1}{2}\sum_{m=0}^{1} \Big[|0\rangle^{(S_1)}\langle m|0\rangle^{(S_2)} + |1\rangle^{(S_1)}\langle m|1\rangle^{(S_2)} \Big] \Big[\langle 0|^{(S_1)}\langle 0|m\rangle^{(S_2)} + \langle 1|^{(S_1)}\langle 1|m\rangle^{(S_2)} \Big] \\ &= \frac{1}{2}\big(|0\rangle\langle 0| + |1\rangle\langle 1| \big) = \frac{1}{2}\mathbb{1}. \end{aligned} \tag{2.42}$$

Conversely, the idea of *purification* allows us to *extend* the state space of a mixed state in order to write it as a pure state.

One might ask if there is any reason, or intuitive explanation as to why we should take a composite system to have this tensor product form. One argument comes from the postulated linearity of the theory. Each component system is, in its own right, a valid quantum system, and therefore subject to the linear rules of quantum mechanics, meaning we require the entire composite system to have a multilinear (linear in each component) structure. The tensor product does indeed have this feature. That being said, this is by no means a complete justification, there are plenty of other multilinear structures out there, but it at least gives us some intuition as to why we make the choice that we do. There has been some work into showing that the tensor product structure is the only choice consistent with the other postulates, which would thereby demote it from its status as a postulate [28], but we do not delve into the details of that here.

2.2.3 Evolution

The third postulate tells us how the state of a *closed* quantum system evolves over time.

> **Postulate 3**
> The evolution of a *closed* quantum system is described by a *unitary transformation.*

Suppose $|\psi(t)\rangle$ is the state of a quantum system at time t, then the state at time t' is given by

$$|\psi(t')\rangle = U_{t't}|\psi(t)\rangle, \tag{2.43}$$

for some unitary linear operator $U_{t't}$ that depends only on the two times t, t'. In density operator form, if $\rho(t)$ is the state of a closed quantum system at time t, then its state at time t' is given by

$$\rho(t') = V_{t't}\rho(t)V_{t't}^\dagger, \tag{2.44}$$

for some unitary linear operator $V_{t't}$ that depends only on the two times t, t'. From here on, we will not explicitly include the time dependence.

Some useful unitaries

Let's write down some unitary operators that are ubiquitous in this work. We will sometimes write these down in multiple forms: matrix form, bra-ket form or in terms of other unitaries. Unless stated otherwise, the basis that we work in is the computational basis, that is, the eigenbasis of σ_z, written in Eq. (2.29). We also relate them to the quantum circuit model, which is a useful way of representing situations where sequences of (unitary) operations are carried out, for instance, during a quantum algorithm. In the language of quantum circuits, we call unitaries *quantum gates*, taking our lead from the circuit model of classical computers. Depending on the context, we will use the following terms interchangeably: gate, unitary operator, unitary matrix, or just unitary.

Let's begin with some single-qubit unitaries, that is, unitary operators acting on a single qubit. Such operators belong to the set U(2). So, let's first write down (again) the Pauli operators in both matrix and

bra-ket form

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \tag{2.45a}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|, \tag{2.45b}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{2.45c}$$

and as gates, shown in Fig. 2.2. In the circuit model, each line represents a qubit, and we can think of the

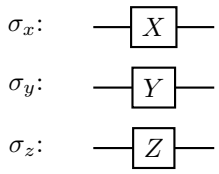

Figure 2.2: The Pauli operators represented as quantum gates.

state(s) being acted on by our operators as moving along these lines from left to right. In this work, we will usually label each of these lines with the qubits they represent. These Pauli gates are exceptions to the rule of how we, in this work, will write single qubit unitaries as quantum gates. Normally, for some single-qubit unitary U, Fig. 2.3 shows how we would represent it as a quantum gate.

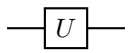

Figure 2.3: Circuit representation of a single-qubit unitary U.

Related to the Pauli operators are the rotation operators associated with them. Given a Pauli operator σ_w, for $w \in \{x, y, z\}$, and recalling that qubits can be thought of as points of the Bloch sphere, the rotation operator $R_W(\theta)$, for $W \in \{X, Y, Z\}$, rotates a qubit around the w axis of the Bloch sphere by θ. They have the form

$$R_W(\theta) := e^{-i\theta\sigma_w/2} = \cos\frac{\theta}{2}\mathbb{1} - i\sin\frac{\theta}{2}\sigma_w, \tag{2.46}$$

or, as matrices,

$$R_X(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{2.47a}$$

$$R_Y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{2.47b}$$

$$R_Z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}. \tag{2.47c}$$

A similar operation to the z-rotation (equivalent up to a phase), is called the phase gate, and is defined (in matrix form), as

$$P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}. \tag{2.48}$$

Although it is equivalent to $R_Z(\theta)$, we introduce it here as we use it in our later circuits. Indeed, we use it as a *controlled* operation (a concept we cover shortly), which makes it inequivalent to its controlled $R_Z(\theta)$ counterpart.

The last single qubit unitary we will write down here is the Hadamard operator H, which changes between the Pauli x and z-(eigen)bases. In terms of σ_x and σ_z, it can be written as

$$H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z), \tag{2.49}$$

or in matrix form, as

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.50}$$

Indeed, we can change between any orthonormal bases using a unitary operator, but the Hadamard matrix is particularly useful to us since the we use the Pauli x and z-bases so heavily.

We don't have to stop at single qubit unitaries. For example, there is a class of two-qubit operations called *controlled* operations. They work by taking in a state made up of a *control* qubit Q_c and a *target* qubit Q_t before carrying out some unitary $V \in \mathrm{U}(2)$ on the target, conditioned on the control qubit being in the state $|1\rangle^{Q_c}$. We will call the operator of this situation a controlled-V operator and denote it as $U_{CV}^{Q_cQ_t}$ or U_{CV} for simplicity. We can write it mathematically as

$$U_{CV}^{Q_cQ_t} = |0\rangle\langle 0|^{Q_c} \otimes \mathbb{1}^{Q_t} + |1\rangle\langle 1|^{Q_c} \otimes V^{Q_t}, \tag{2.51}$$

where we have included the systems to make it clear the role of the control and target qubits. We represent such a controlled-V operation as a gate as shown in Fig. 2.4, where Q_t and Q_c indicate where the target and control qubit states are input respectively.

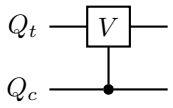

Figure 2.4: Circuit representation of a controlled-V operator U_{CV}.

One controlled-unitary operation is important enough to receive its own name and gate symbol. Namely, the controlled-σ_x, which we call the controlled-NOT or CNOT gate. Indeed, we sometimes call the σ_x operation a NOT gate in analogy to the classical NOT gate that switches a bit value of 0 with a value of 1. This is because, when working in the computational basis (the z-basis), $\sigma_x|0\rangle = |1\rangle$ and $\sigma_x|1\rangle = |0\rangle$. The corresponding unitary U_{CNOT} can be written as a matrix as follows

$$U_{\mathrm{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.52}$$

and is represented as a gate in a circuit as shown in Fig. 2.5. Note that this allows for the creation of

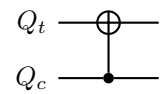

Figure 2.5: Circuit representation of the CNOT (controlled-σ_x) gate.

entangled states from separable ones. Consider the circuit in Fig. 2.6, if we input a state $|00\rangle^{Q_cQ_t}$ to this circuit, then we get the Bell state $|\Phi^+\rangle^{Q_cQ_t}$ out of it. This can be seen explicitly as follows:

$$|00\rangle^{Q_c,Q_t} \xrightarrow{H} \frac{1}{\sqrt{2}}\big(|00\rangle^{Q_cQ_t} + |10\rangle^{Q_cQ_t}\big) \xrightarrow{\mathrm{CNOT}} \frac{1}{\sqrt{2}}\big(|00\rangle^{Q_cQ_t} + |11\rangle^{Q_cQ_t}\big) = |\Phi^+\rangle^{Q_cQ_t}. \tag{2.53}$$

The last explicit gate we'll mention in this subsection is the Tofolli gate, which is a three qubit gate with two control qubits. It is shown in Fig. 2.7. The way it acts is by performing a σ_x operation on the qubit Q_0 *only* when Q_1, Q_2 are *both* in the state $|1\rangle$.

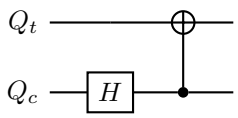

Figure 2.6: Circuit representation of the CNOT (controlled-σ_x) gate.

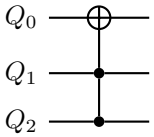

Figure 2.7: Circuit representation of the Toffoli gate.

Non-unitary evolution and quantum operations

It will often be the case that the systems we work with undergo non-unitary evolution. One might wonder why this doesn't contradict the postulate of this section. The reason is that we are often not dealing with a closed system, for instance, if we measure a quantum system[10], some extra measurement-device-system *interacts* with it in order to extract information *from* it. In other words, the system we are interested in is often not isolated from others. If we were to zoom out and include everything in our system (all the other interacting parties etc), unitary evolution would be recovered. However, this is usually unfeasible, so we should write down the rules of how a system evolves when we ignore its (possibly interacting) surroundings.

Suppose the state ρ of a system S evolves according to some linear map, that we call a quantum operation[11], $\mathcal{E} : \mathcal{L}\big(\mathcal{H}^S\big) \to \mathcal{L}\big(\mathcal{H}^{S'}\big)$,

$$\rho \mapsto \rho' = \mathcal{E}(\rho), \tag{2.54}$$

then what properties must $\mathcal{E}$ have? Before we figure this out, let us make what we said in the previous paragraph slightly more precise. It was remarked that if we were to consider the entire, closed system of this situation, the evolution of the state of this whole system would be unitary. Suppose this closed system is the composite system SE, made up of the system we are interested in, S, along with some environment E. Next, assume that, initially, the state of SE is $\tilde{\rho} = \rho \otimes \rho_{\text{env}}$, where "env" stands for "environment". This means we are assuming that when the system S is first prepared in the state ρ, it is totally separate and uncorrelated with the environment E[12]. With all of this, we can think of $\mathcal{E}$ as resulting from the action of some unitary $U_{\mathcal{E}}$ on the state $\tilde{\rho}$ of the entire, closed system SE, before tracing out (and therefore ignoring) the environment:

$$\mathcal{E}(\rho) = \text{Tr}_E \left(U_{\mathcal{E}} \tilde{\rho} \, U_{\mathcal{E}}^\dagger \right). \tag{2.55}$$

So, zooming back into our quantum systems of interest, we can define quantum operations axiomatically. Before we do so, however, we should define a *completely-positive (CP) map*. Take our map $\mathcal{E} : \mathcal{L}\big(\mathcal{H}^S\big) \to \mathcal{L}\big(\mathcal{H}^{S'}\big)$, for instance. It is *positive* if, for any positive operator $\Gamma \in \mathcal{L}\big(\mathcal{H}^S\big)$, $\mathcal{E}(\Gamma) \geq 0$. It is *completely-positive* if, on top of positivity, when we add any arbitrary quantum system B, the map $\mathcal{E}^{(S)} \otimes \mathcal{I}^{(B)} : \mathcal{L}\big(\mathcal{H}^{SB}\big) \to \mathcal{L}\big(\mathcal{H}^{S'B'}\big)$ is also positive, where $\mathcal{I}$ denotes the idenity map. We can now define a quantum operation.

A quantum operation is a map $\mathcal{E} : \mathcal{L}\big(\mathcal{H}^S\big) \to \mathcal{L}\big(\mathcal{H}^{S'}\big)$ satisfying the following three conditions:

1. For any density operator $\rho \in \mathcal{L}\big(\mathcal{H}^S\big)$, $\text{Tr}\, \mathcal{E}(\rho) \in [0, 1]$.

[10] More on quantum measurement in the next postulate.

[11] Note that the input and output systems need not be the same.

[12] This assumption isn't totally in keeping with the physical world. It is impossible to totally separate the state of one system from another, there will always be some correlations. Nevertheless, it is good enough for us, as we are only aiming to gain some intuition about the situation.

2. It is *convex-linear*. That is, for any convex combination of density operators $\sum_i p_i \rho_i$,

$$\mathcal{E}\Big(\sum_i p_i \rho_i\Big) = \sum_i p_i \mathcal{E}(\rho_i).$$

3. It is completely-positive.

One particularly important class of quantum operations are called *quantum channels*. These are subject to the additional constraint that they are *trace-preserving*, that is, $\mathcal{E}_c : \mathcal{L}\big(\mathcal{H}^S\big) \to \mathcal{L}\big(\mathcal{H}^{S'}\big)$ is a quantum channel, if it is a quantum operation and, for any density operator $\rho \in \mathcal{L}\big(\mathcal{H}^S\big)$, $\operatorname{Tr} \mathcal{E}_c(\rho) = 1$. Therefore, quantum channels are often called *completely-positive trace-preserving (CPTP)* maps, with the linearity of them implicitly assumed.

An alternative, but equivalent, way of describing a quantum operation $\mathcal{E}$ mathematically is to use a set of operators $\{E_i\}$ called Kraus operators, named after K. Kraus who first noted this equivalence [29, 30]. As before, let ρ be a density operator in the input space of $\mathcal{E}$, then there exists a set of operators $\{E_i\}$, subject to

$$\sum_i E_i^\dagger E_i \leq \mathbb{I}, \tag{2.56}$$

that allow us to write

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger. \tag{2.57}$$

Being a sum of positive operators, the condition in Eq. (2.56) corresponds to the first axiom of quantum operations: $\operatorname{Tr} \mathcal{E}(\rho) \in [0, 1]$. If $\mathcal{E}$ is CPTP (i.e. a quantum channel), then this condition becomes an equality. We will primarily use this representation of quantum operations, that we call the Kraus representation.

Examples of quantum operations

Before moving on, let's consider some examples of quantum operations to gain some intuition, and become acquainted with the Kraus representation. First, we can describe unitary evolution in this formalism. We saw earlier that a density operator ρ evolves as $\rho \mapsto U\rho U^\dagger$ for some unitary operator U. In our new language, we can define the corresponding quantum operation as

$$\mathcal{U}(\rho) = U\rho U^\dagger, \tag{2.58}$$

from which we can see there is just one Kraus operator: U. Further, this operation is trace-preserving since Eq. (2.56) in this scenario is $U^\dagger U = \mathbb{I}$ (as U is unitary).

Another example is that of Pauli channels [31]. In general, a Pauli channel $\mathcal{P} : \mathcal{L}(\mathcal{H}_{\text{qubit}}) \to \mathcal{L}(\mathcal{H}_{\text{qubit}})$, maps qubit states to qubit states as follows

$$\mathcal{P}(\rho) = p_0\rho + p_x\sigma_x\rho\sigma_x^\dagger + p_y\sigma_y\rho\sigma_y^\dagger + p_z\sigma_z\rho\sigma_z^\dagger, \tag{2.59}$$

for any density operator $\rho \in \mathcal{L}(\mathcal{H}_{\text{qubit}})$, such that $p_0 + p_x + p_y + p_z = 1,\ p_i \geq 0$. So, in this case, the set of Kraus operators is $\{\sqrt{p_0}\mathbb{1}, \sqrt{p_x}\sigma_x, \sqrt{p_y}\sigma_y, \sqrt{p_z}\sigma_z\}$, and, as the name suggests, Pauli channels are trace preserving, since

$$p_0\mathbb{1}^\dagger\mathbb{1} + p_x\sigma_x^\dagger\sigma_x + p_y\sigma_y^\dagger\sigma_y + p_z\sigma_z^\dagger\sigma_z = (p_0 + p_x + p_y + p_z)\mathbb{1} = \mathbb{1}. \tag{2.60}$$

We can go further with this Pauli channel example and see how it can be represented as a unitary operator on some larger state space. In doing so, we get to use some of the other ideas and techniques of this section. For simplicity, let's take $p_0 = p_x = 1/2$ and $p_y = p_z = 0$, and suppose the initial state of the system S is the pure state $\rho_\psi = |\psi\rangle\langle\psi|$. Then to achieve the operation

$$\tilde{\mathcal{P}}(\rho_\psi) = \frac{1}{2}\rho_\psi + \frac{1}{2}\sigma_x\rho_\psi\sigma_x^\dagger, \tag{2.61}$$

we, first, extend our system to one of two qubits, with Hilbert space $\mathcal{H}^S_{\text{qubit}} \otimes \mathcal{H}^E_{\text{qubit}}$ and prepare the additional system E in the state $|0\rangle^E$. Then, let's perform the unitary represented by the circuit in Fig. 2.8. This updates the state of the extended system as follows

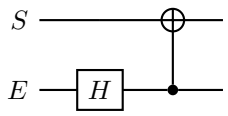

Figure 2.8: Unitary on extended state space.

$$|\Gamma_{\mathrm{i}}\rangle^{SE} := |\psi\rangle^S \otimes |0\rangle^E \mapsto |\Gamma_{\mathrm{f}}\rangle^{SE} := \frac{1}{\sqrt{2}}\Big(|\psi\rangle^S \otimes |0\rangle^E + \sigma_x|\psi\rangle^S \otimes |1\rangle^E\Big). \tag{2.62}$$

Following Eq. (2.55), if we take $\Gamma_{\mathrm{f}}^{SE} := |\Gamma_{\mathrm{f}}\rangle\langle\Gamma_{\mathrm{f}}|^{SE}$, and trace out the extra system E, we obtain the results of the Pauli channel $\tilde{\mathcal{P}}$:

$$\mathrm{Tr}_E\left(\Gamma_{\mathrm{f}}^{SE}\right) = \frac{1}{2}\rho_\psi + \frac{1}{2}\sigma_x\rho_\psi\sigma_x^\dagger. \tag{2.63}$$

2.2.4 Interlude: classical probability and information

Before continuing on with the postulates, we briefly state some ideas from classical probability and information theory that we use in this work, following Ref. [22]. Suppose A is some event with possible outcomes $\{a_i\}$. We write the probability of a_i occurring as $P(a_i)$, such that $P(a_i) \in [0,1]$ and $\sum_i P(a_i) = 1$. Now, suppose another event B has possible outcomes $\{b_j\}$, then the probability of a_i *and* b_j occurring is written as $P(a_i, b_j)$. We can recover the probability of each of these outcomes occurring separately using

$$P(a_i) = \sum_j P(a_i, b_j), \tag{2.64a}$$

$$P(b_j) = \sum_i P(a_i, b_j). \tag{2.64b}$$

If the events A, B are independent from one another, $P(a_i, b_j) = P(a_i)P(b_j)$, else, they are related as follows:

$$P(a_i, b_j) = P(b_j|a_i)P(a_i), \tag{2.65a}$$

$$P(a_i, b_j) = P(a_i|b_j)P(b_j). \tag{2.65b}$$

Here, $P(a_i|b_j)$ denotes a *conditional probability* and corresponds to the *probability of obtaining the outcome a_i given that the outcome of B was b_j* [and similarly for $P(b_j|a_i)$]. From these two equations, we can write down Bayes' theorem:

$$P(a_i|b_j) = \frac{P(b_j|a_i)P(a_i)}{P(b_j)}. \tag{2.66}$$

The information associated with an event A with outcomes $\{a_i\}$ is given by

$$H(A) = -\sum_i P(a_i)\log P(a_i), \tag{2.67}$$

where we will use $\log \equiv \log_2$ throughout. One situation to note is that of a two-outcome event. Suppose an event A has possible outcomes $\{a_0, a_1\}$ such that $P(a_0) = p \in [0,1]$, and thus $P(a_1) = 1 - p$. Then the *binary entropy* is denoted by $h(p)$:

$$h(p) = -p\log p - (1-p)\log(1-p). \tag{2.68}$$

Lastly, again, without going into any detail, the mutual information between two events A, B with respective outcomes $\{a_i\}, \{b_j\}$ is given by

$$H(A:B) = H(A) + H(B) - H(A,B), \tag{2.69}$$

where

$$H(A,B) = -\sum_{i,j} P(a_i, b_j)\log P(a_j, b_j) \tag{2.70}$$

is the information associated with the events A *and* B.

2.2.5 Measurement in quantum mechanics

The final postulate describes how information about a quantum system is extracted, via the process of quantum measurement, and what happens to the state of the system when we do so. We deviate slightly from Ref. [17] when writing down this postulate.

> **Postulate 3**
> A quantum measurement on a quantum system S is described by a set of quantum operations $\mathcal{M} = \{\mathcal{M}_m : \mathcal{L}(\mathcal{H}^S) \to \mathcal{L}(\mathcal{H}^{S'})\}$, such that $\sum_m \mathcal{M}_m$ is CPTP. Each possible outcome of the measurement is given by the index m of the corresponding quantum operation $\mathcal{M}_m$, and the probability of obtaining a measurement outcome m, given that S was prepared in the state ρ, is given by the (generalised) Born rule: $P(m|\rho) = \operatorname{Tr} \mathcal{M}_m(\rho)$.

We call $\mathcal{M}$ a quantum instrument [12, 32], and $\mathcal{M}$ is a sufficiently general description of a quantum measurement to, not only produce the relevant measurement statistics, but also describe how the state of the system changes during such a measurement. That is, if a measurement (described by $\mathcal{M}$) is performed and an outcome of m obtained, then if the state of the system immediately prior to the measurement is $\rho \in \mathcal{L}(\mathcal{H}^S)$, it updates as follows:

$$\rho \mapsto \frac{\mathcal{M}_m(\rho)}{\operatorname{Tr} \mathcal{M}_m(\rho)}. \tag{2.71}$$

If the measurement is performed but the outcome unknown, the state of the system is updated as

$$\rho \mapsto \sum_m \mathcal{M}_m(\rho). \tag{2.72}$$

This description of a quantum measurement can be rewritten in the Kraus representation. That is, for each outcome m of $\mathcal{M}$, the corresponding operation $\mathcal{M}_m$ can be decomposed as follows:

$$\mathcal{M}_m(\rho) = \sum_i M_i^{(m)} \rho M_i^{(m)\dagger}, \tag{2.73}$$

such that the Kraus operators $\{M_i^{(m)}\}$ satisfy

$$\sum_{i,m} M_i^{(m)\dagger} M_i^{(m)} = \mathbb{I}. \tag{2.74}$$

This corresponds to the requirement that $\sum_m \mathcal{M}_m$ be CPTP in order to ensure that the probabilities $P(m|\rho) = \operatorname{Tr} \mathcal{M}_m(\rho)$ sum to unity. If this wasn't the case, there would be some other possible outcome unaccounted for. Note that it follows that

$$\sum_i M_i^{(m)\dagger} M_i^{(m)} \leq \mathbb{I}, \tag{2.75}$$

which corresponds to the definition of a quantum operation, as we'd hope since $\mathcal{M}_m$ is one.

In the circuit picture, a measurement on some system S is represented as shown in Fig. 2.9. In this thesis

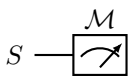

Figure 2.9: Circuit representation of a measurement $\mathcal{M}$.

we will not normally need the full generality of quantum instruments, so let us consider some specific classes of quantum measurements.

Projective measurements and observables

In the original axiomatic formulations of quantum mechanics, this measurement postulate was formulated in terms of *observables*, which are the properties of quantum systems one might hope to access information about, for example position, momentum, spin etc. It was postulated that such observables are represented by Hermitian operators (really self-adjoint operators, which for our finite-dimensional purposes, are the same thing). Suppose $\mathcal{O}_A$ is an observable of a quantum system S, such that it is represented by the Hermitian operator A. In this framework, if someone were to measure this observable $\mathcal{O}_A$ of S, then the possible outcomes of this measurement correspond to the eigenvalues $\{\lambda_i\}$ of A. This gives us some intuition behind the choice of *Hermitian operators* to represent observables. Namely, their eigenvalues are real, which is a quality we'd hope for in our measurement outcomes.

Now, to find out the probability of measuring an outcome λ_i, note that, since A is a Hermitian operator, it has a complete[13] orthonormal set of eigenvectors $\{|\lambda_i\rangle\}$. The Born rule then gives us the probability of obtaining λ_i when measuring a system S, initially in the state ρ:

$$P(\lambda_i|\rho) = \langle\lambda_i|\rho|\lambda_i\rangle = \mathrm{Tr}(|\lambda_i\rangle\langle\lambda_i|\rho). \tag{2.76}$$

Further, having measured the outcome λ_i, the state of the system *"collapses"* to the corresponding eigenstate:

$$\rho \mapsto |\lambda_i\rangle\langle\lambda_i|. \tag{2.77}$$

It is from this discussion of observables, particularly in relation to the orthogonality of eigenstates of the corresponding operator, that we define a projective measurement. In what follows, we will assume the system we are measuring is given by S and has the associated Hilbert space $\mathcal{H}$. A projective measurement [or a projection-valued measure (PVM)] is a set of operators $\Pi_{\mathrm{PVM}} = \{P_j\} \subset \mathcal{L}(\mathcal{H})$ satisfying

$$P_j \geq 0, \ \forall j \tag{2.78a}$$

$$\sum_j P_j = \mathbb{I}, \tag{2.78b}$$

$$P_j P_k = \delta_{jk} P_j, \ \forall j,k. \tag{2.78c}$$

Here, just as an eigenstate $|\lambda_i\rangle\langle\lambda_i|$ corresponded to a measurement outcome of λ_i[14], each *projector* P_j, corresponds to the outcome j of the measurement described by Π_{PVM}. Indeed, given a system prepared in the state ρ, the probability of obtaining a measurement outcome j is once again given by the Born rule:

$$P(j|\rho) = \mathrm{Tr}(P_j\rho). \tag{2.79}$$

Similarly, due to the orthogonality of the elements of Π_{PVM}, if we get an outcome j, the state of the system is postulated to be updated as follows [33, 34]:

$$\rho \mapsto \frac{P_j \rho P_j^\dagger}{\mathrm{Tr}(P_j\rho)}, \tag{2.80}$$

and, in the event that we do not know the outcome of the measurement,

$$\rho \mapsto \sum_j P_j \rho P_j^\dagger. \tag{2.81}$$

Projective measurements are related to the quantum instruments above in that each quantum operation $\mathcal{M}_m$ is described by a *single* Kraus operator P_m.

The first two conditions [Eq. (2.78a,b)] in the definition of a PVM are well motivated physically. With the help of Eq. (2.79), we can see that the requirement that projectors be positive comes from the requirement of probabilities being positive. Further, the completness condition [Eq. (2.78b)] ensures the measurement probabilities sum to one. Having said this, there is no clear reason as to why the third condition, Eq. (2.78c), should be true. This leads us to our next class of quantum measurements: positive operator-valued measures (POVMs).

[13] In the sense of Eq. (2.10).

[14] Ignoring some intricacies to do with degenerate eigenvalues.

Positive operator-valued measures (POVMs)

A POVM is a set of operators $\Pi_{\text{POVM}} = \{\pi_i\} \subset \mathcal{L}(\mathcal{H})$ satisfying the following

$$\pi_i \geq 0, \ \forall i \tag{2.82a}$$

$$\sum_i \pi_i = \mathbb{I}. \tag{2.82b}$$

An alternate way of expressing the positivity of an operator $A \in \mathcal{L}(\mathcal{H})$ is as follows:

$$A \geq 0 \iff \langle\psi|A|\psi\rangle \geq 0, \ \forall|\psi\rangle \in \mathcal{H}. \tag{2.83}$$

A POVM can be used to describe the measurement of a system S, such that we associate the operator (or POVM element, as we will often call it) π_i with the measurement outcome i. Similarly to the PVM case, given a system prepared in the state ρ, the probability of obtaining an outcome i is given by

$$P(i|\rho) = \text{Tr}(\pi_i\rho). \tag{2.84}$$

It turns out that *any* physical measurement can be described as a POVM, at least in terms of measurement statistics. What is not included in the POVM formalism, however, is how the state of a system is updated when a measurement is performed on it. In other words, a POVM doesn't care *how* a measurement is performed, it only worries about the probabilities that result from it. So, when using a POVM to describe a measurement, one has to *choose* how the state updates because of it. The experimental implementation may decide this, but there is one choice that is particularly useful in this work. That is, given a POVM $\{\pi_i\}$ the minimally disturbing measurement is represented by the set of Kraus operators $\{\sqrt{\pi_i}\}$ [34][15]. So, if a measurement outcome of i is obtained when measuring a state ρ,

$$\rho \mapsto \frac{\sqrt{\pi_i}\rho\sqrt{\pi_i}^\dagger}{\text{Tr}(\pi_i\rho)}, \tag{2.85}$$

or, if the outcome is unknown,

$$\rho \mapsto \sum_i \sqrt{\pi_i}\rho\sqrt{\pi_i}^\dagger. \tag{2.86}$$

In this minimally disturbing scenario, we can relate the quantum operations of a quantum instrument to the POVM elements as follows:

$$\mathcal{M}_i(\rho) = \sqrt{\pi_i}\rho\sqrt{\pi_i}^\dagger. \tag{2.87}$$

We can go in the other direction though, that is, start with some quantum instrument $\mathcal{M} = \{\mathcal{M}_m\}$, described by the Kraus operators $\{M_i^{(m)}\}$, and construct a POVM $\{\pi_m\}$. This can be done by defining

$$\pi_m := \sum_i {M_i^{(m)}}^\dagger M_i^{(m)}. \tag{2.88}$$

From this, we can see that the POVM conditions [Eq. (2.82)] are satisfied, and π_m corresponds to the same measurement outcome as $\mathcal{M}_m$.

Physically, it may not be clear how to carry out a POVM. Our intuition about measurement is often linked to physical observables, the measuring of which corresponds to projective measurements. Indeed, current forms of quantum computers access information from the processed quantum states via single qubit (computational basis) projective measurements. So is there any way to carry out, physically, these more abstract measurements in the form of POVMs? The answer, courtesy of Naimark's dilation theorem [35, 36], turns out to be yes. This theorem also gives us the blueprint as to how to do this.

[15] One measure of disturbance is related to the fidelity, which is a measure of how "similar" two states are. For two states ρ, σ, the fidelity between them is given by $F(\rho,\sigma) = \left(\text{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2$. So if a measurement is performed on a state ρ, and the post measurement state is ρ', then one measure of the disturbance caused by this measurement is $D = 1 - F(\rho,\rho')$.

Theorem 2.2.1 (Naimark [36]). *For any POVM $\{\pi_i\}$ on a Hilbert space $\mathcal{H}^S$, there exists a Hilbert space $\mathcal{H}^A$, a pure state $\sigma^A \in \mathcal{L}(\mathcal{H}^A)$, a unitary operation $U \in \mathcal{L}(\mathcal{H}^S \otimes \mathcal{H}^A)$, and a projective measurement $\{P_i\}$ on $\mathcal{H}^A$ such that*

$$\pi_i = Tr_A \Big[(\mathbb{I}^S \otimes \sigma^A)U^\dagger(\mathbb{I}^S \otimes P_i)U\Big]. \tag{2.89}$$

The converse statement is also true.

A proof of this theorem can be found in Ref. [36].

To gain some intuition about this, consider using this theorem to measure some system S, initially in the state $\rho^S \in \mathcal{L}(\mathcal{H}^S)$. In performing the POVM $\{\pi_i\}$, the probability of an outcome i is given by

$$\begin{aligned} P(i) = \mathrm{Tr}(\rho^S \pi_i) &= \mathrm{Tr}_S \left(\rho^S \, \mathrm{Tr}_A \Big[(\mathbb{I}^S \otimes \sigma^A)U^\dagger(\mathbb{I}^S \otimes P_i)U\Big]\right) \\ &= \mathrm{Tr}_{SA} \Big[(\rho^S \otimes \mathbb{I}^A)(\mathbb{I}^S \otimes \sigma^A)U^\dagger(\mathbb{I}^S \otimes P_i)U\Big] \\ &= \mathrm{Tr} \Big[U(\rho^S \otimes \sigma^A)U^\dagger(\mathbb{I}^S \otimes P_i)\Big] \\ &= \mathrm{Tr} \Big[(\mathbb{I}^S \otimes P_i)U(\rho^S \otimes \sigma^A)U^\dagger(\mathbb{I}^S \otimes P_i)\Big], \end{aligned} \tag{2.90}$$

where in the last inequality, we used the fact that $P_i^2 = P_i$. So we can think of carrying out the POVM $\{\pi_i\}$ on a system S, initially in the state ρ^S, by first, extending the system to include some ancilla A, initially in the pure state σ^A:

$$\rho^S \to \rho^S \otimes \sigma^A. \tag{2.91}$$

Following this, we evolve the entire system SA according to the unitary U

$$\rho^S \otimes \sigma^A \to U(\rho^S \otimes \sigma^A)U^\dagger, \tag{2.92}$$

after which a *projective* measurement $\{P_i\}$ on the ancilla system A is performed:

$$U(\rho^S \otimes \sigma^A)U^\dagger \to \sum_i (\mathbb{I}^S \otimes P_i)U(\rho^S \otimes \sigma^A)U^\dagger(\mathbb{I}^S \otimes P_i). \tag{2.93}$$

Naimark's theorem says that there exists a unitary U and a projective measurement $\{P_i\}$ such that the outcome j of $\{P_i\}$, corresponds to the outcome j of the POVM $\{\pi_i\}$. Further, since the only physical measurement is occuring on an ancilla system, the state of the system we are interested in can survive and evolve according to the rules of quantum instruments. The choice of U and $\{P_i\}$ dictate this evolution:

$$\rho^S \to \sum_i \mathrm{Tr}_A \Big[(\mathbb{I}^S \otimes P_i)U(\rho^S \otimes \sigma^A)U^\dagger(\mathbb{I}^S \otimes P_i)\Big]. \tag{2.94}$$

POVMs will be our primary way of describing measurements in this thesis. So let's become better acquainted with them by considering their application to the problem of quantum state discrimination (QSD).

2.2.6 Quantum state discrimination (QSD)

Suppose there is someone, Alice, who prepares a quantum system in one state from the set $\{\rho_i\}$ with probability $\{p_i\}$. If she then sends it to another party, Bob, who knows the possible states, and their respective probabilities of preparation, what measurement should Bob perform to best guess what state he received? This is the problem of quantum state discrimination [37–39]: what measurement $\{\pi_i\}$ (usually a POVM) should we perform to distinguish between the states $\{\rho_i\}$? Of course, it need not be formulated as this game between two parties, quantum state discrimination has far reaching applications in quantum information science, from quantum cryptography [4, 40] to quantum error correction [41].

It is usually the goal to construct a measurement $\{\pi_i\}$ that *optimally* discriminates between the states $\{\rho_i\}$. However, different situations often call for different *figures of merit* when it comes to the optimality of a measurement. Some well studied options are those of unambiguous discrimination [42–44], maximum

confidence [37, 45, 46], or in terms of mutual information [38]. However, we will consider, perhaps the oldest figure of merit: minimum error [47, 48].

Minimum error QSD concerns the minimisation of the probability of misidentifying any of the states. Equivalently, the aim is to maximise the probability of correctly identifying the states. More explicitly, suppose we aim to distinguish between the states in the set $\{\rho_i\}$, such that each state ρ_i is prepared with probability p_i (we will often call p_i priors). Then, in QSD, under the minimum error figure of merit, we aim to find a POVM $\{\pi_i\}$ that minimises

$$P_{\text{error}} = \sum_i \sum_{j\neq i} p_i P(j|\rho_i) = \sum_i \sum_{j\neq i} p_i \operatorname{Tr}(\pi_j \rho_i), \tag{2.95}$$

or equivalently, maximises the rate of a successful classification

$$P_{\text{succ}} = \sum_i p_i P(i|\rho_i) = \sum_i p_i \operatorname{Tr}(\pi_i \rho_i). \tag{2.96}$$

Note that we have described our measurement so that the POVM element π_i corresponds to a measurement outcome i, that says the system was prepared in the state ρ_i. This is why we take the conditional probability $P(i|\rho_i)$ to correspond to the probability of successfully identifying the prepared state to be ρ_i. In this work we will call such a minimum error measurement $\{\pi_i\}$ an optimal measurement, or an optimal POVM, implicitly assuming this is in relation to the minimum error figure of merit.

So how do we find such an optimal POVM? Unfortunately, in general there is no set method[16], but there are conditions that optimal POVMs satisfy [47, 51, 52]. Suppose we are once again presented with the problem of distinguishing the states $\{\rho_i\}$ with corresponding priors $\{p_i\}$. Then the necessary and sufficient conditions that the optimal measurement $\{\pi_i\}$ satisfies are given by

$$\sum_i p_i \rho_i \pi_i - p_j \rho_j \geq 0, \ \forall j, \tag{2.97a}$$

$$\pi_i (p_i \rho_i - p_j \rho_j) \pi_j = 0, \ \forall i, j. \tag{2.97b}$$

This first condition can be shown to be both necessary and sufficient, whilst the second, being consequence of the first, is necessary but not sufficient[17]. The details of the necessity and sufficiency of these conditions can be found in Ref. [54]. In this work, we will usually come up with a candidate for an optimal measurement, and use the first condition (which is both necessary and sufficient) to prove its optimality. It should be noted that, in general, the optimal POVM is not unique. For example, and following Ref. [55], consider the problem of discriminating between the qubit states $\rho_0 = |0\rangle\langle 0|, \rho_1 = |1\rangle\langle 1|, \rho_+ = |+\rangle\langle +|, \rho_- = |-\rangle\langle -|$, each prepared with probability 1/4. Then $\{\pi_{0/1} = |0/1\rangle\langle 0/1|, \pi_\pm = 0\}$ and $\{\pi_{0/1} = 0, \pi_\pm = |\pm\rangle\langle \pm|\}$ are both optimal POVMs.

Although there is no general method for finding the optimal measurement in a quantum state discrimination problem, there are certain classes of scenarios that do allow for this [48, 56, 57]. Further, often thanks to properties such as symmetry in the set of possible states $\{\rho_i\}$, there are a range of examples for which the optimal measurement is known [47, 58–63]. Let's briefly consider two of them.

Two pure states

Let $|\psi_0\rangle, |\psi_1\rangle$ be arbitrary (in general, non-orthogonal) pure states of some quantum system prepared with probabilities p_0, p_1 respectively. Our task is to find the optimal POVM $\{\pi_0, \pi_1\}$ that distinguishes between them. To do this, define $\rho_i = |\psi_i\rangle\langle\psi_i|$ for $i = 0, 1$, and let's consult the probability of successfully distinguishing them:

$$P_{\text{succ}} = p_0 \operatorname{Tr}(\rho_0 \pi_0) + p_1 \operatorname{Tr}(\rho_1 \pi_1). \tag{2.98}$$

Using the completeness of $\{\pi_0, \pi_1\}$, note that $\pi_1 = \mathbb{I} - \pi_0$, meaning we can rewrite P_{succ} as

$$P_{\text{succ}} = p_1 + \operatorname{Tr}\left[(p_0\rho_0 - p_1\rho_1)\pi_0\right]. \tag{2.99}$$

[16] At least analytically. There exist methods to do so numerically: namely, semidefinite programming [49, 50].

[17] Highlighted by the (generically) suboptimal POVM $\{\pi_j = \mathbb{I}, \pi_{k\neq j} = 0\}$ satisfying Eq.(2.97b) [53].

We can see from this that, in order to maximise the probability of success, we need to find a π_0 that maximises the trace term in Eq. (2.99). This occurs when π_0 projects the operator $p_0\rho_0 - p_1\rho_1$ onto the eigenspace corresponding to its largest positive eigenvalue. Unless they are equivalent (i.e. differ by some global phase), $|\psi_0\rangle, |\psi_1\rangle$ span a two-dimensional space. So, without loss of generality, we can define an orthonormal basis $\{|a\rangle, |b\rangle\}$ such that

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big(\sqrt{1+|\langle\psi_0|\psi_1\rangle|}|a\rangle + \sqrt{1-|\langle\psi_0|\psi_1\rangle|}|b\rangle\Big), \tag{2.100a}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big(\sqrt{1+|\langle\psi_0|\psi_1\rangle|}|a\rangle - \sqrt{1-|\langle\psi_0|\psi_1\rangle|}|b\rangle\Big). \tag{2.100b}$$

Following some algebra, we find the eigenvalues of $p_0\rho_0 - p_1\rho_1$ to be

$$\lambda_\pm = \frac{1}{2}\big(p_0 - p_1 \pm \sqrt{1-4p_0p_1|\langle\psi_0|\psi_1\rangle|^2}\big), \tag{2.101}$$

with corresponding eigenvectors

$$|\lambda_\pm\rangle = \frac{1}{\sqrt{2}}(|a\rangle \pm |b\rangle). \tag{2.102}$$

Thus, the optimal success rate [found using Eq. (2.99) and the largest eigenvalue λ_+] is [47]:

$$P_{\text{succ}} = \frac{1}{2}\big(1+\sqrt{1-4p_0p_1|\langle\psi_0|\psi_1\rangle|^2}\big), \tag{2.103}$$

which is achieved using

$$\pi_0 = |\lambda_+\rangle\langle\lambda_+|, \tag{2.104a}$$

$$\pi_1 = |\lambda_-\rangle\langle\lambda_-|. \tag{2.104b}$$

Notice that, in this case, the optimal POVM is a projective measurement, which we will sometimes call the Holevo-Helstrom measurement, named after the founders of the conditions in Eq. (2.97) [47, 51]. Note an important feature of quantum state discrimination: *non-orthogonal quantum states cannot be distinguished with certainty.*

Trine states

Our second example illustrates how symmetry in a set of quantum states can act as a guide when constructing our optimal measurement. Suppose we are tasked with distinguishing the following, equiprobable qubit states:

$$|\psi_0\rangle = |0\rangle, \tag{2.105a}$$

$$|\psi_1\rangle = \frac{1}{2}(|0\rangle - \sqrt{3}|1\rangle), \tag{2.105b}$$

$$|\psi_2\rangle = \frac{1}{2}(|0\rangle + \sqrt{3}|1\rangle), \tag{2.105c}$$

where $\{|0\rangle, |1\rangle\}$ is the computational basis defined in Eq. (2.29). These are known as the trine states and note that they are related to one another via the unitary $R_Y(\pi/3)$, defined in Eq. (2.47). It turns out that an optimal measurement shares this symmetry, and is made up of the operators

$$\pi_0 = \frac{2}{3}|0\rangle\langle 0|, \tag{2.106a}$$

$$\pi_1 = \frac{1}{6}(|0\rangle - \sqrt{3}|1\rangle)(\langle 0| - \sqrt{3}\langle 1|), \tag{2.106b}$$

$$\pi_2 = \frac{1}{6}(|0\rangle + \sqrt{3}|1\rangle)(\langle 0| + \sqrt{3}\langle 1|). \tag{2.106c}$$

We can see that, unlike in the case of two pure states, this optimal measurement is a POVM, *but not* a projective measurement (PVM). Indeed it has been noted more generally how useful symmetry can be in constructing an optimal measurement [58, 59]. We will make heavy use of this observation throughout this work.

2.2.7 Semidefinite programming

As we noted, in general, it is a non-trivial task to find an optimal POVM in a QSD problem. A tool that we can use to aid in our efforts, both analytically and numerically is that of semidefinite programming (SDP[18]). Following Ref. [50], in general, a semidefinite program is a constrained optimisation problem in a Hermitian operator variable X. Given a Hermitian operator A, and sets of Hermitian operators $\{B_i\}_{i=1}^m, \{C_j\}_{j=1}^n$, an SDP can be written as follows:

$$\begin{aligned} \max \quad & \mathrm{Tr}(AX) \\ \text{subject to} \quad & \Phi_i(X) = B_i, \quad i = 1, \ldots, m, \\ & \Gamma_j(X) \geq C_j, \quad j = 1, \ldots, n, \end{aligned} \tag{2.107}$$

where Φ_i, Γ_j are Hermiticity preserving linear maps. That is, they are linear and satisfy $\Phi_i(X^\dagger) = \Phi_i^\dagger(X)$, $\Gamma_j(X^\dagger) = \Gamma_j^\dagger(X)$ for any operator X. We call this a *primal* SDP, and associated with is a *dual* SDP corresponding to a minimisation problem. Full details can be found in Refs. [49, 50]

On one hand, the primal and dual programs often allow for analytical values and bounds to be derived for a given optimisation problem. But on the other, there are many efficient numerical approaches known to solve them. Therefore, if a constrained optimisation problem can be formulated as an SDP, there are numerical tools out there to help us find the solution. One such problem is that of quantum state discrimination. Suppose we are tasked with finding a POVM $\{\pi_i\}$ that discriminates between the states $\{\rho_i\}$ with priors $\{p_i\}$, whilst minimising the probability of error (or maximising the probability of success). Then we can formulate this as an SDP as follows:

$$\begin{aligned} \max \quad & P_{\text{succ}} = \sum_i p_i \,\mathrm{Tr}(\pi_i \rho_i) \\ \text{s.t.} \quad & \sum_i \pi_i = \mathbb{I}, \\ & \pi_i \geq 0, \ \forall i, \end{aligned} \tag{2.108}$$

where "s.t." stands for "subject to". In general, being a type of optimisation problem, SDPs are hugely useful throughout quantum information science and beyond, but since we use them sparingly in this work, and only for their numerical qualities, we refer the reader to the aforementioned references for more in depth discussion.

2.3 Groups and representations

In this section we lay out, briefly, the basics of group and representation theory, before going on to discuss an important result for our work: Schur-Weyl duality. We end by briefly introducing the Haar measure. Unless stated otherwise, we follow the following texts [64–68].

2.3.1 Elements of group theory

We begin with the definition of a group.

Definition 2.3.1. *A group is a double $(G, *)$, made up of a set G together with a binary operation $* : G \times G \to G$ satisfying the following three axioms:*

1. *For any $a, b, c \in G$, $a * (b * c) = (a * b) * c$.*
2. *There exists an element $e \in G$ called the identity such that $e * a = a = a * e$, for all $a \in G$.*
3. *For any $a \in G$ there exists a unique inverse element $a^{-1} \in G$ such that $a^{-1} * a = e = a * a^{-1}$.*

[18] We take SDP as an acronym for both semidefinite programming, and semidefinite program.

We will usually call G a group, specifying the group operation only if necessary. Also, unless the binary operation is unclear, we will write $a * b$ as ab, often calling this the product of a and b, or a multiplied by b. Of course, $*$ need not be multiplication in the traditional sense, it could be addition, matrix multiplication or cycle composition, to name a few. Two elements a, b of a group G are said to *commute* if $ab = ba$.

Definition 2.3.2. *Let G be a group. A subset H of G is a subgroup of G, written as $H \leq G$, if it satisfies the following:*

1. $H \neq \varnothing$.
2. $a, b \in H \implies ab \in H$.
3. $a \in H \implies a^{-1} \in H$.

In words, a subgroup H of G is a nonempty subset of G that is a group under the same binary operation as G.

Definition 2.3.3. *For any $H \leq G$ with group operation $*$, and let $g \in G$, a left coset of H in G is the set*

$$gH := \{g * h \ : \ h \in H\}.$$

Likewise, the right coset is $Hg := \{h * g \ : \ h \in H\}$.

It turns out that the set of all left (or right) cosets of H in G forms a partition of G. The reason for this is that left cosets can be thought of equivalence classes with respect to the following equivalence relation on G:

$$g \sim g' \iff g' \in gH, \tag{2.109}$$

for any $g, g' \in G$, and as we saw earlier, the set of equivalence classes forms a partition on the corresponding set.

Definition 2.3.4. *Let $(G, *)$ and $(H, \cdot)$ be groups. A group homomorphism is a map $\varphi : G \to H$ satisfying*

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b),$$

for all $a, b \in G$. If φ is also bijective, we call it an isomorphism and say G and H are isomorphic, written $G \cong H$.

In words, a homomorphism between groups preserves the relationships between group elements.

Examples

There are two examples of groups that are particularly important in this thesis. First, the symmetric group on $\mathbf{n} := \{1, 2, \ldots, n\}$, denoted S_n. This is the group of all possible permutations of the elements in $\mathbf{n}$. We will represent the elements of S_n as *cycles* which can be "multiplied" together via *cycle composition*[19]. For more detail on the symmetric group and cycles, see Ref. [69], but for now, let's just consider the example of S_3 to understand how it works a little better. Being a finite group, we can write S_3 explicitly in terms of its cycles:

$$S_3 = \{e, (12), (23), (13), (123), (132)\}, \tag{2.110}$$

where e is the identity cycle. This group permutes the elements of $\{1, 2, 3\}$. For example if $\sigma = (12)$, then $\sigma(1) = 2,\ \sigma(2) = 1$ and $\sigma(3) = 3$. We can see how the elements of S_3 multiply together (or, more precisely, compose) by consulting the multiplication table (Table 2.1). A subgroup of S_n that we'll use in this work is S_{n-1}, which we take to be the group of permutations of the set $\{1, 2, \ldots, n-1\} \subset \mathbf{n}$.

The second group of importance is the *special unitary group* $\mathrm{SU}(d, \mathbb{C})$, defined in Eq. (2.5) such that the group operation is matrix multiplication. In this thesis, we will exclusively use the $d = 2$ case: $\mathrm{SU}(2) := \mathrm{SU}(2, \mathbb{C})$.

[19] That is, the group operation is cycle composition.

σ	e	(12)	(23)	(13)	(123)	(132)
e	e	(12)	(23)	(13)	(123)	(132)
(12)	(12)	e	(123)	(132)	(23)	(13)
(23)	(23)	(132)	e	(123)	(13)	(12)
(13)	(13)	(123)	(132)	e	(12)	(23)
(123)	(123)	(13)	(12)	(23)	(132)	e
(132)	(132)	(23)	(13)	(12)	e	(123)

Table 2.1: Multiplication table of the group S_3.

2.3.2 Elements of representation theory

Representation theory allows us to express group elements as linear operations.

Definition 2.3.5. *A representation of a group G is a pair $(\mathbf{D}, V)$, such that V is a complex vector space and $\mathbf{D} : G \to GL(V)$ is a group homomorphism.*

The dimension of the representation $(\mathbf{D}, V)$ is given by the dimesnion of the vector space V. As mentioned earlier, we will often have a particular basis in mind when thinking about linear transformations, so we will usually be considering *matrix representations*. In this picture, $\mathbf{D}$ is a group homomorphism that takes elements of G to (invertible) matrices acting on V:

$$g \in G \mapsto \mathbf{D}(g) \in \mathrm{GL}(d, \mathbb{C}), \tag{2.111}$$

where $d = \dim V$.

Definition 2.3.6. *A representation $(\mathbf{D}, V)$ of a group G is called a trivial representation if $\mathbf{D}(g)|v\rangle = |v\rangle$ for all $g \in G$, $|v\rangle \in V$. If this is not the case, we will often call $(\mathbf{D}, V)$ non-trivial.*

If a trivial representation is irreducible (a concept we define later), it is one-dimensional.

Definition 2.3.7. *Two representations $(\mathbf{D}, V), (\mathbf{D}', V')$ of a group G are equivalent if there exists an invertible operator S such that, for every $g \in G$,*

$$\mathbf{D}'(g) = S\mathbf{D}(g)S^{-1}.$$

If this is the case, we use the notation $\mathbf{D}(G) \simeq \mathbf{D}'(G)$.

If $V = V'$, then $\mathbf{D}(G)$ and $\mathbf{D}'(G)$ are related via a change of basis.

Definition 2.3.8. *A representation $(\mathbf{D}, V)$ of G, is a unitary representation if, for every $g \in G$, $\mathbf{D}(g)$ is unitary.*

All of the representations we encounter in this work will be unitary.

Let's consider an example. Suppose our group is S_3 and we hope to construct a representation $(\mathbf{D}, V)$ such that our vector space V is $\mathbb{C}^3$. Then we can write down the elements of $\mathbf{D}(S_3)$ as 3×3 matrices:

$$\begin{aligned}
&\mathbf{D}[e] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{D}[(123)] = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mathbf{D}[(132)] = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \\
&\mathbf{D}[(12)] = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{D}[(23)] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mathbf{D}[(13)] = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.
\end{aligned} \tag{2.112}$$

The fact that this produces the multiplication table in Table 2.1 [with $\sigma \to \mathbf{D}(\sigma)$], confirms that this is a (three-dimensional) representation of S_3.

Reducibility

Of particular importance are irreducible representations (irreps). We define them via the definition of reducible representations.

Definition 2.3.9. *A representation $(\mathbf{D}, V)$ of a group G is called reducible if there exist representations of G, $(\mathbf{D}_1, V_1), (\mathbf{D}_2, V_2)$, where $V_1, V_2 \neq \varnothing$, such that*

$$\mathbf{D}(g) \simeq \mathbf{D}_1(g) \oplus \mathbf{D}_2(g),$$

for all $g \in G$. The spaces $V_1, V_2 \subset V$ are called invariant subspaces with respect to G.[20] A representation is called irreducible if it is not reducible.

In this work, we will reserve lowercase bold letters for irreps, using upper case bold letters otherwise.

We look to Ref. [70] to see how a reducible (matrix) representation decomposes in general. Suppose the set $\hat{G}$ contains the labels λ of every inequivalent irrep $(\mathbf{d}_\lambda, V_\lambda)$ of a group G. Then, for any reducible (matrix) representation $(\mathbf{D}, V)$ of G, and for any $g \in G$,

$$\mathbf{D}(g) \simeq \bigoplus_{\lambda \in \hat{G}} \mathbb{I}_{m_\lambda} \otimes \mathbf{d}_\lambda(g). \tag{2.113}$$

where the two sides of this expression are related via some change of basis. The reason for the m_λ-dimensional identity matrix $\mathbb{I}_{m_\lambda}$ making an appearance here is that a reducible representation can have more than one copy of an irrep: i.e. $m_\lambda \geq 0$ copies[21]. We therefore call m_λ the multiplicity of the irrep $(\mathbf{d}_\lambda, V_\lambda)$. The vector space V decomposes in a similar way, via the same change of basis as in Eq. (2.113):

$$V \cong \bigoplus_{\lambda \in \hat{G}} \mathbb{C}^{m_\lambda} \otimes V_\lambda. \tag{2.114}$$

This block diagonal form hints at a useful fact about invariant subspaces. Namely that the invariant subspaces corresponding to inequivalent irreps are orthogonal to one another. As always, we refer the reader to the aforementioned references for proof of this.

Let's now consider one of the most useful lemmas for this work: Schur's Lemma.

Lemma 2.3.1 (Schur)**.** *Suppose $(\mathbf{d}, V)$ is a d-dimensional irrep of a group G, and let $A \in \mathcal{L}(V)$ be some operator (or $d \times d$ matrix) on V. If*

$$[A, \mathbf{d}(g)] = 0$$

for all $g \in G$, then A is a constant operator (or matrix) on V: $A \propto \mathbb{I}$.

Note that we sometimes use alternate language: if A commutes with $\mathbf{d}(g)$ [or the whole set $\mathbf{d}(G)$], then we often say A is invariant under $\mathbf{d}(g)$ [or $\mathbf{d}(G)$]. Here, we have used the commutator bracket on linear operators:

$$[A, B] := AB - BA, \tag{2.115}$$

such that $A, B \in \mathcal{L}(V)$. There is a similar bracket, called the anticommutator bracket

$$\{A, B\} := AB + BA. \tag{2.116}$$

Using Eq. (2.113), a similar statement about reducible representations can be made. Suppose $(\mathbf{D}, V)$ is a reducible representation of a group G with decomposition given in Eq. (2.113), then

$$[\mathbf{D}(g), A] = 0, \ \forall g \in G \implies A \simeq \bigoplus_{\lambda \in \hat{G}} \Lambda_{m_\lambda} \otimes \mathbb{I}_\lambda, \tag{2.117}$$

where Λ_{m_λ} is some diagonal matrix whose dimension corresponds to the multiplicity m_λ of the irrep $(\mathbf{d}_\lambda, V_\lambda)$, and $\mathbb{I}_\lambda$ denotes the identity on the invariant subspace V_λ. In words, since A commutes with $\mathbf{D}(G)$, there

[20] We may also call them *G-invariant*, or just *invariant*.
[21] When $m_\lambda = 0$, $\mathbb{I}_{m_\lambda} = 0$.

is a basis in which it can be written as the direct sum of constant matrices on each irreducible invariant subspace.

Let's apply Schur's Lemma to an example. Let G be a (finite) group and $(\mathbf{d}, V)$ be an irrep of it. We can take any operator $\rho \in \mathcal{L}(V)$ and turn it into a constant operator by doing the following:

$$\rho \to \sum_{g\in G} \mathbf{d}(g)\,\rho\,\mathbf{d}^\dagger(g). \tag{2.118}$$

Schur's Lemma allows us to see quickly that since the right hand side commutes with $\mathbf{d}(G)$, it must be constant. This mapping allows us to see instantly that the Pauli channel, described in Eq. (2.59), such that $p_i = 1/4$, turns any state ρ into $\mathbb{1}/2$, since it is invariant with respect to the Pauli group[22], indeed an irrep of the Pauli group.

2.3.3 Schur-Weyl duality

Schur-Weyl duality is a result linking the irreducible representations of $\mathrm{SU}(d,\mathbb{C})$ and S_n.[23] In particular, we focus on SU(2) and two-dimensional Hilbert spaces. For $\mathrm{SU}(d,\mathbb{C})$ and d-dimensional vector spaces $\mathbb{C}^d$, we refer the reader to Ref. [70], and for full generality, to Ref. [66].

Consider a composite system of n qubits in an arbitrary pure state:

$$|\xi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle \in \mathcal{H}^{\otimes n}, \tag{2.119}$$

where $\mathcal{H}$ is the Hilbert space associated with a single qubit. If $U \in \mathrm{SU}(2)$, let $\left(\mathbf{Q}^{(n)}, \mathcal{H}^{\otimes n}\right)$ be a representation of SU(2) that acts on $|\xi\rangle$ as follows:

$$\mathbf{Q}^{(n)}(U)|\xi\rangle = U|\psi_1\rangle \otimes U|\psi_2\rangle \otimes \cdots \otimes U|\psi_n\rangle. \tag{2.120}$$

Likewise if $\sigma \in S_n$, let $\left(\mathbf{P}^{(n)}, \mathcal{H}^{\otimes n}\right)$ be a representation of S_n that acts on $|\xi\rangle$ as follows:

$$\mathbf{P}^{(n)}(\sigma)|\xi\rangle = |\psi_{\sigma^{-1}(1)}\rangle \otimes |\psi_{\sigma^{-1}(2)}\rangle \otimes \cdots \otimes |\psi_{\sigma^{-1}(n)}\rangle \tag{2.121}$$

that is, it shuffles the qubits around according to σ. For instance, if $n = 3$ and $\sigma = (123)$, $\mathbf{P}^{(3)}[(123)]|\psi_1\psi_2\psi_3\rangle = |\psi_3\psi_1\psi_2\rangle$. It turns out that $\left(\mathbf{Q}^{(n)}, \mathcal{H}^{\otimes n}\right)$ and $\left(\mathbf{P}^{(n)}, \mathcal{H}^{\otimes n}\right)$ are reducible, so let $(\mathbf{q}_\lambda, \mathcal{Q}_\lambda)$ and $(\mathbf{p}_\mu, \mathcal{P}_\mu)$ be the irreducible representations of SU(2) and S_n respectively. As noted in Eq. (2.113), we can write

$$\mathbf{Q}^{(n)}(U) \simeq \bigoplus_\lambda \mathbb{I}_{m_\lambda} \otimes \mathbf{q}_\lambda(U), \tag{2.122a}$$

$$\mathbf{P}^{(n)}(\sigma) \simeq \bigoplus_\mu \mathbb{I}_{n_\mu} \otimes \mathbf{p}_\mu(\sigma), \tag{2.122b}$$

such that $U \in \mathrm{SU}(2),\ \sigma \in S_n$ are arbitrary, and m_λ, n_μ are the multiplicities of the irreps of SU(2) and S_n respectively.

Now, letting $|\psi_i'\rangle = U|\psi_i\rangle\ \forall i$, since $|\psi_i\rangle \in \mathcal{H}$ were arbitrary,

$$\mathbf{P}^{(n)}(\sigma)\mathbf{Q}^{(n)}(U)|\xi\rangle = \mathbf{P}^{(n)}(\sigma)\left(|\psi_1'\rangle \otimes |\psi_2'\rangle \otimes \cdots \otimes |\psi_n'\rangle\right) \tag{2.123}$$

$$= |\psi'_{\sigma^{-1}(1)}\rangle \otimes |\psi'_{\sigma^{-1}(2)}\rangle \otimes \cdots \otimes |\psi'_{\sigma^{-1}(n)}\rangle \tag{2.124}$$

$$= \mathbf{Q}^{(n)}(U)\left(|\psi_{\sigma^{-1}(1)}\rangle \otimes |\psi_{\sigma^{-1}(2)}\rangle \otimes \cdots \otimes |\psi_{\sigma^{-1}(n)}\rangle\right) = \mathbf{Q}^{(n)}(U)\mathbf{P}^{(n)}(\sigma)|\xi\rangle, \tag{2.125}$$

for all $U \in \mathrm{SU}(2),\ \sigma \in S_n$. So, since $|\xi\rangle$ was arbitrary, it follows that

$$\left[\mathbf{Q}^{(n)}(U), \mathbf{P}^{(n)}(\sigma)\right] = 0, \tag{2.126}$$

[22] The Pauli group is defined as $\{\pm\mathbb{1}, \pm i\mathbb{1}, \pm\sigma_x, \pm i\sigma_x, \pm\sigma_y, \pm i\sigma_y, \pm\sigma_z, \pm i\sigma_z\}$.

[23] Actually, it is not just $\mathrm{SU}(d,\mathbb{C})$, it also covers the group $\mathrm{GL}(d,\mathbb{C})$ and some of its subgroups. However $\mathrm{SU}(d,\mathbb{C})$ is most useful to us.

for all $U \in \mathrm{SU}(2),\ \sigma \in S_n$. Further, the commutant of $\mathbf{Q}^{(n)}[\mathrm{SU}(2)]$ is $\mathbf{P}^{(n)}(S_n)$ and vice versa [66, 70, 71]. It follows from this that

$$\mathbf{Q}^{(n)}(U)\mathbf{P}^{(n)}(\sigma) = \mathbf{P}^{(n)}(\sigma)\mathbf{Q}^{(n)}(U) = \bigoplus_{\lambda} \mathbf{q}_\lambda(U) \otimes \mathbf{p}_\lambda(S_n). \tag{2.127}$$

This direct sum of representations induces the following decomposition of our n-qubit Hilbert space $\mathcal{H}^{\otimes n}$:

$$\mathcal{H}^{\otimes n} \cong \bigoplus_{\lambda} \mathcal{Q}_\lambda \otimes \mathcal{P}_\lambda, \tag{2.128}$$

such that the basis that realises this direct sum is called the Schur basis $\{|\lambda\rangle|q_\lambda\rangle|p_\lambda\rangle\} \subset \mathcal{Q}_\lambda \otimes \mathcal{P}_\lambda$. It follows that the irreps of SU(2) and S_n act on $\mathcal{H}^{\otimes n}$ as follows:

$$\mathbf{q}_{\lambda'}(U)\big(|\lambda\rangle \otimes |q_\lambda\rangle \otimes |p_\lambda\rangle\big) = \delta_{\lambda\lambda'}|\lambda\rangle \otimes \big[\mathbf{q}_\lambda(U)|q_\lambda\rangle\big] \otimes |p_\lambda\rangle, \tag{2.129a}$$

$$\mathbf{p}_{\lambda'}(\sigma)\big(|\lambda\rangle \otimes |q_\lambda\rangle \otimes |p_\lambda\rangle\big) = \delta_{\lambda\lambda'}|\lambda\rangle \otimes |q_\lambda\rangle \otimes \big[\mathbf{p}_\lambda(\sigma)|p_\lambda\rangle\big], \tag{2.129b}$$

for any $U \in \mathrm{SU}(2),\ \sigma \in S_n$.

It turns out that we can use 2-partitions λ of n to simultaneously label irreps of SU(2) and S_n. We can write a 2-partition (or just a partition, as we'll call it from here on) of n as $\lambda = (\lambda_0, \lambda_1)$, such that $\lambda_0 \geq \lambda_1 \geq 0$ and $\lambda_0 + \lambda_1 = n$.[24] For an alternative labelling system, note that, by focusing on SU(2) [rather than SU(d)], we are dealing with the symmetry group of a spin-half particle. This is useful because we can think of our composite system $\mathcal{H}^{\otimes n}$ as a composite system of n spin-half particles. All of this motivates that an alternate way of labelling the irreps of SU(2) and therefore (via Schur-Weyl duality) S_n is with the use of the total spin of a quantum system. Indeed, writing our partitions of n as $\lambda_k = (n-k, k)$, such that $k \leq n/2$, we relate these to the total spin s_k via [72]

$$s_k = \frac{n-2k}{2}. \tag{2.130}$$

So, in this notation,

$$\mathcal{H}^{\otimes n} \cong \bigoplus_{k=0}^{\lfloor n/2 \rfloor} \mathcal{Q}_{s_k} \otimes \mathcal{P}_{s_k}. \tag{2.131}$$

We write the Schur basis as $\{|s_k, m_{s_k}\rangle|p_{s_k}\rangle\}$, where we can think of m_{s_k} as the z-component of the total spin s_k:

$$m_{s_k} \in \{-s_k, -s_k+1, \ldots, s_k\}. \tag{2.132}$$

To make more sense of the Schur basis, let's recall the rules of spin addition of spin-half particles: in particular, $s \otimes \frac{1}{2} \cong \big(s+\frac{1}{2}\big) \oplus \big(s-\frac{1}{2}\big)$. Consider the cases of two, three and four spin half particles:

$$\left(\frac{1}{2}\right)^{\otimes 2} \cong 1 \oplus 0, \tag{2.133a}$$

$$\left(\frac{1}{2}\right)^{\otimes 3} \cong \frac{3}{2} \oplus \frac{1}{2} \oplus \frac{1}{2}, \tag{2.133b}$$

$$\left(\frac{1}{2}\right)^{\otimes 4} \cong 2 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0, \tag{2.133c}$$

respectively. These relations can be calculated iteratively, for example, finding $(1/2)^{\otimes 3}$ using $(1/2)^{\otimes 2}$:

$$\left(\frac{1}{2}\right)^{\otimes 3} = \left(\frac{1}{2}\right)^{\otimes 2} \otimes \frac{1}{2} \cong (1 \oplus 0) \otimes \frac{1}{2} \cong \left[\left(1+\frac{1}{2}\right) \oplus \left(1-\frac{1}{2}\right)\right] \oplus \left(0+\frac{1}{2}\right) \cong \frac{3}{2} \oplus \frac{1}{2} \oplus \frac{1}{2}. \tag{2.134}$$

Figure 2.10 shows a visual representation of this spin addition. These rules come from the Clebsch-Gordan decomposition of the Hilbert space of n spin-half particles, which details how $\mathcal{H}^{\otimes n}$ decomposes into subspaces

[24] Note that, if we were instead considering $\mathrm{SU}(d, \mathbb{C})$, we would consider d-partitions $(\lambda_0, \cdots, \lambda_d)$.

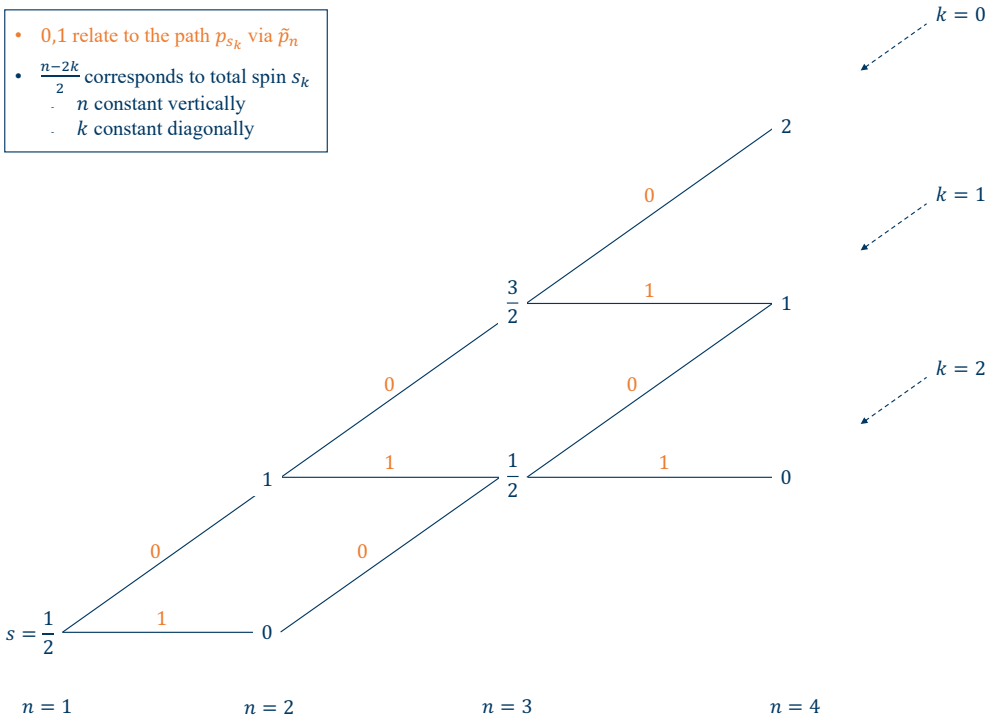

Figure 2.10: Visual representation of the addition of n spin-half particles. Nodes correspond to the total spin s_k of the invariant subspaces and vertices are labelled based on how the n node relates to the $n-1$ node. Note that the number of particles n is constant vertically, while the value k, which relates to the irrep labelling partitions $\lambda_k = (n-k, k)$ or spin s_k, is constant diagonally.

invariant under SU(2) alone. For two, three and four qubits (spin-half particles):

$$\mathcal{H}^{\otimes 2} \cong \mathcal{Q}_1^{(2)} \oplus \mathcal{Q}_0^{(2)}, \tag{2.135a}$$
$$\mathcal{H}^{\otimes 3} \cong \mathcal{Q}_{\frac{3}{2}}^{(3)} \oplus \mathcal{Q}_{\frac{1}{2}}^{(3)} \oplus \mathcal{Q}_{\frac{1}{2}}^{(3)}, \tag{2.135b}$$
$$\mathcal{H}^{\otimes 4} \cong \mathcal{Q}_2^{(4)} \oplus \mathcal{Q}_1^{(4)} \oplus \mathcal{Q}_1^{(4)} \oplus \mathcal{Q}_1^{(4)} \oplus \mathcal{Q}_0^{(4)} \oplus \mathcal{Q}_0^{(4)}, \tag{2.135c}$$

respectively, where we have included the number of qubits n as an index since $\mathcal{Q}_s^{(n)} \neq \mathcal{Q}_s^{(n')}$ for $n \neq n'$.

What Schur-Weyl duality says is that the spaces $\mathcal{Q}_s$ labelled by the same s, are identical in terms of how they are affected by $\mathbf{q}_s[\mathrm{SU}(2)]$, but are orthogonal and only differ by some extra, permutation degree of freedom, sensitive to $\mathbf{p}_s(S_n)$. Once again for the respective cases of two, three and four qubits, Schur-Weyl duality says that

$$\mathcal{H}^{\otimes 2} \cong \left[\mathcal{Q}_1^{(2)} \otimes \mathcal{P}_1^{(2)}\right] \oplus \left[\mathcal{Q}_0^{(2)} \otimes \mathcal{P}_0^{(2)}\right], \tag{2.136a}$$
$$\mathcal{H}^{\otimes 3} \cong \left[\mathcal{Q}_{\frac{3}{2}}^{(3)} \otimes \mathcal{P}_{\frac{3}{2}}^{(3)}\right] \oplus \left[\mathcal{Q}_{\frac{1}{2}}^{(3)} \otimes \mathcal{P}_{\frac{1}{2}}^{(3)}\right], \tag{2.136b}$$
$$\mathcal{H}^{\otimes 4} \cong \left[\mathcal{Q}_2^{(4)} \otimes \mathcal{P}_2^{(4)}\right] \oplus \left[\mathcal{Q}_1^{(4)} \otimes \mathcal{P}_1^{(4)}\right] \oplus \left[\mathcal{Q}_0^{(4)} \otimes \mathcal{P}_0^{(4)}\right]. \tag{2.136c}$$

By comparing this with the multiplicities of the SU(2) subspaces $\mathcal{Q}_s^{(n)}$ in Eq. (2.135), we can quickly see that the dimensions of the corresponding S_n subspaces are $\dim \mathcal{P}_1^{(2)} = \dim \mathcal{P}_0^{(2)} = \dim \mathcal{P}_{\frac{3}{2}}^{(3)} = \dim \mathcal{P}_2^{(4)} = 1$, $\dim \mathcal{P}_{\frac{1}{2}}^{(3)} = \dim \mathcal{P}_0^{(4)} = 2$, and $\dim \mathcal{P}_1^{(4)} = 3$.

By considering spin addition again, there is a natural choice of basis $\left\{\left|p_s^{(n)}\right\rangle\right\}$ for $\mathcal{P}_s$ [72]. Consider the visual representation of spin addition depicted in Fig. 2.10. The values of n correspond to the number of

qubits, and the nodes are labelled by the total spin s_k, and therefore correspond to the SU(2) subspaces $\mathcal{Q}_{s_k}^{(n)}$. The orange numbers are a way of noting which subspace arises from which. Regardless of k, if $s^{(n)} = s^{(n-1)} \pm (1/2)$, then we define the orange numbers by

$$\tilde{p}_n := \frac{1}{2} - s^{(n)} + s^{(n-1)}. \tag{2.137}$$

Now, note that each copy of $\mathcal{Q}_s^{(n)}$ is orthogonal, and each copy arises by traversing a different path in the graph in Fig. 2.10. It follows that, since the multiplicity of $\mathcal{Q}_s^{(n)}$ and therefore the dimension of $\mathcal{P}_s^{(n)}$ is equal to the number of paths by which $\mathcal{Q}_s^{(n)}$ can be reached, we can define an orthogonal basis of $\mathcal{P}_s^{(n)}$ as the set of vectors labelled by the paths to $\mathcal{Q}_s^{(n)}$:

$$\left|p_s^{(n)}\right\rangle := |\tilde{p}_1, \ldots, \tilde{p}_n\rangle. \tag{2.138}$$

We will often call the S_n component of vectors, states, spaces etc the path component due to this interpretation. For example, consulting Fig. 2.10 for guidance. We can define a basis for the three-dimensional space $\mathcal{P}_1^{(4)}$ using the vectors:

$$|0\rangle_{\mathcal{P}_1^{(4)}} = |0,0,0,1\rangle, \tag{2.139a}$$

$$|1\rangle_{\mathcal{P}_1^{(4)}} = |0,0,1,0\rangle, \tag{2.139b}$$

$$|2\rangle_{\mathcal{P}_1^{(4)}} = |0,1,0,0\rangle, \tag{2.139c}$$

corresponding to the top, middle and bottom paths to $\mathcal{Q}_1^{(4)}$ respectively. Note that we have included an extra 0 at the start. This is because the one-particle spin-half space has a one-dimensional subspace $\mathcal{P}_{1/2}^{(1)}$ attached, whose basis we define as $\left\{|0\rangle_{\mathcal{P}_{1/2}^{(1)}}\right\}$. We will usually omit the subscripts labelling the S_n subspace as these path vectors will always be attached to an irrep-labelling vector $|s_k\rangle$ or $|\lambda_k\rangle$. Further, the number of qubits will normally be clear by context.

Thinking in terms of spin has been invaluable for gaining intuition about Schur-Weyl duality. It should be noted however that we will work, both in terms of spin s_k *and* partitions λ_k. Before moving on, let's write down expressions for the dimension of the invariant subspaces $\mathcal{Q}_{s_k}^{(n)}, \mathcal{P}_{s_k}^{(n)}$. First, the dimension of $\mathcal{Q}_{s_k}^{(n)}$ (equivalently $\mathcal{Q}_{\lambda_k}^{(n)}$) can be found using the fact that the dimension of the space associated with a spin-s particle is given by $d = 2s + 1$. Therefore, recalling Eq. (2.130) that relates λ_k with s_k,

$$\dim \mathcal{Q}_{s_k}^{(n)} \equiv \dim \mathcal{Q}_{\lambda_k}^{(n)} = n - 2k + 1. \tag{2.140}$$

Slightly more involved is the dimension of $\mathcal{P}_{s_k}^{(n)}$ $\left[\text{equivalently } \mathcal{P}_{\lambda_k}^{(n)}\right]$, which is

$$\dim \mathcal{P}_{s_k}^{(n)} \equiv \dim \mathcal{P}_{\lambda_k}^{(n)} = \binom{n}{k} \frac{n-2k+1}{n-k+1}. \tag{2.141}$$

We refer the reader to Refs. [71, 73] for the derivation of this. We can at least be reassured by the sight of the combinatorial factor ${}^nC_k$ since the number of paths in Fig. 2.10 to a subspace $\mathcal{Q}_{\lambda_k}^{(n)}$ is related to the number k of horizontal steps in the n-step path (including the trivial step to the initial qubit).

Two and three-qubit Schur bases

Let's write down, explicitly, the[25] Schur bases of the Hilbert spaces associated with two particularly important systems in this work: a two and three-qubit system. First, the Schur basis (that we use) for the two-qubit Hilbert space,

$$\mathcal{H}^{\otimes 2} \cong \left[\mathcal{Q}_1^{(2)} \otimes \mathcal{P}_1^{(2)}\right] \oplus \left[\mathcal{Q}_0^{(2)} \otimes \mathcal{P}_0^{(2)}\right], \tag{2.142}$$

[25] We say "the", but in general, the Schur basis in not unique. As with any multi-dimensional vector subspace, there is a choice of bases. This choice is strictly within each invariant subspace though, else the direct-sum-form of the whole space would be destroyed.

is given by

$$\begin{aligned}
\mathcal{Q}_1^{(2)} \otimes \mathcal{P}_1^{(2)} : \;& |1,1\rangle = |00\rangle, \\
& |1,0\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\
& |1,-1\rangle = |11\rangle, \\
\mathcal{Q}_0^{(2)} \otimes \mathcal{P}_0^{(2)} : \;& |0,0\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),
\end{aligned} \tag{2.143}$$

where the right hand side is written in the computational basis. Recall that, in the spin picture, the second component in the kets on the left hand side correspond to m_s, the z-component of the spin s. Note the lack of a path component $|p_{0/1}\rangle$. We will often omit $|p_s\rangle$ if the corresponding subspace $\mathcal{P}_s$ is one-dimensional.

Likewise, the Schur basis (that we will use) of the three-qubit Hilbert space,

$$\mathcal{H}^{\otimes 3} \cong \left[\mathcal{Q}_{\frac{3}{2}}^{(3)} \otimes \mathcal{P}_{\frac{3}{2}}^{(3)}\right] \oplus \left[\mathcal{Q}_{\frac{1}{2}}^{(3)} \otimes \mathcal{P}_{\frac{1}{2}}^{(3)}\right], \tag{2.144}$$

is given by

$$\begin{aligned}
\mathcal{Q}_{\frac{3}{2}}^{(3)} \otimes \mathcal{P}_{\frac{3}{2}}^{(3)} : \;& \left|\frac{3}{2},\frac{3}{2}\right\rangle = |000\rangle, \\
& \left|\frac{3}{2},\frac{1}{2}\right\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle), \\
& \left|\frac{3}{2},-\frac{1}{2}\right\rangle = \frac{1}{\sqrt{3}}(|011\rangle + |101\rangle + |011\rangle), \\
& \left|\frac{3}{2},-\frac{3}{2}\right\rangle = |111\rangle, \\
\mathcal{Q}_{\frac{1}{2}}^{(3)} \otimes \mathcal{P}_{\frac{1}{2}}^{(3)} : \;& \left|\frac{1}{2},\frac{1}{2}\right\rangle|1\rangle = \frac{1}{\sqrt{6}}(|100\rangle + |010\rangle - 2|001\rangle), \\
& \left|\frac{1}{2},-\frac{1}{2}\right\rangle|1\rangle = \frac{1}{\sqrt{6}}(-|011\rangle - |101\rangle + 2|110\rangle), \\
& \left|\frac{1}{2},\frac{1}{2}\right\rangle|0\rangle = \frac{1}{\sqrt{2}}(|100\rangle - |010\rangle), \\
& \left|\frac{1}{2},-\frac{1}{2}\right\rangle|0\rangle = \frac{1}{\sqrt{2}}(|101\rangle - |011\rangle).
\end{aligned} \tag{2.145}$$

where the right hand side is written in the computational basis. Once again, due to the one-dimensionality of $\mathcal{P}_{3/2}^{(3)}$, we have ignored the path component of the corresponding basis vectors. Let's conclude this discussion by noting how a basis state is updated when an extra spin-half particle is added to the system [72]:

$$|s,m\rangle|p\rangle \otimes \left|\frac{1}{2},\pm\frac{1}{2}\right\rangle \to \sqrt{\frac{s \pm m + 1}{2s+1}}\left|s+\frac{1}{2},m\pm\frac{1}{2}\right\rangle|p,0\rangle \mp \sqrt{\frac{s \mp m}{2s+1}}\left|s-\frac{1}{2},m\pm\frac{1}{2}\right\rangle|p,1\rangle. \tag{2.146}$$

2.3.4 The Haar measure and integrating over SU(2)

We very briefly introduce the Haar measure so that we have the tools required to integrate over the group SU(2). This will allow us to integrate over (multi-)qubit states, and therefore consider continuous distributions of pure states. We do not go into the basics of measure theory, referring the reader to any standard textbook on the subject, e.g. Refs. [74, 75].

Measure theory allows us, among many other things, to integrate over more general sets than just the real or complex numbers. In this work we will need to "sum" over every pure qubit state on the Bloch sphere. Being a *continuous set* of (pure) states, we will have to somehow *integrate* over this set. The key to doing this will be by integrating with respect to the Haar measure μ_H on SU(2). We do not delve into the details of the Haar measure here, just stating a definition of it, taken from [76].

Definition 2.3.10. *The Haar measure μ_H on $SU(2)$ is the unique probability measure satisfying*

$$\int_{SU(2)} f(U)d\mu_H(U) = \int_{SU(2)} f(UV)d\mu_H(U) = \int_{SU(2)} f(VU)d\mu_H(U), \tag{2.147}$$

for all $V \in SU(2)$ and for all integrable functions f.

Since μ_H is a probability measure, $\int_{\mathrm{SU}(2)} d\mu_H(U) = 1$. Note that the Haar measure is more general than presented here, the same definition applies when we replace SU(2) with any compact group.

This concludes our discussion of the background theory. We now have the mathematical and physical tools required to understand the bulk of this thesis.

Chapter 3

Measurement disturbance tradeoffs in three-qubit unsupervised quantum classification

The contents of this chapter is largely taken directly from our published work, found in Ref. [77].

3.1 Introduction

With large data sets becoming more and more prevalent in almost all parts of the modern world, and with hopes that quantum technologies and data will soon revolutionise many sectors, applying the ideas of machine learning to the quantum domain has been an increasingly active line of research. This work has taken a number of different directions [78]: firstly, using classical machine learning techniques to understand and analyse quantum systems and phenomena [79, 80]. This is done using the classical data made up, for instance, from the results output by measuring such quantum systems and processes. There are natural limitations to the analysis of the quantum world using classical methods due to the fact that the classical resources required to fully characterise quantum systems and processes scale exponentially with the number of quantum systems. Indeed, it was this feature that prompted Feynman to suggest the need for quantum computation in order to simulate a quantum world [81]. The second, and perhaps most heavily studied flavour of quantum learning is that of using quantum information processing (QIP) techniques with the hopes of reducing the resources required to perform machine learning tasks on classical data sets [82–91]. Sometimes this involves using quantum techniques to speed up or improve the performance of a particular subroutine within a quantum algorithm, for example when using quantum annealing to aid in optimisation [85–87]. Conversely, this sometimes involves quantum algorithms that tackle the whole machine learning problem, for example when solving linear equations [88], performing linear regression [90] or carrying out principle component analysis [91].

This chapter, however, concerns a third direction in quantum learning: that of learning about *quantum data* by analysing it directly, rather than via the classical data output from some collection of measurements. Although less studied than the other forms of quantum learning we have discussed, the importance of considering it is becoming clear [71, 92–99]. Indeed, we are starting to see that there may be benefits to manipulating and learning about quantum data directly. For example, Huang et al. [99] showed that analysing the quantum output of an experiment directly using a quantum computer can require exponentially fewer runs of the experiment than if the classical measurement results were to be analysed instead. But quantum data is fundamentally different to classical data, and learning strategies are therefore subject to different, peculiarly quantum limitations, which are not yet well explored. As an example, quantum data famously cannot be cloned [2, 3], in stark contrast to the classical case. In addition, it is not possible to extract information about a quantum system without causing disturbance [10]. Measurement strategies must therefore be carefully chosen and generically (but not always) the globally optimal strategy for any learning

task involves waiting until all data has been received and then performing a joint measurement over all systems [71, 100–106].

Such considerations thus pose a problem unique to the quantum case: can we learn about a subset of data without compromising performance on the dataset as a whole? We might expect a measurement-disturbance type tradeoff between performance on the subset and performance on the whole dataset. In this chapter we take the first steps towards understanding this tradeoff, studying the simplest case of unsupervised binary classification of qubit states, with three samples. A binary classification task is one in which the aim is to assign each sample provided to one of two possible classes, as accurately as possible. Unsupervised means that there is no labelled training data provided, and the user or algorithm must do as well as possible by comparing the data samples to each other. We give, analytically, the precise tradeoff between learning about the first two samples provided and learning about all three samples. This case is simple enough to allow analytic results, while rich enough to demonstrate the tradeoff. Surprisingly, for a range of strategies on the first two qubits, it is possible to avoid any reduction in performance on all three.

Our work is related to the problem of sequential observers extracting information about a system [107–110], however, so far, the literature has mostly considered the case in which sequential observers have access to the *same* system. Here, in the learning scenario, we are interested in how measurements on some part of a system (the first two subsystems in the example considered here) affect measurement on the whole. In addition, prior work has considered the supervised learning case, in which a labelled training set is provided and used to induce a function to label test instances. Here it is known that in the limit of many test instances, global measurements over training and test data are not required for optimal performance, and the training data may be measured in advance without access to the test data [100]. The unsupervised case is more complicated, as the algorithm seeks to both learn from and classify each instance provided.

This chapter is structured as follows: in Sec. 3.2 we will begin by discussing what we mean by an unsupervised binary classification of quantum data by considering examples on datasets of two and three qubits. Next, in Sec. 3.3, we derive the main results of this chapter - the tradeoff between the two classifications. Then, in Sec. 3.4, we construct a quantum circuit to run this protocol. We run this circuit on a Qiskit quantum computer simulator and replicate the tradeoff derived in Sec. 3.3. Finally, we end this chapter with a brief discussion of the results as well as possible future directions this line of research could take.

3.2 Unsupervised classification on two and three-qubit datasets

In this section, we aim to gain some intuition about the quantum learning task we are considering in this chapter: the unsupervised classification of quantum data. We do this by considering the simplest non-trivial examples - a binary classification on datasets with two and three qubits. The details of this section are published in [77].

3.2.1 Optimal classification of two-qubit dataset

Let's begin by understanding what we mean by the binary classification of a two-qubit dataset. Suppose we have a dataset consisting of two qubits that can each be in one of two states $|\varphi_0\rangle, |\varphi_1\rangle$, then the aim of a *binary* classification is to group, or cluster, these qubits into *two* classes based on their state. So, in the case of a dataset consisting of two qubits, our first thought may be that, in order to perform a binary classification, our aim is to distinguish between the following four states (corresponding to each possible quantum dataset): $|\varphi_0\rangle|\varphi_0\rangle$, $|\varphi_0\rangle|\varphi_1\rangle$, $|\varphi_1\rangle|\varphi_0\rangle$ and $|\varphi_1\rangle|\varphi_1\rangle$. However, we are interested in an *unsupervised* classification, so this isn't quite right.

Being unsupervised means that we have no prior information about the state of each element in our dataset, that is $|\varphi_0\rangle$ and $|\varphi_1\rangle$ are totally unknown (and therefore independent), equiprobable qubit states [71]. We can deal with this lack of knowledge by writing the possible states of our quantum datasets as the following mixed states

$$\rho_{ij} = \int |\varphi_i\rangle|\varphi_j\rangle\langle\varphi_i|\langle\varphi_j| \, d\varphi_0 d\varphi_1, \tag{3.1}$$

where $i = 0,\ j \in \{0, 1\}$, and the integral is with respect to the Haar measure on SU(2), and over the entire

Bloch sphere[1]. Note that, when averaging over the Bloch sphere, all information about whether each qubit is $|\varphi_0\rangle$ or $|\varphi_1\rangle$ is lost and all that remains is information about their relative positions on the Bloch sphere. This means that $\rho_{00} \equiv \rho_{11}$ and $\rho_{01} \equiv \rho_{10}$, and our aim is thus to distinguish between the states ρ_{00} and ρ_{01}, which tells us something about whether the two samples are the same or different from one another.

Alternatively, if we parameterise our qubits as was done in Eq. (2.32),

$$|\varphi_i\rangle = \cos\frac{\theta_i}{2}|0\rangle + e^{i\phi_i}\sin\frac{\theta_i}{2}|1\rangle, \tag{3.2}$$

where $i \in \{0, 1\}$, then we can, instead integrate over θ_i, ϕ_i as follows:

$$\rho_{ij} = \frac{1}{16\pi^2}\int_0^{2\pi} d\phi_0 d\phi_1 \int_0^{\pi} d\theta_0 d\theta_1 \sin\theta_0 \sin\theta_1 \, |\varphi_i\rangle|\varphi_j\rangle\langle\varphi_i|\langle\varphi_j|. \tag{3.3}$$

Here, the normalisation constant $1/(16\pi^2)$ comes from us integrating over two independent Bloch spheres (indexed by 0 and 1) each with surface area 4π. Having written this, it turns out that, especially as we increase the size of our dataset, the previous, "non-parameterised" version of ρ_{ij} is more convenient to use.

So, how do we write down, explicitly, our two-qubit states ρ_{00}, ρ_{01}? Let's begin with ρ_{00}. Using Eq. (3.1), the fact that $\int d\varphi_i = 1 \; \forall i$, and the SU(2) invariance of the Haar measure, notice that, for any $U \in \mathrm{SU}(2)$,

$$\mathbf{Q}^{(2)}(U)\rho_{00}\mathbf{Q}^{(2)^\dagger}(U) = \rho_{00}. \tag{3.4}$$

To see this, we can rewrite ρ_{00}, perhaps more rigorously, as

$$\rho_{00} = \int_{SU(2)} V_0^{\otimes 2}|\psi\psi\rangle\langle\psi\psi|V_0^{\otimes 2^\dagger} d\mu(V_0), \tag{3.5}$$

where $|\psi\rangle$ is some fixed pure qubit state, and μ is the Haar measure on SU(2). This is related to Eq. (3.1) by noting that $|\varphi_0\rangle = V_0|\psi\rangle$ for some $V_0 \in \mathrm{SU}(2)$. The reason for performing this integral with respect to the Haar measure on SU(2) is that this ensures the states $\{|\varphi_0\rangle = V_0|\psi\rangle \;:\; V_0 \in \mathrm{SU}(2)\}$ are uniformly distributed on the surface of the Bloch sphere, which is what we're assuming. As we saw in Sec. 2.3.4, a property of the Haar measure is that, for any integrable function f, $\int_{\mathrm{SU}(2)} f(UV)d\mu(V) = \int_{\mathrm{SU}(2)} f(V)d\mu(V)$ for any $U \in \mathrm{SU}(2)$ [76]. It follows that

$$\begin{aligned}
\mathbf{Q}^{(2)}(U)\rho_{00}\mathbf{Q}^{(2)^\dagger}(U) &= U^{\otimes 2}\bigg(\int_{SU(2)} V_0^{\otimes 2}|\psi\psi\rangle\langle\psi\psi|V_0^{\otimes 2^\dagger} d\mu(V_0)\bigg)U^{\otimes 2^\dagger} \\
&= \int_{SU(2)} (UV_0)^{\otimes 2}|\psi\psi\rangle\langle\psi\psi|(UV_0)^{\otimes 2^\dagger} d\mu(V_0) \\
&= \int_{SU(2)} V_0^{\otimes 2}|\psi\psi\rangle\langle\psi\psi|V_0^{\otimes 2^\dagger} d\mu(V_0) = \rho_{00}.
\end{aligned} \tag{3.6}$$

So, by Schur's Lemma, there exist bases, for example the Schur basis given in Eq. (2.143), such that

$$\rho_{00} = \alpha_1 \mathbb{I}_1 \oplus \alpha_0 \mathbb{I}_0, \tag{3.7}$$

where $\alpha_0, \alpha_1 \geq 0$ by the positivity of quantum states and $\mathbb{I}_s$ are the identity operators on the spaces $\mathcal{Q}_s^{(2)}$. Recalling Eq. (2.142), note that the subscripts reference the total spin of the SU(2) invariant subspaces.

However, notice that for any qubit $|\varphi_0\rangle = \cos\frac{\theta_0}{2}|0\rangle + e^{i\phi_0}\sin\frac{\theta_0}{2}|1\rangle$,

$$|\varphi_0\varphi_0\rangle = \cos^2\frac{\theta_0}{2}|00\rangle + \frac{1}{2}e^{i\phi_0}\sin\theta_0\,(|01\rangle + |10\rangle) + \sin^2\frac{\theta_0}{2}|11\rangle. \tag{3.8}$$

[1] This is a shorthand notation, we write this more rigorously later, in Eq. (3.5).

So, comparing with Eq. (2.143), $|\varphi_0\varphi_0\rangle$ lives entirely in $\mathcal{Q}_1^{(2)} \otimes \mathcal{P}_1^{(2)}$. This implies that $\alpha_0 = 0$ and therefore, by the normalisation of ρ_{00},

$$\begin{aligned}\rho_{00} &= \frac{1}{3}\mathbb{I}_1 \\ &= \frac{1}{3}\left(|1,1\rangle\langle 1,1| + |1,0\rangle\langle 1,0| + |1,-1\rangle\langle 1,-1|\right).\end{aligned} \tag{3.9}$$

Next, for ρ_{01}, notice that,

$$\begin{aligned}\rho_{01} &= \int |\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1| d\varphi_0 d\varphi_1 \\ &= \int |\varphi_0\rangle\langle\varphi_0| \otimes |\varphi_1\rangle\langle\varphi_1| d\varphi_0 d\varphi_1 \\ &= \int |\varphi_0\rangle\langle\varphi_0| d\varphi_0 \otimes \int |\varphi_1\rangle\langle\varphi_1| d\varphi_1 \\ &= \frac{1}{4}\mathbb{1} \otimes \mathbb{1},\end{aligned} \tag{3.10}$$

where the last equality is obtained by the invariance of $\int |\varphi_i\rangle\langle\varphi_i| d\varphi_i$ under $\mathbf{Q}^{(1)}[SU(2)]$ (or, more physically, due to each of the integrals describing a maximally mixed qubit) and where the $1/4$ is required for normalisation. Therefore, ρ_{01} is proportional to the identity on the two-qubit Hilbert space $\mathcal{H}^{(2)}$, and hence, we can rewrite it as the identity in the Schur basis:

$$\begin{aligned}\rho_{01} &= \frac{1}{4}\mathbb{I}_1 \oplus \mathbb{I}_0 \\ &= \frac{1}{4}\big(|1,1\rangle\langle 1,1| + |1,0\rangle\langle 1,0| + |1,-1\rangle\langle 1,-1| + |0,0\rangle\langle 0,0|\big).\end{aligned} \tag{3.11}$$

We can therefore see that our task in an unsupervised binary classification of a two qubit dataset is to distnguish, as best we can, between the following two states:

$$\rho_{00} = \frac{1}{3}\left(|1,1\rangle\langle 1,1| + |1,0\rangle\langle 1,0| + |1,-1\rangle\langle 1,-1|\right), \tag{3.12a}$$

$$\rho_{01} = \frac{1}{4}\big(|1,1\rangle\langle 1,1| + |1,0\rangle\langle 1,0| + |1,-1\rangle\langle 1,-1| + |0,0\rangle\langle 0,0|\big). \tag{3.12b}$$

So, we can view a classification as a quantum state discrimination problem. That is, in order to classify our quantum dataset, we must construct a quantum measurement that distinguishes between ρ_{00} and ρ_{01}. Note that, from here onward, we will often discuss these classification problems in the language of quantum measurement problems (e.g. a quantum classification being a quantum measurement).

The optimal quantum measurement that distinguishes between ρ_{00} and ρ_{01} was found, by Barnett et al [92], to be made up of the projectors onto the symmetric ($s = 1$) and anti-symmetric ($s = 0$) SU(2) invariant subspaces respectively:

$$P_+ = |1,1\rangle\langle 1,1| + |1,0\rangle\langle 1,0| + |1,-1\rangle\langle 1,-1|, \tag{3.13a}$$

$$P_- = |0,0\rangle\langle 0,0|, \tag{3.13b}$$

where P_+ (P_-) is the outcome associated with measuring the state ρ_{00} (ρ_{01}). Here we use the $+/-$ subscripts rather than 00/01 respectively, anticipating the notation in the later sections of this chapter. This measurement can be motivated by realising that ρ_{00} and ρ_{01} commute with one another, which means they have a common set of eigenstates. So we take the optimal measurement operators P_+, P_- to be the (sum of) projectors onto the eigenstates with the largest eigenvalues of ρ_{00}, ρ_{01} respectively. Alternatively, it is the Holevo-Helstrom measurement (see Sec. 2.2.6) for distinguishing between two quantum states [17]. It is also worth noting an asymmetry in this measurement gives rise to: $P(+|\rho_{00}) = 1$ but $P(-|\rho_{01}) = 1/4$. In other words, the state ρ_{00} is never misidentified, whereas ρ_{01} can be.

Using Eq. (2.96), the maximal probability of successfully classifying two equally-likely, unknown qubits is calculated as follows:

$$P_{\text{succ}} = \frac{1}{2}[\text{Tr}(P_+\rho_{00}) + \text{Tr}(P_-\rho_{01})], \tag{3.14}$$

where the $1/2$ comes from the two states ρ_{00}, ρ_{01} being equiprobable. This results in a success rate of

$$P_{\text{succ}} = \frac{5}{8} = 62.5\%. \tag{3.15}$$

To reiterate, what has been derived here is the average probability of success for this task. In reality, two well defined states $|\varphi_0\rangle, |\varphi_1\rangle$ would make up the dataset. So we can see how the measurement $\{P_\pm\}$ fairs with respect to the possible pure states of the dataset. Without loss of generality, we can take

$$|\varphi_0\rangle = |0'\rangle, \tag{3.16a}$$
$$|\varphi_1\rangle = \cos\theta|0'\rangle + e^{i\phi}\sin\theta|1'\rangle, \tag{3.16b}$$

where $\{|0'\rangle, |1'\rangle\}$ is some arbitrary orthonormal basis of a qubit and $\theta \in [0, \pi], \phi \in [0, 2\pi)$. When performing the measurement $\{P_\pm\}$, we associate the outcome "$+$" with the data being prepared in the state $|\varphi_0\varphi_0\rangle$ *or* $|\varphi_1\varphi_1\rangle$, and the outcome "$-$" with the data being prepared in the state $|\varphi_0\varphi_1\rangle$ *or* $|\varphi_1\varphi_0\rangle$. With that, the probability of success, as a function of θ, ϕ can be shown to be

$$\begin{aligned} P_{\text{succ}}(\theta,\phi) &= \frac{1}{4}\big(\langle\varphi_0\varphi_0|P_+|\varphi_0\varphi_0\rangle + \langle\varphi_1\varphi_1|P_+|\varphi_1\varphi_1\rangle + \langle\varphi_0\varphi_1|P_-|\varphi_0\varphi_1\rangle + \langle\varphi_1\varphi_0|P_-|\varphi_1\varphi_0\rangle\big) \\ &= \frac{1}{2} + \frac{1}{4}\sin^2\theta, \end{aligned} \tag{3.17}$$

from which Eq. (3.15) can be recovered by averaging over θ (and ϕ). We can see that the success rate varies from that of a guess $P_{\text{succ}}(0,\phi) = 1/2$ when $|\varphi_0\rangle = |\varphi_1\rangle$, to $P_{\text{succ}}(\pi/2,\phi) = 3/4$ when $\langle\varphi_0|\varphi_1\rangle = 0$. Note that in order to achieve the maximal *average* success rate, we have sacrificed the measurement's ability in specific cases. For example, it does not perfectly distinguish the states of the dataset when $\langle\varphi_0|\varphi_1\rangle = 0$.

3.2.2 Optimal classification of three-qubit dataset

Similarly to the two-qubit case, we begin by writing down the possible three-qubit states. In general, we once again express these states as

$$\rho_{ijk} = \int |\varphi_i\rangle|\varphi_j\rangle|\varphi_k\rangle\langle\varphi_i|\langle\varphi_j|\langle\varphi_k|\, d\varphi_0 d\varphi_1, \tag{3.18}$$

where $i = 0,\ j,k \in \{0,1\}$. Once again, it is useful for understanding the problem to write down explicitly the possible states of our three-qubit dataset.

Similar arguments to those used to find ρ_{00} in the previous section tell us that we can write the following:

$$\rho_{000} = \alpha_{\frac{3}{2}}\mathbb{I}_{\frac{3}{2}} \oplus \alpha_{\frac{1}{2}}\mathbb{I}_{\frac{1}{2}} \oplus \alpha'_{\frac{1}{2}}\mathbb{I}_{\frac{1}{2}} \tag{3.19}$$

due to the commutivity of ρ_{000} with all the elements of $\mathbf{Q}^{(3)}[SU(2)]$. Here, similarly to before, $\mathbb{I}_s$ is the identity operator on the space $\mathcal{Q}_s^{(3)}$. Note the presence of two copies of the $\mathcal{Q}_{\frac{1}{2}}^{(3)}$ space implied here, discussed in more detail in Sec. 2.3.3. To find $\alpha_{\frac{1}{2}}, \alpha'_{\frac{1}{2}}$, notice that[2] for all $\sigma \in S_3$, and for all qubit states $|\varphi_0\rangle$,

$$\mathbf{P}^{(3)}(\sigma)|\varphi_0\rangle^{\otimes 3} = |\varphi_0\rangle^{\otimes 3}. \tag{3.20}$$

This implies that $|\varphi_0\rangle^{\otimes 3}$ lives entirely within $\mathcal{Q}_{\frac{3}{2}}^{(3)} \otimes \mathcal{P}_{\frac{3}{2}}^{(3)}$. If it didn't, $\mathbf{P}^{(3)}(\sigma)|\varphi_0\rangle^{\otimes 3}$ would have a component in $\mathcal{Q}_{\frac{1}{2}}^{(3)} \otimes \mathcal{P}_{\frac{1}{2}}^{(3)}$, meaning that $|\varphi_0\rangle^{\otimes 3}$ would not be acted on trivially by $\mathbf{P}^{(3)}(S_3)$.[3] We therefore have that

[2] Bearing in mind how $\mathbf{P}^{(3)}(S_3)$ acts on $\mathcal{H}^{(3)}$ as discussed in Sec. 2.3.3.

[3] since the irrep $\left(\mathbf{p}_{\frac{1}{2}}, \mathcal{P}_{\frac{1}{2}}^{(3)}\right)$ is non-trivial.

$\rho_{000} \in \mathcal{L}\big(\mathcal{Q}^{(3)}_{\frac{3}{2}} \otimes \mathcal{P}^{(3)}_{\frac{3}{2}}\big)$, meaning $\alpha_{\frac{1}{2}}, \alpha'_{\frac{1}{2}} = 0$ and

$$\rho_{000} = \frac{1}{4}\mathbb{I}_{\frac{3}{2}}, \tag{3.21}$$

where, again, $1/4$ is the normalisation constant.

Now, for ρ_{001}, similarly to ρ_{01} in the previous subsection,

$$\begin{aligned}
\rho_{001} =& \int |\varphi_0\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_0\varphi_1| d\varphi_0 d\varphi_1 \\
=& \int |\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0| d\varphi_0 \otimes \int |\varphi_1\rangle\langle\varphi_1| d\varphi_1 \\
=& \frac{1}{2}\rho_{00} \otimes \mathbb{1} \\
=& \alpha\left(|1,1\rangle\langle 1,1| + |1,0\rangle\langle 1,0| + |1,-1\rangle\langle 1,-1|\right) \otimes \left(\left|\frac{1}{2},\frac{1}{2}\right\rangle\left\langle\frac{1}{2},\frac{1}{2}\right| + \left|\frac{1}{2},-\frac{1}{2}\right\rangle\left\langle\frac{1}{2},-\frac{1}{2}\right|\right),
\end{aligned} \tag{3.22}$$

where α is the normalisation constant. In order to rewrite this in the Schur basis of $(\mathcal{Q}^{(3)}_{\frac{3}{2}} \otimes \mathcal{P}^{(3)}_{\frac{3}{2}}) \otimes (\mathcal{Q}^{(3)}_{\frac{1}{2}} \otimes \mathcal{P}^{(3)}_{\frac{1}{2}})$, we use Eq. (2.146), rewritten here for convenience,

$$|s,m\rangle|p\rangle \otimes \left|\frac{1}{2}, \pm\frac{1}{2}\right\rangle \to \sqrt{\frac{s \pm m + 1}{2s+1}}\left|s + \frac{1}{2}, m \pm \frac{1}{2}\right\rangle |p,0\rangle \mp \sqrt{\frac{s \mp m}{2s+1}}\left|s - \frac{1}{2}, m \pm \frac{1}{2}\right\rangle |p,1\rangle. \tag{2.146}$$

For our case, $s = 1, m \in \{1,0,-1\}$ and p has been omitted since $\dim \mathcal{P}^{(2)}_1 = 1 = \dim \mathcal{P}^{(2)}_0$. Applying Eq. (2.146) to Eq. (3.22), we obtain

$$\rho_{001} = \frac{1}{6}\left(\mathbb{I}_{\frac{3}{2}} + \mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|\right), \tag{3.23}$$

where $\alpha = 1/6$ was found by again requiring $\mathrm{Tr}(\rho_{001}) = 1$.

Finally, we can find ρ_{010}, ρ_{011}. Noting that,

$$\begin{aligned}
\rho_{011} &= \int |\varphi_0\varphi_1\varphi_1\rangle\langle\varphi_0\varphi_1\varphi_1| d\varphi_0 d\varphi_1 \\
&= \int |\varphi_1\varphi_0\varphi_0\rangle\langle\varphi_1\varphi_0\varphi_0| d\varphi_0 d\varphi_1 = \rho_{100},
\end{aligned} \tag{3.24}$$

in order to obtain ρ_{010}, ρ_{011}, we just have to permute the qubits in ρ_{001}. To do this, first notice that $\mathbb{I}_{\frac{3}{2}}$ is invariant under permutations of qubits since $\mathbf{P}^{(3)}(S_3)$ acts trivially on $\mathcal{P}^{(3)}_{\frac{3}{2}}$. Therefore, the only part of ρ_{001} affected by permutations is $\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|$.

Intuitively, we can guess the form of ρ_{010}, ρ_{011} by the fact that,

$$\cdots \rho_{001} \xrightarrow{(123)} \rho_{010} \xrightarrow{(123)} \rho_{011} \xrightarrow{(123)} \rho_{001} \cdots, \tag{3.25}$$

where $(123) \in S_3$. Since permutations only have an effect on the path components of the states, it seems that $\rho_{001}, \rho_{010}, \rho_{011}$ should be evenly distributed in the two-dimensional space $\mathcal{P}^{(3)}_{\frac{1}{2}}$. That is, since each state can be accessed by repeated application of the permutation (123), we'd expect each state be accessible by the repeated application of some two-dimensional transformation. In particular, since ρ_{001} is known, we might guess that the remaining states could be found by rotating its $\mathcal{P}^{(3)}_{\frac{1}{2}}$ component by $2\pi/3$. This indeed results in the states we're aiming for [given in Eq. (3.26)]. More concretely, we can derive ρ_{010} using the following three steps:

1. Rewrite ρ_{001} in the computational basis [using Eq. (2.145)].
2. Permute the qubits $|\psi_1\psi_2\psi_3\rangle \to |\psi_2\psi_3\psi_1\rangle$ to obtain ρ_{010} in the computational basis.

3. Rewrite the state in the Schur basis given in Eq. (2.145).

And similarly for ρ_{011}. Either way, the states ρ_{ijk} turn out to have the following form:

$$\rho_{000} = \frac{1}{4}\mathbb{I}_{\frac{3}{2}}, \tag{3.26a}$$

$$\rho_{001} = \frac{1}{6}\mathbb{I}_{\frac{3}{2}} + \frac{1}{6}\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{3.26b}$$

$$\rho_{010} = \frac{1}{6}\mathbb{I}_{\frac{3}{2}} + \frac{1}{24}\mathbb{I}_{\frac{1}{2}} \otimes \Big(|1\rangle - \sqrt{3}|0\rangle\Big)\Big(\langle 1| - \sqrt{3}\langle 0|\Big), \tag{3.26c}$$

$$\rho_{011} = \frac{1}{6}\mathbb{I}_{\frac{3}{2}} + \frac{1}{24}\mathbb{I}_{\frac{1}{2}} \otimes \Big(|1\rangle + \sqrt{3}|0\rangle\Big)\Big(\langle 1| + \sqrt{3}\langle 0|\Big). \tag{3.26d}$$

We can now see more clearly the states we aim to discriminate between in order to perform an unsupervised binary classification on a three-qubit dataset.

The optimal measurement that distinguishes the four states in Eq. (3.26) is made up of the POVM elements,

$$\pi_{000} = \mathbb{I}_{\frac{3}{2}}, \tag{3.27a}$$

$$\pi_{001} = \frac{2}{3}\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{3.27b}$$

$$\pi_{010} = \frac{1}{6}\mathbb{I}_{\frac{1}{2}} \otimes \Big(|1\rangle - \sqrt{3}|0\rangle\Big)\Big(\langle 1| - \sqrt{3}\langle 0|\Big), \tag{3.27c}$$

$$\pi_{011} = \frac{1}{6}\mathbb{I}_{\frac{1}{2}} \otimes \Big(|1\rangle + \sqrt{3}|0\rangle\Big)\Big(\langle 1| + \sqrt{3}\langle 0|\Big). \tag{3.27d}$$

To motivate this, notice that $\rho_{001}, \rho_{010}, \rho_{011}$ have S_3 permutation symmetry in their qubits. We can therefore require the optimal measurement to distinguish these three states to have this same symmetry. So, all we need to do is construct π_{000}, π_{001} to optimally distinguish between ρ_{000}, ρ_{001}. From this, we can obtain π_{010}, π_{011} via the S_3 symmetry mentioned. The construction of π_{000}, π_{001} follows the same reasoning as that of two-qubit measurement in Eq. (3.13) aside from the factor of $2/3$ in π_{001} which is required for completeness. Therefore, using this measurement and Eq. (2.96), the maximal probability of successfully distinguishing the (equally likely) states in Eq. (3.26) is

$$P_{\text{succ}} = \frac{5}{12} \approx 41.7\%. \tag{3.28}$$

In other words, and at risk of overemphasising, this is the optimal success rate in an unsupervised binary classification on a three-qubit dataset.

3.3 Measurement disturbance tradeoff

In this section, we consider a simple sequential learning task to take some first steps into understanding how learning about quantum data affects how well something else can be learnt about this data at a later stage. When considering classical data, this seems like a trivial problem: given a classical picture of a dog, Alice may recognise that the subject of the photo is a Labrador, but in doing so, she does not affect Bob's chances of independently identifying that the dog is female. In other words, when Alice learns something about some classical data, Bob also has access to the same data, whether Alice leaves it unaltered or makes a copy before she analyses it.

In general, the same cannot be said when we instead have quantum data. For a start, it is well known that unknown quantum states cannot be perfectly copied [2, 3]. Further, when information is extracted from some quantum system (i.e. in some learning scenario), the system is generically disturbed in some way. This is related to the measurement disturbance discussed in Chapter 2, since a quantum measurement must be performed on a quantum system in order to access any information it contains. Therefore, we can see that the problem is not so trivial in the quantum regime: although Alice may manage to determine that the dog in a "quantum photo" is a Labrador, in doing so, she would generically alter it in some way. So, since

she couldn't perfectly copy the quantum photo beforehand, Bob would only be able to use some distorted version of it to try and figure out whether the dog is male or female.

To explore this intuition in a more concrete setting, we consider the following question: how is an unsupervised binary classification (as described in the previous section) on a dataset of three qubits affected by an intermediate one on a subset containing the first two qubits? To investigate this question, we first gain some intuition by considering the intermediate classification to be the optimal one (as discussed in Sec. 3.2.1). Following this, we derive the full tradeoff between the success rate of an intermediate classification with that of the three-qubit one. This scenario is simple enough to allow analytic results, while rich enough to demonstrate the tradeoff. Surprisingly, for a range of strategies on the first two qubits, it is possible to avoid any reduction in performance on all three. Once again, the contents of this section closely follow the published work [77].

3.3.1 Optimal intermediate measurement

Suppose we have a quantum dataset containing three-qubits that can each be in one of two unknown states $|\varphi_0\rangle, |\varphi_1\rangle$. As mentioned, let's first consider what happens when we perform the optimal measurement $\{P_\pm\}$ given in Eq. (3.13) to classify the first two qubits, followed by an optimal measurement on all three. In particular, we consider the case in which the outcome of the two-qubit measurement is known, and the measurement on all three is updated accordingly. After the first measurement has been performed with an outcome k being obtained, as discussed earlier with Eq. (2.85), the two qubit states update as follows[4]:

$$\rho_{0ij} \to \rho_{0ij}^k = \frac{\left(\sqrt{P_k} \otimes \mathbb{1}\right)\rho_{0ij}\left(\sqrt{P_k} \otimes \mathbb{1}\right)^\dagger}{\mathrm{Tr}(P_k \otimes \mathbb{1}\rho_{0ij})}, \tag{3.29}$$

where ρ_{0ij} are the states in Eq. (3.26) and $\mathbb{1}$ denotes the identity operator on a single qubit.

Explicitly, the states are as follows:

$$\rho_{000}^+ = \frac{1}{4}\mathbb{I}_{\frac{3}{2}}, \tag{3.30a}$$
$$\rho_{001}^+ = \frac{1}{6}\mathbb{I}_{\frac{3}{2}} + \frac{1}{6}\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{3.30b}$$
$$\rho_{01k}^+ = \frac{2}{9}\mathbb{I}_{\frac{3}{2}} + \frac{1}{18}\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{3.30c}$$
$$\rho_{000}^- = 0 = \rho_{001}^-, \tag{3.30d}$$
$$\rho_{01k}^- = \frac{1}{2}\mathbb{I}_{\frac{1}{2}} \otimes |0\rangle\langle 0| \tag{3.30e}$$

for $k = 0, 1$. For each of the first measurement outcomes $P_\pm$, we can therefore find the optimal measurement to be made up of the following projectors:

$$\pi_{000}^+ = \mathbb{I}_{\frac{3}{2}}, \tag{3.31a}$$
$$\pi_{001}^+ = \mathbb{I}_{\frac{1}{2}\otimes\frac{1}{2}}, \tag{3.31b}$$
$$\pi_{01k}^+ = 0, \tag{3.31c}$$
$$\pi_{000}^- = \mathbb{I}_{\frac{3}{2}}, \tag{3.31d}$$
$$\pi_{001}^- = 0, \tag{3.31e}$$
$$\pi_{01k}^- = \frac{1}{2}\mathbb{I}_{\frac{1}{2}\otimes\frac{1}{2}}, \tag{3.31f}$$

where $\mathbb{I}_{\frac{1}{2}\otimes\frac{1}{2}}$ denotes the identity on the subspace $\mathcal{Q}_{\frac{1}{2}}^{(3)} \otimes \mathcal{P}_{\frac{1}{2}}^{(3)}$. These measurements can be motivated by the fact that $\pi_i^\pm$ projects its corresponding state, $\rho_i^\pm$, onto the components with coefficients that are larger, or the same as, the same components in all the other states.

[4]Note that this measurement $\{P_k\}$ is only performed on the first two qubits of the state (dataset).

Now, the probability of a successful second measurement is given by

$$\begin{aligned} P_{\text{succ}}^{\text{2nd}} &= \sum_{k\in\{+,-\}} \sum_{i,j\in\{0,1\}} P(\rho_{0ij}) P(P_k, \pi_{0ij}^k | \rho_{0ij}), \\ &= \sum_k \sum_{i,j} P(\pi_{0ij}^k | \rho_{0ij}^k) P(P_k | \rho_{0ij}) P(\rho_{0ij}) \\ &= \frac{1}{4} \sum_k \sum_{i,j} \text{Tr}\left[\pi_{0ij}^k \left(\sqrt{P_k} \otimes \mathbb{1}\right) \rho_{0ij} \left(\sqrt{P_k} \otimes \mathbb{1}\right)^\dagger \right], \end{aligned} \tag{3.32}$$

where $P(\rho_{0ij})$ is the probability that the system is prepared in the state ρ_{0ij} (this is $1/4$ for all i, j), $P(P_k, \pi_{0ij}^k|\rho_{0ij})$ denotes the probability that the first measurement outcome is k and the second is $0ij$ given that the state was prepared in the state ρ_{0ij}, and $P(\pi_{0ij}^k|\rho_{0ij}^k) \equiv P(\pi_{0ij}^k|\rho_{0ij}, P_k)$. We therefore find that the probability of a successful second classification has been affected by an optimal first classification and has been reduced to the following value:

$$P_{\text{succ}}^{\text{2nd}} = \frac{19}{48} \approx 39.6\%. \tag{3.33}$$

Although this is a small reduction in the success rate of the three-qubit measurement from the optimal value of $5/12 \approx 41.7\%$, it demonstrates the principle of measurement disturbance caused by the intermediate classification.

3.3.2 Weakening the intermediate measurement

3.3.2.1 Weak two-qubit measurement

Our ultimate aim is to understand how a classification on two qubits affects our ability to perform a subsequent classification in general. So, instead of considering only the optimal measurement on two qubits, we interpolate between this and the weakest possible measurement: the identity measurement. This weakened measurement can be written as

$$\begin{aligned} \pi_- &= \alpha P_- + \beta \mathbb{I}, \\ \pi_+ &= \alpha P_+ + (1 - \alpha - \beta) \mathbb{I}, \end{aligned} \tag{3.34}$$

such that $\alpha \in [0, 1-\beta]$ and $\beta \in [0, 1]$ to ensure the positivity condition of POVMs, given in Eq. (2.82a), as well as the convention we are adopting: we take the measurement outcome π_+ (π_-) to correspond to the measurement of the state ρ_{00} (ρ_{01})[5]. Note also that, by construction, this POVM is complete, as required [see Eq. (2.82b)]. To reduce future work, note that we can change between the two situations corresponding to different measurement outcomes by performing the swaps:

$$\begin{aligned} \alpha &\to -\alpha, \\ \beta &\to 1 - \beta. \end{aligned} \tag{3.35}$$

So, once again using Eq. (2.96) with equiprobable states ρ_{00}, ρ_{01}, the probability of a successful two-qubit classification using the POVM in Eq. (3.34) is given by

$$P_{\text{succ}}^{\text{1st}} = \frac{1}{2}\left(1 + \frac{\alpha}{4}\right), \tag{3.36}$$

where the superscript is included in anticipation of the second classification introduced next.

3.3.2.2 Subsequent three-qubit classification

Now, let's return to our quantum dataset made up of three qubits, each either $|\varphi_0\rangle$ or $|\varphi_1\rangle$. Following the weakened intermediate measurement $\{\pi_\pm\}$, the state of our dataset ρ_{0ij} is updated as[6]

$$\rho_{0ij} \to \rho_{0ij}^\pm = \frac{(\sqrt{\pi_\pm} \otimes \mathbb{1}) \rho_{0ij} (\sqrt{\pi_\pm} \otimes \mathbb{1})^\dagger}{\text{Tr}(\pi_\pm \otimes \mathbb{1} \rho_{0ij})}. \tag{3.37}$$

[5] That is, we require $P(\pi_+|\rho_{00}) \geq P(\pi_-|\rho_{00})$ and $P(\pi_-|\rho_{01}) \geq P(\pi_+|\rho_{01})$.

[6] Explicitly, $\sqrt{\pi_-} = \sqrt{\alpha + \beta} P_- + \sqrt{\beta} P_+$ and $\sqrt{\pi_+} = \sqrt{1 - \alpha - \beta} P_- + \sqrt{1 - \beta} P_+$.

Explicitly, in the case when the measurement outcome on the first two qubits is "$-$", using similar techniques as those found in Eqs. (2.146, 3.23) to find $\sqrt{\pi_-} \otimes \mathbb{1}$ in the Schur basis, the states ρ^-_{0ij} can be shown to be

$$\rho^-_{000} = \frac{1}{4}\mathbb{I}_{\frac{3}{2}}, \tag{3.38a}$$

$$\rho^-_{001} = \frac{1}{6}\mathbb{I}_{\frac{3}{2}} + \frac{1}{6}\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{3.38b}$$

$$\rho^-_{010} = \frac{4\beta}{6(\alpha+4\beta)}\mathbb{I}_{\frac{3}{2}} + \frac{1}{6(\alpha+4\beta)}\mathbb{I}_{\frac{1}{2}} \otimes \Big(\sqrt{\beta}|1\rangle - \sqrt{3(\alpha+\beta)}|0\rangle\Big)\Big(\sqrt{\beta}\langle 1| - \sqrt{3(\alpha+\beta)}\langle 0|\Big), \tag{3.38c}$$

$$\rho^-_{011} = \frac{4\beta}{6(\alpha+4\beta)}\mathbb{I}_{\frac{3}{2}} + \frac{1}{6(\alpha+4\beta)}\mathbb{I}_{\frac{1}{2}} \otimes \Big(\sqrt{\beta}|1\rangle + \sqrt{3(\alpha+\beta)}|0\rangle\Big)\Big(\sqrt{\beta}\langle 1| + \sqrt{3(\alpha+\beta)}\langle 0|\Big) \tag{3.38d}$$

with probabilities (derived in Appendix 3.A.1)

$$p^-_{000} = p^-_{001} = \frac{2\beta}{\alpha+8\beta}, \tag{3.39a}$$

$$p^-_{010} = p^-_{011} = \frac{\alpha+4\beta}{2(\alpha+8\beta)}. \tag{3.39b}$$

To find $\rho^+_{0ij},\ p^+_{0ij}$, we can just perform the swaps in Eq. (3.35).

In order to achieve our aim of classifying the resulting three-qubit system, we construct a measurement $\{\pi^-_i\}$ that distinguishes between the states $\{\rho^-_i\}$ above (for additional detail, see Appendix 3.A.2). To do this, first, notice that the totally symmetric components (the $s = 3/2$ components) of $\rho^-_{001}, \rho^-_{01l}$ have coefficients that are strictly less than those of ρ^-_{000}. Further, ρ^-_{000} has no $s = \frac{1}{2}$ components. This motivates the fact that the optimal way to distinguish ρ^-_{000} from the other states is to take

$$\pi^-_{000} = \mathbb{I}_{\frac{3}{2}} \tag{3.40}$$

while keeping the remaining measurement operators in $\mathcal{L}\big(\mathcal{Q}^{(3)}_{\frac{1}{2}} \otimes \mathcal{P}^{(3)}_{\frac{1}{2}}\big)$. Next, note that in the $s = \frac{1}{2}$ subspaces, $\rho^-_{001}, \rho^-_{010}, \rho^-_{011}$ have a mirror symmetric form in their path degree of freedom (spanned by $|p_{\frac{1}{2}}\rangle = |0\rangle, |1\rangle$) as $p^-_{010} = p^-_{011}$ and the set is invariant under reflection about $|0\rangle$. The optimal measurement to distinguish these three states is known [63] and has the form (including π^-_{000} for completeness)

$$\pi^-_{000} = \mathbb{I}_{\frac{3}{2}}, \tag{3.41a}$$

$$\pi^-_{001} = (1 - a_-^2)\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{3.41b}$$

$$\pi^-_{010} = \frac{1}{2}\mathbb{I}_{\frac{1}{2}} \otimes (a_-|1\rangle - |0\rangle)\,(a_-\langle 1| - \langle 0|)\,, \tag{3.41c}$$

$$\pi^-_{011} = \frac{1}{2}\mathbb{I}_{\frac{1}{2}} \otimes (a_-|1\rangle + |0\rangle)\,(a_-\langle 1| + \langle 0|)\,, \tag{3.41d}$$

where $a_- \in [0, 1]$ to preserve positivity. A closed form analytic expression for a_- in terms of the prior probabilities and overlaps of the states is given in [63], which we use below. Once again, to obtain $\{\pi^+_i\}$, we just perform the swaps in Eq. (3.35). Looking back at Eq. (3.41), we can reinterpret this measurement as a two step process: first, a projection based on total spin s which tells us something about how many of each type of qubit the dataset has (ρ^-_{000} versus $\rho^-_{001}, \rho^-_{010}, \rho^-_{011}$). The second step is to learn about the order of the qubits in the dataset by considering the permutation, or path component $\mathcal{L}\big(\mathcal{P}^{(3)}_s\big)$, of all the states that share the same number of each qubit as one another.

So, how does a_- relate to the parameters (α, β) of the first measurement that dictate the level of disturbance between $\rho^-_{001}, \rho^-_{010}, \rho^-_{011}$? To figure this out, we utilise [63] which requires us to first define a prior probability for the states $\rho^-_{001}, \rho^-_{010}, \rho^-_{011}$ when projected into the $s = 1/2$ subspace. In Appendix 3.A.2, we write these updated priors as q^-_{001}, q^-_{01i} respectively. We can then directly use the results of [63] to find the optimal value of the parameter a_-. Updating the prior probabilities gives

$$p^- = \frac{3\alpha + 4\beta}{6(\alpha + 2\beta)} \tag{3.42}$$

such that $q^-_{010} = q^-_{011} = p^-,\ q^-_{001} = 1 - 2p^-$. The full derivation of this can be found in Appendix 3.A.2. Using the analytical expression in [63] then gives (again more detail is given in Appendix 3.A.2):

$$a_- = \begin{cases} \sqrt{\frac{\alpha+\beta}{3\beta}} & \text{if } \alpha \in [0, \min\{1-\beta, 2\beta\}], \\ 1 & \text{if } \alpha \in (2\beta, 1-\beta] \text{ with } 2\beta < 1-\beta \end{cases} \tag{3.43}$$

such that $\beta \in [0,1]$ as always. Note that the conditions $2\beta < 1-\beta,\ \beta \in [0,1]$ can be rewritten as $\beta \in \left[0, \frac{1}{3}\right)$. Similarly, when the outcome of the first measurement is π_+, we arrive at

$$a_+ = \sqrt{\frac{1-\alpha-\beta}{3(1-\beta)}} \tag{3.44}$$

for all valid α, β. To achieve our aim and observe how the success probability of the first and second measurements compare to one another, we consider the two cases of Eq. (3.43).

Case 1: $\alpha \in [0, \min\{1-\beta, 2\beta\}],\ \beta \in [0,1]$

Consider the first case in Eq. (3.43), that is, when

$$a_- = \sqrt{\frac{\alpha+\beta}{3\beta}}, \tag{3.45a}$$

$$a_+ = \sqrt{\frac{1-\alpha-\beta}{3(1-\beta)}}. \tag{3.45b}$$

Using Eq. (3.32) with $P_\pm \to \pi_\pm$, in this region, it is straightforward, albeit requiring a little algebra, to show that the probability of a successful second classification stays constant at the optimal value for distinguishing three undisturbed qubits:

$$P^{\text{2nd}}_{\text{succ}} = \frac{5}{12} \tag{3.46}$$

for all $\alpha \in [0, \min\{1-\beta, 2\beta\}],\ \beta \in [0,1]$.

Case 2: $\alpha \in (2\beta, 1-\beta], \beta \in \left[0, \frac{1}{3}\right)$.

Considering now the second case in Eq. (3.43), let $a_- = 1$ and a_+ be as written in Eq. (3.44). Once again, using Eq. (3.32) with $P_\pm \to \pi_\pm$, after a little algebra, we find

$$P^{\text{2nd}}_{\text{succ}} = \frac{5}{12} - \frac{\beta}{12} - \frac{\alpha}{48} + \frac{1}{24}\sqrt{3\beta(\alpha+\beta)}. \tag{3.47}$$

Now, we want $P^{\text{2nd}}_{\text{succ}}$ to be at its optimal value for each value of $P^{\text{1st}}_{\text{succ}}$. Since $P^{\text{1st}}_{\text{succ}}$ has the form given in Eq. (3.36) (linear in α alone), to do this, we hold α constant, and maximise $P^{\text{2nd}}_{\text{succ}}$ with respect to β. This occurs when

$$\beta = -\frac{3\alpha}{2} \quad \text{or} \quad \beta = \frac{\alpha}{2}. \tag{3.48}$$

The first option only holds when $\alpha = 0 \notin (2\beta, 1-\beta]$. The second option corresponds to the boundary of the two scenarios in Eq. (3.43) - that is, when $\alpha = 2\beta$. This tells us that for $\alpha > 2\beta$, there are no stationary points with respect to β, and we must therefore look to the boundaries of β: $\beta = 0$ or $\beta = 1-\alpha$. However, the optimal boundary can be shown to be $\beta = 1-\alpha$ when we notice that $P^{\text{2nd}}_{\text{succ}}$ is monotonically increasing with respect to β in the region $\alpha \in (2\beta, 1-\beta],\ \beta \in \left[0, \frac{1}{3}\right]$. This can be shown using the fact that there are no stationary points in this region, so it must therefore be monotonically increasing or decreasing, along with the fact there exists a point [e.g $(\alpha, \beta) = (5/6, 1/6)$] in this region such that $\frac{\partial P^{\text{2nd}}_{\text{succ}}}{\partial \beta} > 0$. So, using $\beta = 1-\alpha$ along with Eq. (3.36), we find the optimal probability of success in this region to be

$$P^{\text{2nd}}_{\text{succ}} = \frac{1}{12} + \frac{P^{\text{1st}}_{\text{succ}}}{2} + \frac{1}{24}\sqrt{3(5 - 8P^{\text{1st}}_{\text{succ}})}. \tag{3.49}$$

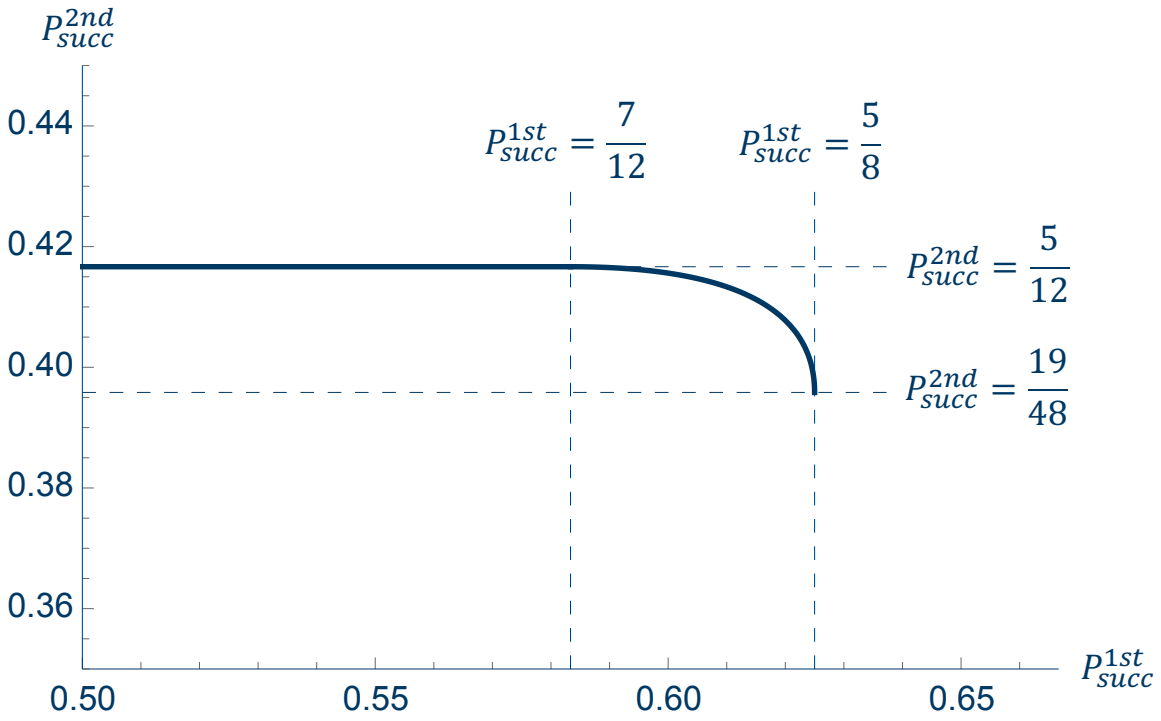

Figure 3.1: Plot of the tradeoff between the success rate of an intermediate binary classification on a subset of two qubits with that of a second binary classification on the entire three-qubit dataset. The probability of success of the first (second) measurement is denoted $P_{\text{succ}}^{\text{1st}}$ ($P_{\text{succ}}^{\text{2nd}}$).

We can re-express the boundaries in $P_{\text{succ}}^{\text{2nd}}$ in terms of $P_{\text{succ}}^{\text{1st}}$ by noting that we'd like Eq. (3.46) to be the success rate for as large a region as possible. This can be seen by noting that Eq. (3.47) can be rewritten as

$$P_{\text{succ}}^{\text{2nd}} = \frac{5}{12} - \frac{1}{48}\left(\sqrt{\alpha+\beta} - \sqrt{3\beta}\right)^2 \tag{3.50}$$

and therefore is less than or equal to the optimal value of 5/12. So, to make the region in which Eq. (3.46) is true as large as possible, we must maximise $\min\{2\beta, 1-\beta\}$. That is, when $\beta = 1/3$ and so $\alpha \in \left[0, \frac{2}{3}\right]$. Therefore, using Eq. (3.36), we take $P_{\text{succ}}^{\text{2nd}}$ to be given by Eq. (3.46) when $P_{\text{succ}}^{\text{1st}} \in \left[\frac{1}{2}, \frac{7}{12}\right]$, and by Eq. (3.49) when $P_{\text{succ}}^{\text{1st}} \in \left(\frac{7}{12}, \frac{5}{8}\right]$.

3.3.3 Results

Summarising what we have found, the tradeoff between the first and second classification is given by

$$P_{\text{succ}}^{\text{2nd}} = \begin{cases} \frac{5}{12} & \text{if } P_{\text{succ}}^{\text{1st}} \in \left[\frac{1}{2}, \frac{7}{12}\right], \\ \frac{1}{12} + \frac{P_{\text{succ}}^{\text{1st}}}{2} + \frac{1}{24}\sqrt{3(5-8P_{\text{succ}}^{\text{1st}})} & \text{if } P_{\text{succ}}^{\text{1st}} \in \left(\frac{7}{12}, \frac{5}{8}\right]. \end{cases} \tag{3.51}$$

A plot of this tradeoff can be seen in Fig. 3.1.

To gain some intuition for this result and plot, it is useful to consider how the three qubit states and second measurement vary with the strength of the first measurement. First, since $\rho_{000}^{\pm}, \pi_{000}^{\pm}$ are left invariant by the first measurement, no intuition is gained by considering them, so we only need look at the remaining states and measurement operators. Noting that they only differ in their $s = 1/2$ path components[7] - that is,

[7] Which agrees with our intuition from before: there are no differences in the numbers they have of each type of qubit (their $\mathcal{Q}_{1/2}^{(3)}$ components). All the differences lie in the order, or permutation, of the qubits (their $\mathcal{P}_{1/2}^{(3)}$ components).

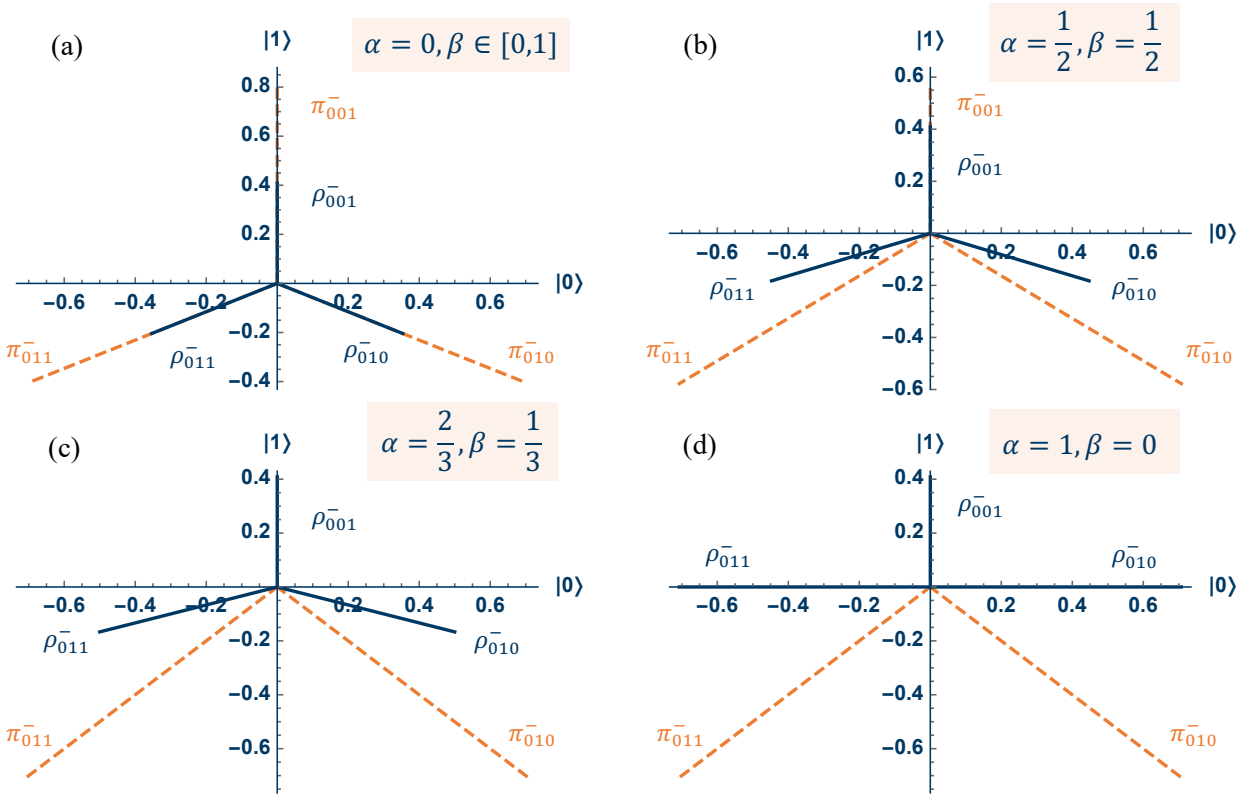

Figure 3.2: Plots showing the effect that a measurement on the first two qubits of a system, with outcome π_- (for various values of α, β), has on the three-qubit states and measurement operators $\{\rho^-_{001}, \rho^-_{010}, \rho^-_{011}\}$ and $\{\pi^-_{001}, \pi^-_{010}, \pi^-_{011}\}$ respectively. Note that the states and measurement operators vary with the strength of the two-qubit measurement until $\alpha = \frac{2}{3}$, $\beta = \frac{1}{3}$ [Fig. 3.2(c)], after which, while the states continue to change, the measurement operators stay constant. Fig. 3.2(c) corresponds to the boundary between the constant and variable regions in Fig. 3.1. Further, Fig. 3.2(a) corresponds to the case in which no measurement is performed on the first two qubits and Fig. 3.2(d) to when the optimal measurement is performed on the first two qubits.

their components when restricted to the subspace $\mathcal{P}^{(3)}_{1/2}$. We do this in Fig. 3.2 which shows how the states $\rho^-_{001}, \rho^-_{010}, \rho^-_{011}$ and measurement operators $\pi^-_{001}, \pi^-_{010}, \pi^-_{011}$ compare to one another for various values of α, β. Note the mirror symmetry of the states and measurement operators in their $|0\rangle$ components throughout, as discussed earlier when constructing the optimal measurement of the three-qubit states. Further, notice that the adjustment of the second measurement appears to compensate for the disturbance caused by the first measurement in the region $\alpha \in [0, \min\{1-\beta, 2\beta\}], \beta \in [0,1]$. This allows for the success rate of the second classification to remain at its optimal value and therefore corresponds to the constant region in Fig. 3.1. When $\alpha \in (2\beta, 1-\beta]$, however, $a_- = 1$ and the second measurement, in some sense, "gives up" trying to compensate for the disturbance caused by the first measurement. This is why we start to see the success rate of the second classification drop off beyond $P^{\text{1st}}_{\text{succ}} = 7/12$. Indeed, it is purely due to the "$-$" outcome that this drop off occurs. This is due to the fact a_+ is given by Eq. (3.44) across the entire range of α, β, meaning the second measurement $\{\pi^+_i\}$ compensates for the first measurement's disturbance throughout (when the outcome is "$+$").

Let's note some points of interest. Firstly, when we require the second measurement to be optimal, the best first measurement occurs when $\alpha = \frac{2}{3}$ and $\beta = 1 - \alpha = \frac{1}{3}$. Here, the intermediate measurement is made

up from

$$\pi_+ = \frac{2}{3}\mathbb{I}_1, \tag{3.52a}$$

$$\pi_- = \frac{1}{3}\mathbb{I}_1 + \mathbb{I}_0. \tag{3.52b}$$

and results in

$$P^{\text{1st}}_{\text{succ}} = \frac{7}{12} \approx 58.3\%, \tag{3.53a}$$

$$P^{\text{2nd}}_{\text{succ}} = \frac{5}{12} \approx 41.7\%. \tag{3.53b}$$

So the success rate of the first measurement, under the requirement that $P^{\text{2nd}}_{\text{succ}}$ is optimal, ranges from $\frac{1}{2}$ to $\frac{7}{12}$. It is worth reiterating that the transition from optimal to sub-optimal second-measurement success rate occurs at the boundary of the two cases in Eq. (3.51) or Eq. (3.43). That is, given a first outcome of π_-, when the second measurement stops varying with respect to α, β as can be seen in Fig. 3.2.

The next point to consider is when we optimise $P^{\text{1st}}_{\text{succ}}$. Here $\alpha = 1$ and $\beta = 1 - \alpha = 0$ which means that

$$P^{\text{1st}}_{\text{succ}} = \frac{5}{8} = 62.5\%, \tag{3.54a}$$

$$P^{\text{2nd}}_{\text{succ}} = \frac{19}{48} \approx 39.6\%, \tag{3.54b}$$

as was found in Sections 3.2.1 and 3.3.1. This limited success rate of the second measurement can perhaps be expected due to the fact the $\rho^-_{010}, \rho^-_{011}$ are parallel to one another as can be seen in Fig. 3.2(d).

3.4 Three-qubit disturbance as a quantum circuit

In this section we show how the protocol of the previous sections can be carried out on a quantum computer, by expressing it as quantum circuit. But before we do this, let's go over the preliminaries required to understand the approach we take.

3.4.1 POVM as a sequence of two-outcome measurements

It turns out that we can perform our POVMs of interest as a sequence of two-outcome measurements [111, 112]. Let's see how this works for one of the three qubit measurements we aim to perform in our quantum circuit. Namely, $\{\pi^-_{000}, \pi^-_{001}, \pi^-_{010}, \pi^-_{011}\}$ to distinguish the states $\{\rho^-_{000}, \rho^-_{001}, \rho^-_{010}, \rho^-_{011}\}$, discussed in Sec. 3.3.2.2:

$$\pi^-_{000} = \mathbb{I}_{\frac{3}{2}}, \tag{3.55a}$$

$$\pi^-_{001} = \frac{2\beta - \alpha}{3\beta}\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{3.55b}$$

$$\pi^-_{010} = \frac{1}{2}\mathbb{I}_{\frac{1}{2}} \otimes \left(\sqrt{\frac{\alpha+\beta}{3\beta}}|1\rangle - |0\rangle\right)\left(\sqrt{\frac{\alpha+\beta}{3\beta}}\langle 1| - \langle 0|\right), \tag{3.55c}$$

$$\pi^-_{011} = \frac{1}{2}\mathbb{I}_{\frac{1}{2}} \otimes \left(\sqrt{\frac{\alpha+\beta}{3\beta}}|1\rangle + |0\rangle\right)\left(\sqrt{\frac{\alpha+\beta}{3\beta}}\langle 1| + \langle 0|\right), \tag{3.55d}$$

where $\alpha \in [0, \min\{1-\beta, 2\beta\}]$, $\beta \in [0, 1]$. Define $\{M_{ijk}\}$ to be the set of measurement operators corresponding to the POVM $\{\pi^-_{ijk}\}$:

$$\pi^-_{ijk} = {M_{ijk}}^\dagger M_{ijk}. \tag{3.56}$$

We will be taking $M_{ijk} = \sqrt{\pi^-_{ijk}}$.

Step 1: 000 **vs.** $\overline{000}$

Suppose we are performing the measurement $\{\pi^-_{ijk}\}$ on some state ρ_1. In this first step, our aim is to perform a measurement[8] $\{N_{000}, N_{\overline{000}}\}$ that distinguishes ρ_{000} from the other possible states $\rho_{001}, \rho_{010}, \rho_{011}$. That is, the two outcomes of this first step are $\mathcal{O}^{(1)} = 000$ and $\mathcal{O}^{(1)} = \overline{000}$, where $\overline{000}$ means *"not* 000*"*, and $\mathcal{O}^{(j)}$ denotes the outcome of the jth step. Explicitly, and taking into account Eq. (3.55) with $M_{ijk} = \sqrt{\pi^-_{ijk}}$,

$$N_{000} = M_{000} = \mathbb{I}_{\frac{3}{2}}, \tag{3.57a}$$

$$N_{\overline{000}} = \sqrt{\mathbb{I} - |N_{000}|^2} = \mathbb{I}_{\frac{1}{2}\otimes\frac{1}{2}}, \tag{3.57b}$$

where $|N_{ijk}|^2 := N^\dagger_{ijk} N_{ijk}$ and $\mathbb{I}$ is the identity on the entire Hilbert space. We denote the corresponding POVM to this measurement $\{\pi_{000}, \pi_{\overline{000}}\}$, such that $\pi_{000} = N^\dagger_{000} N_{000}, \pi_{\overline{000}} = N^\dagger_{\overline{000}} N_{\overline{000}}$.

If we find $\mathcal{O}^{(1)} = 000$, we have obtained a valid outcome so we can stop here. If, however $\mathcal{O}^{(1)} = \overline{001}$, the conclusion we must draw is that ρ_1 is *not* the state ρ_{000}. Therefore, to figure out which state ρ_1 is, we must carry on to Step 2.

Step 2: 001 **vs.** $\overline{001}$

Note, at this stage of the protocol, an outcome of $\mathcal{O}^{(1)} = \overline{000}$ meant that we should restrict our attention to $\mathcal{L}(\mathcal{Q}_{1/2} \otimes \mathcal{P}_{1/2})$, which we do from here on. The aim of this step is to perform a measurement $\{N_{001}, N_{\overline{001}}\}$ that distinguishes ρ_{001} from ρ_{010}, ρ_{011}. To write down this measurement we should note that we are receiving an updated state ρ_2 from Step 1:

$$\rho_2 \propto N_{\overline{000}} \rho_1 N^\dagger_{\overline{000}}, \tag{3.58}$$

meaning that the effects of the Step 1 measurement must be taken into account in $\{N_{001}, N_{\overline{001}}\}$. We write these operators as follows:

$$N_{001} = M_{001} N^{-1}_{\overline{000}}, \tag{3.59a}$$

$$N_{\overline{001}} = \sqrt{\mathbb{I}_{\frac{1}{2}\otimes\frac{1}{2}} - |N_{001}|^2}, \tag{3.59b}$$

where N^{-1}_{ijk} denotes the Moore-Penrose inverse of N_{ijk} [111]. Using Eq. (3.55), $M_{001} = \sqrt{\pi^-_{001}}$ and $N_{\overline{000}} = \mathbb{I}_{\frac{1}{2}\otimes\frac{1}{2}} = N^{-1}_{\overline{000}}$, we can write these explicitly as

$$W_{001} N_{001} = \sqrt{\frac{2\beta - \alpha}{3\beta}} \mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{3.60a}$$

$$W_{\overline{001}} N_{\overline{001}} = \mathbb{I}_{\frac{1}{2}} \otimes \left(\sqrt{\frac{\alpha + \beta}{3\beta}} |1\rangle\langle 1| + |0\rangle\langle 0| \right), \tag{3.60b}$$

where W_{ijk} are the unitaries arising from from the non-uniqueness of the square root $\sqrt{\pi^-_{ijk}}$. As before, if $\mathcal{O}^{(2)} = 001$, we conclude that ρ_1 was prepared in the state ρ_{001}, but if $\mathcal{O}^{(2)} = \overline{001}$, we progress to the third and final step.

Step 3: 010 **vs.** 011

If we have made it to this stage, we have found that $\mathcal{O}^{(1)} \neq 000$, $\mathcal{O}^{(2)} \neq 001$, so we must conclude that the state ρ_1 is either ρ_{010} or ρ_{011}. So, similarly to the other steps, our task is to write down a measurement $\{N_{010}, N_{011}\}$ that distinguishes between these final two options. Just as we saw in Step 2, the state received at this step is

$$\rho_3 \propto N_{\overline{001}} \rho_2 N^\dagger_{\overline{001}} \propto N_{\overline{001}} N_{\overline{000}} \rho_1 N^\dagger_{\overline{000}} N^\dagger_{\overline{001}} = N_{\overline{001}} \rho_1 N^\dagger_{\overline{001}}, \tag{3.61}$$

[8] That is, $N_{000}, N_{\overline{000}}$ are measurement operators, not POVM elements.

where the last equality comes from $N_{\overline{000}} = \mathbb{I}_{\frac{1}{2}\otimes\frac{1}{2}}$. Therefore, $\{N_{010}, N_{011}\}$ must, in some sense, include the reversal of $N_{\overline{001}}$. That is,

$$N_{010} = M_{010}N_{\overline{001}}^{-1}, \tag{3.62a}$$

$$N_{011} = M_{011}N_{\overline{001}}^{-1}, \tag{3.62b}$$

where

$$M_{01k} = \sqrt{\pi_{01k}^{-}} = \sqrt{\frac{6\beta}{\alpha+4\beta}}W_{01k}\pi_{01k}^{-}. \tag{3.63}$$

Here, $W_{01k} \in \mathcal{L}(\mathcal{Q}_{1/2} \otimes \mathcal{P}_{1/2})$ are unitaries that arise in the square root of π_{01k}^{-}. Explicitly, N_{01k} are defined as follows:

$$W_{010}N_{010} = \frac{1}{\sqrt{2(\alpha+4\beta)}}\mathbb{I}_{\frac{1}{2}} \otimes \Big(\sqrt{\alpha+\beta}|1\rangle - \sqrt{3\beta}|0\rangle\Big)\Big(\langle 1| - \langle 0|\Big), \tag{3.64a}$$

$$W_{010}N_{011} = \frac{1}{\sqrt{2(\alpha+4\beta)}}\mathbb{I}_{\frac{1}{2}} \otimes \Big(\sqrt{\alpha+\beta}|1\rangle + \sqrt{3\beta}|0\rangle\Big)\Big(\langle 1| + \langle 0|\Big). \tag{3.64b}$$

These operators give us access to final two possible measurement outcomes $\mathcal{O}^{(3)} = 010, 011$, thus completing this implementation of $\{\pi_{ijk}^{-}\}$.

To make it clearer what measurement is actually being performed at this step, it is useful to consult the corresponding POVM $\{N_{010}^\dagger N_{010}, N_{011}^\dagger N_{011}\}$:

$$N_{010}^\dagger N_{010} = \mathbb{I}_{\frac{1}{2}} \otimes |-\rangle\langle -|, \tag{3.65a}$$

$$N_{011}^\dagger N_{011} = \mathbb{I}_{\frac{1}{2}} \otimes |+\rangle\langle +|. \tag{3.65b}$$

Thus, it is really just a Pauli-x measurement in the path component.

Why decompose a POVM in this way?

The reason for decomposing our POVMs in this way is that, as we will see later, we can conveniently express the above two-outcome measurements as quantum circuits. Indeed, any two-outcome qubit measurement $\{N_0, N_1\}$ can be decomposed into parts that can be carried out on a quantum computer using rotation R_X, R_Y, R_Z and controlled-P gates [112]. Explicitly for this qubit case, note first that, being a measurement,

$$N_0^\dagger N_0 + N_1^\dagger N_1 = \mathbb{1}, \tag{3.66}$$

which means $[N_0^\dagger N_0, N_1^\dagger N_1] = 0$, and thus, there exists some unitary V that simultaneously diagonalises $N_i^\dagger N_i$ for $i = 0, 1$. So, using the singular value decomposition, we can write (for $i = 0, 1$)

$$N_i = U_i D_i V^\dagger, \tag{3.67}$$

where U_i are unitaries, and D_i are diagonal measurement operators. Since there are two possible outcomes $0, 1$, N_i can be expressed in terms of some two-dimensional basis, and thus, D_i can be written as

$$D_0 = \sqrt{p}|u\rangle\langle u| + \sqrt{1-q}|v\rangle\langle v|, \tag{3.68a}$$

$$D_1 = \sqrt{1-p}|u\rangle\langle u| + \sqrt{q}|v\rangle\langle v|, \tag{3.68b}$$

for some $p, q \in [0, 1]$, and $|u\rangle, |v\rangle$ satisfying $\langle u|v\rangle = \delta_{uv}$. All three elements of this decomposition $U_i, \{D_i\}, V$ are (relatively) easily represented as quantum circuits, making it a natural route to take in writing our sequential classification protocol as a quantum circuit. Let's write down $U_i, \{D_i\}, V$ for each step of the measurement described above.

Step 1 - The measurement in this step doesn't actually correspond to the qubit measurement situation described in Eqs. (3.66 - 3.68). However, since it is already a projective measurement, we will see that we can perform this on a quantum computer.

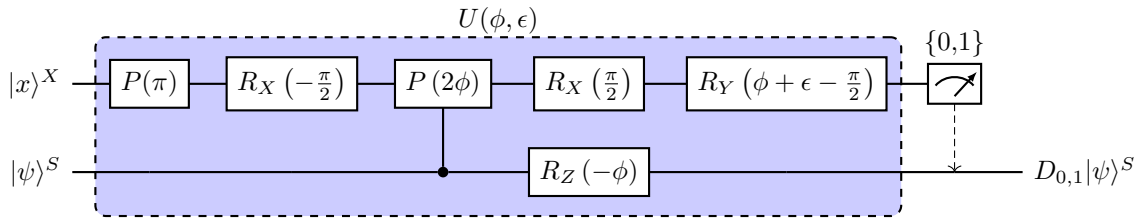

Figure 3.3: Circuit that performs the generalised two-outcome measurement $\{D_0, D_1\}$ on the state $|\psi\rangle$. We take the unitary performed within the purple box to be called $U(\phi, \epsilon)$.

Step 2 - Again, this measurement $\{N_{001}, N_{\overline{001}}\}$ isn't on a qubit. However, since $\pi^-_{001}, \pi^-_{010}, \pi^-_{011}$ share the same $\mathcal{L}(\mathcal{Q}_{1/2})$ projection $\mathbb{I}_{1/2}$, we can think of this as as a three-outcome measurement on the qubit space $\mathcal{L}(\mathcal{P}_{1/2})$. So, although we also include the projection $\mathbb{I}_{1/2}$ for completeness, the techniques of Eqs. (3.67,3.68) apply here. Indeed, the $\mathcal{L}(\mathcal{P}_{1/2})$ components of $N_{001}, N_{\overline{001}}$ are already in the diagonal form we'd like to have in D_{001}, $D_{\overline{001}}$, meaning that we can take $D_{001} = N_{001}, D_{\overline{001}} = N_{\overline{001}}$, and $U_{001} = \mathbb{I}_{\frac{1}{2}\otimes\frac{1}{2}} = U_{\overline{001}} = V_2$.

Step 3 - Finally, we saw that the POVM corresponding to $\{N_{010}, N_{011}\}$ was effectively just the Pauli-x measurement on the path degree of freedom. This makes the following decomposition unsurprising. Namely, that $\{N_{010}, N_{011}\}$ can be diagonalised to

$$D_{010} = \mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{3.69a}$$

$$D_{011} = \mathbb{I}_{\frac{1}{2}} \otimes |0\rangle\langle 0|, \tag{3.69b}$$

using $V_3 = \mathbb{I}_{\frac{1}{2}} \otimes H$, where H is the Hadamard matrix [Eq. (2.50)], and some unitaries U_{01k}, defined via

$$U_{010}\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle = \frac{1}{\sqrt{(\alpha+4\beta)}}\mathbb{I}_{\frac{1}{2}} \otimes \Big(\sqrt{\alpha+\beta}|1\rangle - \sqrt{3\beta}|0\rangle\Big), \tag{3.70a}$$

$$U_{011}\mathbb{I}_{\frac{1}{2}} \otimes |0\rangle = \frac{1}{\sqrt{(\alpha+4\beta)}}\mathbb{I}_{\frac{1}{2}} \otimes \Big(\sqrt{\alpha+\beta}|1\rangle + \sqrt{3\beta}|0\rangle\Big). \tag{3.70b}$$

3.4.2 Generalised quantum measurement as a quantum circuit

In the gate model of quantum computers, quantum information is accessed using projective measurements onto basis kets $|b_i\rangle$ of each qubit (or qudit). This is done by first performing a unitary operation to change the basis of the qubits to be measured into the basis of the measurement apparatus $\{|b_i\rangle\}$. Following this, the projective measurement $\{|b_i\rangle\langle b_i|\}$ can be performed. However, generalised, non-orthogonal measurements (or POVMs) are often of interest which leads to the question of how we can do this if our measurement apparatus only allows for projective measurements. The answer comes from the Naimark (or Neumark) extension [17, 22, 111] discussed in Sec. 2.2.5, which says that using an extra ancilliary system X, any POVM acting on a system S can be thought of as a unitary transformation of the composite system SX followed by a projective measurement on X.

We also saw in Sec. 3.4.1 that our measurements of interest can be decomposed into a series of two-outcome measurements, expressible as a combination of unitary operations and diagonal measurement operators $\{D_0, D_1\}$, as described in Eqs. (3.67, 3.68). Such a "diagonal measurement" can then be carried out using the quantum circuit presented in Fig. 3.3. In this circuit diagram, deviating briefly from our normal labelling convention, $|x\rangle^X$ is the state (initially $|0\rangle$) of the ancilla qubit X required by the Naimark extension to perform the POVM $\{D_0^\dagger D_0, D_1^\dagger D_1\}$ on the state $|\psi\rangle^S$ of the system S. Taking

$$\phi = \frac{1}{2}\left[\sin^{-1}(2p-1) + \sin^{-1}(2q-1)\right], \tag{3.71a}$$

$$\epsilon = \frac{1}{2}\left[\sin^{-1}(2p-1) - \sin^{-1}(2q-1)\right], \tag{3.71b}$$

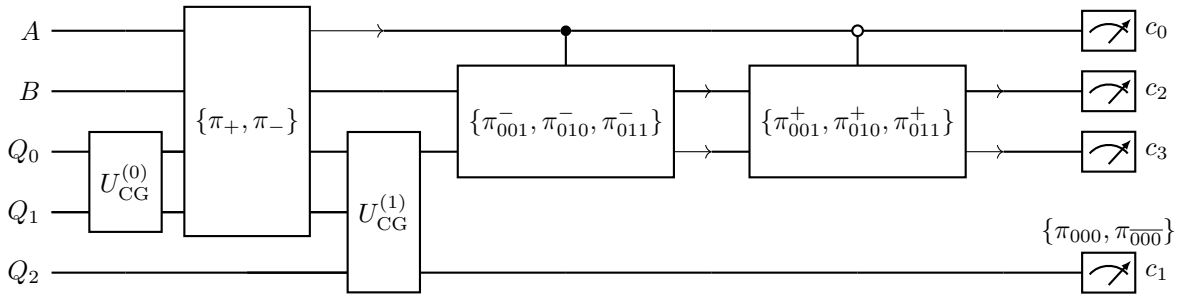

Figure 3.4: Circuit diagram outlining how we implement the sequential three-qubit classification of Sec. 3.3 as a quantum circuit. The arrows output from each measurement indicate which qubit(s) holds the corresponding measurement outcome(s). If a qubit is not used after an operation, we terminate its corresponding line at said operation.

and denoting the circuit in Fig. 3.3 (before the measurement) by $U(\phi, \epsilon)$, we can observe that the projective measurement $\{|0\rangle\langle 0|^X, |1\rangle\langle 1|^X\}$ on X with outcomes $0, 1$ forces the following operations on S:

$$\langle 0|^X U(\phi,\epsilon)|0\rangle^X = \sqrt{\frac{1+\sin(\phi+\epsilon)}{2}}|0\rangle\langle 0|^S + \sqrt{\frac{1-\sin(\phi-\epsilon)}{2}}|1\rangle\langle 1|^S \equiv D_0, \tag{3.72a}$$

$$\langle 1|^X U(\phi,\epsilon)|1\rangle^X = \sqrt{\frac{1-\sin(\phi+\epsilon)}{2}}|0\rangle\langle 0|^S + \sqrt{\frac{1+\sin(\phi-\epsilon)}{2}}|1\rangle\langle 1|^S \equiv D_1 \tag{3.72b}$$

respectively.

3.4.3 Circuit setup and first measurement

We are now equipped to understand the quantum circuit we constructed to perform the sequential classification of Sec. 3.3. Let's begin by setting up our quantum circuit. In order to perform this scenario using a quantum circuit, aside from the three qubits we are classifying, denoted Q_0, Q_1, Q_2, we use two ancilla qubits A, B. All of these qubits are initially prepared in the state $|0\rangle$. The general outline of how we carry out this protocol as a quantum circuit can be found in Fig. 3.4. Let's go through and see how each part works.

The first thing to do in our circuit is perform the POVM $\{\pi_\pm\}$ on the first two qubits Q_0Q_1. Recall that, to do this, we use the POVM given in Eq. (3.34), which can be rewritten as

$$\pi_+ = (1-\beta)P_+ + (1-\alpha-\beta)P_-, \tag{3.73a}$$

$$\pi_- = \beta P_+ + (\alpha+\beta)P_-, \tag{3.73b}$$

such that $\alpha \in [0, 1-\beta]$ and $\beta \in [0,1]$. Noting that these are written in the two-qubit Schur basis given in Eq. (2.143), we must first convert the state of Q_0Q_1 into the Schur basis of $\left(\mathcal{Q}_1^{(2)} \otimes \mathcal{P}_1^{(2)}\right) \oplus \left(\mathcal{Q}_0^{(2)} \otimes \mathcal{P}_0^{(2)}\right)$. Given that there's a trivial path degree of freedom when considering two qubits, the quantum Schur-Weyl transform (QSWT) in this case corresponds to the Clebsch-Gordon transform $U_{\mathrm{CG}}^{(0)}$ of two spin-half particles[9] [72]. This can be done using the circuit depicted in Fig. 3.5. Concentrating on Q_0Q_1, this does the following to the basis states given in Eq. (2.143):

$$\begin{aligned} s=1 \ &\begin{cases} |00\rangle \ \to |00\rangle\,, \\ \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \ \to |01\rangle\,, \\ |11\rangle \ \to |10\rangle\,, \end{cases} \\ s=0 \ &\left\{ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \ \to |11\rangle\,. \right. \end{aligned} \tag{3.74}$$

[9] We include the superscript in $U_{\mathrm{CG}}^{(0)}$ as we require the use of a second Clebsch-Gordon transform $U_{\mathrm{CG}}^{(1)}$ when we consider the three-qubit QSWT later.

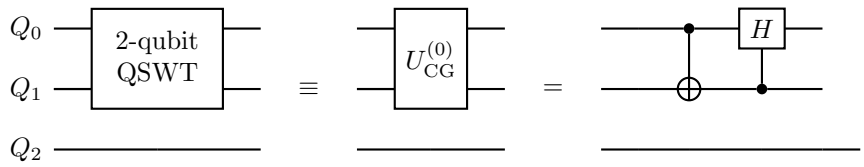

Figure 3.5: Circuit diagram of a two-qubit quantum Schur-Weyl transform (QSWT). This is equivalent the Clebsch-Gordon transform $U_{\mathrm{CG}}^{(0)}$ on two spin-half particles.

Now, note that the first measurement, given in Eq. (3.73), really only has two degrees of freedom: one in the $s = 1$ space, $\mathcal{Q}_1^{(2)} \otimes \mathcal{P}_1^{(2)}$ and one in the $s = 0$ space, $\mathcal{Q}_0^{(2)} \otimes \mathcal{P}_0^{(2)}$. We can transfer the information about the spin onto an ancilla qubit B, initially in the state $|0\rangle$, using a Toffoli gate controlled on Q_0Q_1. Given our two qubit states [Eq. (3.12)], which can be rewritten as

$$\rho_{00} = \frac{1}{3}\mathbb{I}_1, \tag{3.75a}$$

$$\rho_{01} = \frac{1}{4}\mathbb{I}_1 + \frac{1}{4}\mathbb{I}_0, \tag{3.75b}$$

this does the following:

$$|0\rangle\langle 0|^{(B)} \otimes \rho_{00}^{(Q_0Q_1)} = |0\rangle\langle 0| \otimes \frac{1}{3}\mathbb{I}_1 \to \frac{1}{3}|0\rangle\langle 0| \otimes \mathbb{I}_1, \tag{3.76a}$$

$$|0\rangle\langle 0|^{(B)} \otimes \rho_{01}^{(Q_0Q_1)} = |0\rangle\langle 0| \otimes \frac{1}{4}(\mathbb{I}_1 + \mathbb{I}_0) \to \frac{1}{4}|0\rangle\langle 0| \otimes \mathbb{I}_1 + \frac{1}{4}|1\rangle\langle 1| \otimes \mathbb{I}_0, \tag{3.76b}$$

where ρ_i and $\mathbb{I}_s$ are encoded on Q_0Q_1 and the remaining component is encoded in B as indicated by the superscripts on the left hand side. The thing to notice from this is that B is in the state $|1\rangle$ only when the state of Q_0Q_1 is in $\mathcal{Q}_0^{(2)} \otimes \mathcal{P}_0^{(2)}$. So, performing the PVM $\{P_+, P_-\}$ on Q_0Q_1 is equivalent to performing the PVM $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ on B, such that an outcome of $+$ $(-)$ on Q_0Q_1 corresponds to an outcome of 0 (1) on B. Therefore, instead of performing the POVM $\{\pi_\pm\}$, written in Eq. (3.73), on Q_0Q_1, we can perform the POVM, with elements

$$\tilde{\pi}_+ = (1-\beta)|0\rangle\langle 0| + (1-\alpha-\beta)|1\rangle\langle 1|, \tag{3.77a}$$

$$\tilde{\pi}_- = \beta|0\rangle\langle 0| + (\alpha+\beta)|1\rangle\langle 1|, \tag{3.77b}$$

on B and then transfer the post measurement state information back to Q_0Q_1 using another Toffoli gate.

Relating to the work of [112], and Eq. (3.68), since $\tilde{\pi}_\pm$ are diagonal, we can see directly that

$$D_{0/1} = \sqrt{\tilde{\pi}_{+/-}} \tag{3.78}$$

if $p = 1-\beta, q = \alpha+\beta$, $|u\rangle = |0\rangle, |v\rangle = |1\rangle$. So, in order to perform this first measurement, we use the circuit given in Fig. 3.3 with

$$\phi = \phi_1 := \frac{1}{2}\left[\sin^{-1}(1-2\beta) + \sin^{-1}(2\alpha+2\beta-1)\right], \tag{3.79a}$$

$$\epsilon = \epsilon_1 := \frac{1}{2}\left[\sin^{-1}(1-2\beta) - \sin^{-1}(2\alpha+2\beta-1)\right] \tag{3.79b}$$

and $X = A, S = B$. The subscripts in ϕ_1, ϵ_1, indicate that this is the first measurement. So, following on from Eq. (3.76), applying the Toffoli gate and $U(\phi_1, \epsilon_1)$ on ABQ_0Q_1, our states would be updated as follows:

$$|00\rangle\langle 00|^{(AB)} \otimes \rho_{00}^{(Q_0Q_1)} \to \frac{1}{3}\left[|0\rangle\langle 0| \otimes \left(\sqrt{\tilde{\pi}_+}|0\rangle\langle 0|\sqrt{\tilde{\pi}_+}^\dagger\right) + |1\rangle\langle 1| \otimes \left(\sqrt{\tilde{\pi}_-}|0\rangle\langle 0|\sqrt{\tilde{\pi}_-}^\dagger\right)\right] \otimes \mathbb{I}_1, \tag{3.80a}$$

$$\begin{aligned}|00\rangle\langle 00|^{(AB)} \otimes \rho_{01}^{(Q_0Q_1)} \to &\frac{1}{4}\left[|0\rangle\langle 0| \otimes \left(\sqrt{\tilde{\pi}_+}|0\rangle\langle 0|\sqrt{\tilde{\pi}_+}^\dagger\right) + |1\rangle\langle 1| \otimes \left(\sqrt{\tilde{\pi}_-}|0\rangle\langle 0|\sqrt{\tilde{\pi}_-}^\dagger\right)\right] \otimes \mathbb{I}_1 \\ &+ \frac{1}{4}\left[|0\rangle\langle 0| \otimes \left(\sqrt{\tilde{\pi}_+}|1\rangle\langle 1|\sqrt{\tilde{\pi}_+}^\dagger\right) + |1\rangle\langle 1| \otimes \left(\sqrt{\tilde{\pi}_-}|1\rangle\langle 1|\sqrt{\tilde{\pi}_-}^\dagger\right)\right] \otimes \mathbb{I}_0.\end{aligned} \tag{3.80b}$$

If we then reapply the same Toffoli gate controlled on Q_0Q_1 with target B, noting that we've rearranged the qubits in order to write the states down more succinctly, we end up with

$$|00\rangle\langle 00|^{(BA)} \otimes \rho_{00}^{(Q_0Q_1)} \to \frac{1}{3}|0\rangle\langle 0| \otimes \Big[|0\rangle\langle 0| \otimes \Big(\sqrt{\pi_+}\,\mathbb{I}_1\sqrt{\pi_+}^\dagger\Big) + |1\rangle\langle 1| \otimes \Big(\sqrt{\pi_-}\,\mathbb{I}_1\sqrt{\pi_-}^\dagger\Big)\Big], \tag{3.81a}$$

$$|00\rangle\langle 00|^{(BA)} \otimes \rho_{01}^{(Q_0Q_1)} \to \frac{1}{4}|0\rangle\langle 0| \otimes \Big[|0\rangle\langle 0| \otimes \Big(\sqrt{\pi_+}\,\mathbb{I}_1\sqrt{\pi_+}^\dagger + \sqrt{\pi_+}\,\mathbb{I}_0\sqrt{\pi_+}^\dagger\Big) + |1\rangle\langle 1| \otimes \Big(\sqrt{\pi_-}\,\mathbb{I}_1\sqrt{\pi_-}^\dagger + \sqrt{\pi_-}\,\mathbb{I}_0\sqrt{\pi_-}^\dagger\Big)\Big]. \tag{3.81b}$$

From here, it is clear to see that if we measure A in the z-basis[10], an outcome of $0\,(1)$ corresponds to a measurement outcome of $+\,(-)$ on Q_0Q_1. Notice also that B is guaranteed to return to its initial state of $|0\rangle$, meaning we are free to use it in our later steps.

All together, the circuit used to perform the first measurement and update our three-qubit states in the way given in Eq. (2.85) is given in Fig. 3.6. The arrow exiting $U(\phi_1, \epsilon_1)$ indicates the qubit that contains the $\{\pi_\pm\}$ measurement outcome. Note that until A is measured, the system is left in a mixture of the two possible outcomes: 0 or 1, as written explicitly in Eq. (3.81). The approach taken here waits until the end of the whole protocol to measure A and, instead, uses it as a control qubit to dictate whether the second measurement will be $\{\pi_{ijk}^+\}$ or $\{\pi_{ijk}^-\}$ (corresponding to A being in the state $|0\rangle$ or $|1\rangle$ respectively). Alternatively, one could measure A earlier and perform the subsequent measurement based on the classical measurement result. This would save quantum resources, but the platform we used to simulate this circuit (Qiskit) was, at the time, less amenable to this latter approach of classical conditioning. When A is eventually measured, the outcome will be mapped onto the classical bit c_0 with $c_0 = 0$ corresponding to a measurement outcome[11] of $\mathcal{O}_1 = +$ and $c_0 = 1$ to $\mathcal{O}_1 = -$.

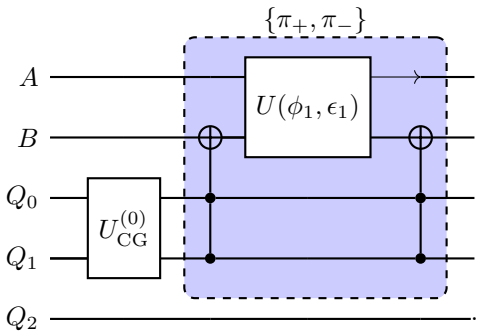

Figure 3.6: Circuit diagram corresponding to the intermediate measurement $\{\pi_+^{(Q_0Q_1)}, \pi_-^{(Q_0Q_1)}\}$ given in Eq. (3.73). The operation $U_{\mathrm{CG}}^{(0)}$ indicates the two-qubit QSWT used to put the state in the Schur basis, and the blue box corresponds to the measurement $\{\pi_\pm\}$. The arrow output from $U(\phi_1, \epsilon_1)$ indicates the qubit that the measurement result is contained within.

3.4.4 Second measurement

Due to the piece-wise nature of the second measurement $\{\pi_{ijk}^-\}$, different circuits are required for the two regions. We discuss these separately in the two following subsections: first, the region corresponding to the constant portion of the tradeoff in Fig. 3.1 which we call Region I. We then go onto discuss the variable region, which we call Region II, of this tradeoff.

[10] The assumed single qubit basis of measurement in a quantum circuit.

[11] We will denote the ith measurement outcome as $\mathcal{O}_i$. If there are multiple steps within a measurement, the outcome of the jth step of the ith measurement will be denoted $\mathcal{O}_i^{(j)}$.

3.4.4.1 Region I

We begin by discussing the, more complicated, constant region in Eq. (3.51). That is, when $\alpha \in [0, \min\{1-\beta, 2\beta\}], \beta \in [0,1]$. Here, using $a_- = \sqrt{(\alpha+\beta)/3\beta}$ and Eq. (3.41),

$$\pi^-_{000} = \mathbb{I}_{\frac{3}{2}}, \tag{3.82a}$$

$$\pi^-_{001} = \frac{2\beta-\alpha}{3\beta}\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{3.82b}$$

$$\pi^-_{010} = \frac{1}{2}\mathbb{I}_{\frac{1}{2}} \otimes \left(\sqrt{\frac{\alpha+\beta}{3\beta}}|1\rangle - |0\rangle\right)\left(\sqrt{\frac{\alpha+\beta}{3\beta}}\langle 1| - \langle 0|\right), \tag{3.82c}$$

$$\pi^-_{011} = \frac{1}{2}\mathbb{I}_{\frac{1}{2}} \otimes \left(\sqrt{\frac{\alpha+\beta}{3\beta}}|1\rangle + |0\rangle\right)\left(\sqrt{\frac{\alpha+\beta}{3\beta}}\langle 1| + \langle 0|\right), \tag{3.82d}$$

and $\{\pi^+_{ijk}\}$ can be found using the swaps in Eq. (3.35)[12].

Now that we are considering the three-qubit measurement, we now require our states $\rho^{\pm}_{ijk}$ to be in the three-qubit Schur basis given in Eq. (2.145). As is discussed in more detail, and more generally in Ref. [72], the three-qubit QSWT can expressed as a quantum circuit using sequential Clebsch-Gordon transforms $U^{(0)}_{\text{CG}}, U^{(1)}_{\text{CG}}$. In this picture, step one corresponds to putting the state of Q_0Q_1 in the two-qubit Schur basis using $U^{(0)}_{\text{CG}}$, after which $U^{(1)}_{\text{CG}}$ adds the extra "spin-half particle" Q_2 thereby putting the state of the whole system $Q_0Q_1Q_2$ in the Schur basis. This is depicted in Fig. 3.7.

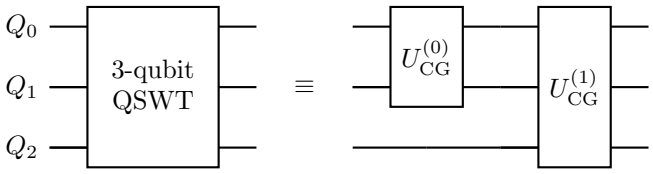

Figure 3.7: Schematic of how a three-qubit QSWT can be performed as a quantum circuit using sequential Clebsch-Gordon transforms. More detail can be found in Ref. [72].

More explicitly, we use a slightly adapted version of the circuit used in [113] to perform the three-qubit QSWT, as shown in Fig. 3.8.

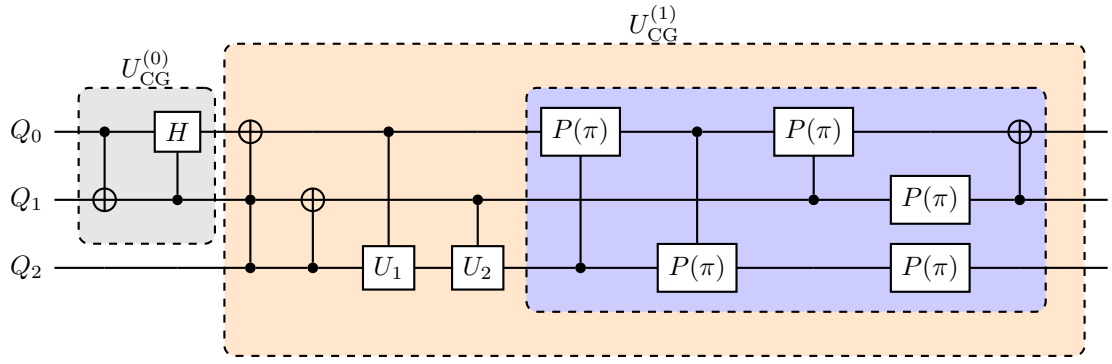

Figure 3.8: Circuit implementation of a three-qubit quantum Schur-Weyl transform.

[12] Recall that $\{\pi^+_{ijk}\}$ has this form for all α, β.

Here,

$$U_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & \sqrt{2} \\ -\sqrt{2} & 1 \end{pmatrix} = R_Y\left(-2\cos^{-1}\sqrt{\frac{1}{3}}\right), \tag{3.83a}$$

$$U_2 = \frac{1}{\sqrt{3}}\begin{pmatrix} \sqrt{2} & 1 \\ 1 & -\sqrt{2} \end{pmatrix} = ZR_Y\left(-2\cos^{-1}\sqrt{\frac{2}{3}}\right). \tag{3.83b}$$

Note that, by this stage in our protocol, the state of Q_0Q_1 is already in the two-qubit Schur basis. Therefore, we need not carry out $U_{\text{CG}}^{(0)}$ as this has already been done. Note also that the gates in the purple box in Fig. 3.8 do not feature in [113] but are included here in order for the Schur basis to match the one chosen in Eq. (2.145).

The above circuit maps the basis states in Eq. (2.145) as follows:

$$\begin{aligned}
\mathcal{Q}^{(3)}_{\frac{3}{2}} \otimes \mathcal{P}^{(3)}_{\frac{3}{2}} : \quad & \left|\frac{3}{2},\frac{3}{2}\right\rangle \to |000\rangle^{(Q_0Q_1Q_2)}, \\
& \left|\frac{3}{2},\frac{1}{2}\right\rangle \to -|110\rangle, \\
& \left|\frac{3}{2},-\frac{1}{2}\right\rangle \to |100\rangle, \\
& \left|\frac{3}{2},-\frac{3}{2}\right\rangle \to |010\rangle, \\
\mathcal{Q}^{(3)}_{\frac{1}{2}} \otimes \mathcal{P}^{(3)}_{\frac{1}{2}} : \quad & \left|\frac{1}{2},\frac{1}{2}\right\rangle|1\rangle \to |111\rangle, \\
& \left|\frac{1}{2},-\frac{1}{2}\right\rangle|1\rangle \to -|101\rangle, \\
& \left|\frac{1}{2},\frac{1}{2}\right\rangle|0\rangle \to -|011\rangle, \\
& \left|\frac{1}{2},-\frac{1}{2}\right\rangle|0\rangle \to -|001\rangle,
\end{aligned} \tag{3.84}$$

where, as indicated in the first line, these three-qubit states are encoded on the qubits Q_0, Q_1, Q_2. Note that the subspaces $\mathcal{Q}^{(3)}_{\frac{3}{2}} \otimes \mathcal{P}^{(3)}_{\frac{3}{2}}$ and $\mathcal{Q}^{(3)}_{\frac{1}{2}} \otimes \mathcal{P}^{(3)}_{\frac{1}{2}}$ can be distinguished based on the state of Q_2. So we can interpret Q_2 as the "total spin" qubit, where $|0\rangle^{Q_2} := |s = 3/2\rangle$ and $|1\rangle^{Q_2} := |s = 1/2\rangle$. Further, notice that the basis vectors of $\mathcal{Q}^{(3)}_{\frac{1}{2}} \otimes \mathcal{P}^{(3)}_{\frac{1}{2}}$ are mapped to states of the form $|q_0, q_1, q_2\rangle^{(Q_0Q_1Q_2)} = |p, m, s\rangle$ where p denotes the path (permutation) degree of freedom and $|0\rangle := |m = -1/2\rangle$, $|1\rangle := |m = 1/2\rangle$ denotes the z-component of the spin. Let's now follow the three-step protocol of Sec. 3.4.1 to carry out $\{\pi^{\pm}_{ijk}\}$.

Step 1: 000 **vs.** $\overline{000}$

The form of $\{\pi^{\pm}_{ijk}\}$ hints that we can use Q_2 to differentiate $\pi^{\pm}_{000}$ from the other POVM elements since $\pi^{\pm}_{000}$ only have $s = 3/2$ components, whereas $\pi^{\pm}_{001}, \pi^{\pm}_{010}, \pi^{\pm}_{011}$ only have $s = 1/2$ components. Making this explicit, notice, after going through the three-qubit QSWT circuit, the form of $\pi^{\pm}_{000}$:

$$\pi^{\pm}_{000} = \mathbb{I}_{\frac{3}{2}} = \left|\frac{3}{2},\frac{3}{2}\right\rangle\left\langle\frac{3}{2},\frac{3}{2}\right| + \left|\frac{3}{2},\frac{1}{2}\right\rangle\left\langle\frac{3}{2},\frac{1}{2}\right| + \left|\frac{3}{2},-\frac{1}{2}\right\rangle\left\langle\frac{3}{2},-\frac{1}{2}\right| + \left|\frac{3}{2},-\frac{3}{2}\right\rangle\left\langle\frac{3}{2},-\frac{3}{2}\right| \\ \to \mathbb{I}^{(Q_0Q_1)} \otimes |0\rangle\langle 0|^{(Q_2)}, \tag{3.85}$$

where $\mathbb{I}^{(Q_0Q_1)}$ denotes the identity operator on the first two qubits. This tells us that the action of $\mathbb{I}_{3/2}$ on $Q_0Q_1Q_2$ is equivalent to the action of $|0\rangle\langle 0|$ on Q_2 whilst leaving Q_0Q_1 invariant. Further, since $\pi^{\pm}_{000}$ is the same regardless of the outcome of the first measurement (unlike the other three-qubit POVM elements)

we can distinguish a measurement outcome of 000 from the others without having to condition it on the outcome of the first measurement. So, at this stage, if we were to measure Q_2 in the $\{|0\rangle, |1\rangle\}$ basis and obtain an outcome of 0, this would correspond to a three-qubit measurement outcome of 000, and, as we mentioned before, we can therefore stop, or ignore any outcomes that follow. However, as we saw earlier, if the outcome is 1, we can only conclude that the measurement outcome is *not* 000. So, more work is required to find out whether we've measured the system to be (initially prepared) in the state ρ_{001}, ρ_{010} or ρ_{011}. In the remainder of the protocol, we will be working in the $s = 1/2$ subspace, meaning that Q_2 has no use in the steps to come, so we are free to measure it. We map this measurement outcome to the classical bit c_1 such that $c_1 = 0$ corresponds to an outcome of $\mathcal{O}_2^{(1)} = 000$ and $c_1 = 1$ to an outcome of $\mathcal{O}_2^{(1)} \neq 000$.

Let's now move on to the measurements $\{\pi^{\pm}_{000}, \pi^{\pm}_{010}, \pi^{\pm}_{011}\}$. Ideally, we'd want one of these to be performed *only* if $\mathcal{O}_2^{(1)} \neq 000$, however, we can reduce the number of qubits and multi-qubit gates by always carrying out one of these measurements, whilst only taking note of the results when $c_1 = 1$ (i.e. when $\mathcal{O}_2^{(1)} \neq 000$). We do, however, have to take into account the result of the first measurement $\{\pi_{\pm}\}$, which we do by controlling $\{\pi^{\pm}_{000}, \pi^{\pm}_{010}, \pi^{\pm}_{011}\}$ on the qubit A, as shown in Fig. 3.4. Note that in this figure, $\{\pi^{+}_{001}, \pi^{+}_{010}, \pi^{+}_{011}\}$ only occurs when $|a\rangle = |0\rangle$ and $\{\pi^{-}_{001}, \pi^{-}_{010}, \pi^{-}_{011}\}$ when A is in the state $|1\rangle$ as we'd hope. Our task is further simplified when we notice that $\pi^{\pm}_{001}, \pi^{\pm}_{010}, \pi^{\pm}_{011}$ live entirely in $\mathcal{L}\big(\mathcal{Q}^{(3)}_{1/2} \otimes \mathcal{P}^{(3)}_{1/2}\big)$ and differ only in their path degree of freedom. Therefore, according to Eq. (3.84), we only require the Q_0 component $\rho^{\pm}_{ijk}$ for this part of the measurement. From here on, we will only consider, in full detail, the case in which $\mathcal{O}_1 = -$. The $\mathcal{O}_1 = +$ case can be found by performing the swaps in Eq. (3.35).

As mentioned, we only need to focus on the path component, encoded in Q_0, so our aim is to perform the POVM made up of the elements

$$\tilde{\pi}^{-}_{001} = \frac{2\beta - \alpha}{3\beta} |1\rangle\langle 1|^{(Q_0)}, \tag{3.86a}$$

$$\tilde{\pi}^{-}_{010} = \frac{1}{2}\left(\sqrt{\frac{\alpha+\beta}{3\beta}}|1\rangle - |0\rangle\right)\left(\sqrt{\frac{\alpha+\beta}{3\beta}}\langle 1| - \langle 0|\right), \tag{3.86b}$$

$$\tilde{\pi}^{-}_{010} = \frac{1}{2}\left(\sqrt{\frac{\alpha+\beta}{3\beta}}|1\rangle + |0\rangle\right)\left(\sqrt{\frac{\alpha+\beta}{3\beta}}\langle 1| + \langle 0|\right). \tag{3.86c}$$

Step 2: 001 **vs.** $\overline{001}$

Following the notation of the previous subsections, we first distinguish between $\mathcal{O}_2^{(2)} = 001$ and $\mathcal{O}_2^{(2)} = \overline{001}$ (which means $\mathcal{O}_2 \neq 001$), using the measurement operators

$$N_{001} = M_{001} = \sqrt{\frac{2\beta - \alpha}{3\beta}}|1\rangle\langle 1|, \tag{3.87a}$$

$$N_{\overline{001}} = \sqrt{\mathbb{1} - \big|N_{001}\big|^2} = \sqrt{\frac{\alpha+\beta}{3\beta}}|1\rangle\langle 1| + |0\rangle 0|, \tag{3.87b}$$

similarly to as we saw in Sec. 3.4.1 albeit with N_i, M_i belonging to different spaces. This can be done using the circuit in Fig. 3.3 with $X = B, S = Q_0$, and $U(\phi_2^-, \epsilon_2^-)$ such that

$$\phi_2^- = -\frac{1}{2}\left[\frac{\pi}{2} - \sin^{-1}\left(\frac{2\alpha - \beta}{3\beta}\right)\right], \tag{3.88a}$$

$$\epsilon_2^- = -\frac{1}{2}\left[\frac{\pi}{2} + \sin^{-1}\left(\frac{2\alpha - \beta}{3\beta}\right)\right], \tag{3.88b}$$

where the superscripts indicate that this corresponds to the case $\mathcal{O}_1 = -$. To access the measurement result, we can measure the qubit B and map the result onto c_2, with $c_2 = 0$ corresponding to $\mathcal{O}_2^{(2)} = 001$, and $c_2 = 1$ corresponding to $\mathcal{O}_2^{(2)} \neq 001$.

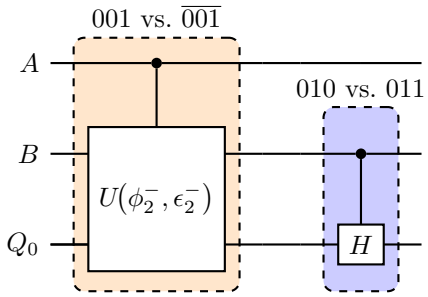

Figure 3.9: Circuit representation of the two step process used to perform the POVM $\{\pi_{001}^-, \pi_{010}^-, \pi_{011}^-\}$. Note the control on the qubit A which is required to ensure that this POVM is carried out *only* if the first measurement resulted in $\mathcal{O}_1 = -$.

Taking stock so far, if $c_1 = 0$, and therefore $\mathcal{O}_2^{(1)} = 000$, we ignore c_2, for we already obtained a valid measurement result in Step 1. If, however $c_1 = 1$, meaning $\mathcal{O}_2^{(1)} \neq 000$, we must take into account the measured value of B: $c_2 = 0$ for $\mathcal{O}_2^{(2)} = 001$, and $c_2 = 1$ for $\mathcal{O}_2^{(2)} \neq 001$. Just as we did in Step 1, if $c_2 = 0$, we can ignore everything that follows, but if $c_2 = 1$, we require Step 3 to finish our measurement. Once again, this is taken into account by controlling the measurement in Step 3 on B.

Step 3: 010 **vs.** 011

In this step, our task is to perform a measurement $\{N_{010}, N_{011}\}$ on it, with the final two possible outcomes: $\mathcal{O}_2^{(3)} = 010$ and $\mathcal{O}_2^{(3)} = 011$. As we noted in Sec. 3.4.1, and since we're performing this measurement purely on the path degree of freedom (contained in Q_0), the POVM corresponding to $\{N_{010}, N_{011}\}$ is just the Pauli-x measurement on Q_0. Therefore, we can take

$$N_{010} = |-\rangle\langle -|, \tag{3.89a}$$
$$N_{011} = |+\rangle\langle +|. \tag{3.89b}$$

So, in order to perform $\{N_{010}, N_{011}\}$ we just need to apply a Hadamard gate, controlled[13] on B, to Q_0 and then measure Q_0 in the computational basis. Steps 2 and 3 are shown in Fig. 3.9. When we come to measure Q_0 to determine $\mathcal{O}_2^{(3)}$, we map the measurement result onto c_3, taking[14] $c_3 = 1$ to mean $\mathcal{O}_2^{(3)} = 010$ and $c_3 = 0$ to mean $\mathcal{O}_2^{(3)} = 011$. This is because $HN_{010}H^\dagger = |1\rangle\langle 1|$ and $HN_{011}H^\dagger = |0\rangle\langle 0|$.

This concludes the circuit describing the sequential classification for Region I. Table 3.1 summarises how to interpret the values of the classical bits used, and what they correspond to in terms of the first and second measurement results. Note that we call the final outcome of the second measurement $\mathcal{O}_2$.

3.4.4.2 Region II

Let us now move onto the variable region of Fig. 3.1 - that is, when $\alpha \in (2\beta, 1-\beta]$ with $\beta \in [0, 1]$. We should first notice that nothing changes for $\{\pi_{ijk}^+\}$, so, when $\mathcal{O}_1 = +$, and therefore the A component of the state is $|0\rangle$, the circuit runs as described in the previous section. But when $\mathcal{O}_1 = -$ and A is in the state $|1\rangle$, $\{\pi_{ijk}^-\}$

[13] Controlled on B since we only perform this part of the measurement when $\mathcal{O}_2^{(2)} \neq 001$.
[14] Of course, that is unless $c_2 = 0$ and/or $c_1 = 0$, in which case we ignore the result stored in c_3.

c_0 (+ vs. −)	$\mathcal{O}_1$	c_1 (000 vs. $\overline{000}$)	c_2 (001 vs. $\overline{001}$)	c_3 (011 vs. 010)	$\mathcal{O}_2$
0	+	0	0	0	000
				1	
			1	0	
				1	
		1	0	0	001
				1	
			1	0	011
				1	010
1	−	0	0	0	000
				1	
			1	0	
				1	
		1	0	0	001
				1	
			1	0	011
				1	010

Table 3.1: Table summarising the classical bits, what measurement they describe, and what measurement outcomes $\mathcal{O}_1, \mathcal{O}_2$ their values correspond to. Where multiple adjacent entries in the same column share the same value, for readability, we only include one representative - for instance, the far left column represents eight 0s in the top box, and eight 1s in the bottom one.

has the form:

$$\pi^-_{000} = \mathbb{I}_{\frac{3}{2}}, \tag{3.90a}$$

$$\pi^-_{001} = 0, \tag{3.90b}$$

$$\pi^-_{010} = \frac{1}{2}\mathbb{I}_{\frac{1}{2}} \otimes (|1\rangle - |0\rangle)(\langle 1| - \langle 0|), \tag{3.90c}$$

$$\pi^-_{011} = \frac{1}{2}\mathbb{I}_{\frac{1}{2}} \otimes (|1\rangle + |0\rangle)(\langle 1| + \langle 0|). \tag{3.90d}$$

This follows from Eq. (3.41) and Eq. (3.43).

We can see that, as before, π^-_{000} can be distinguished from the others by measuring Q_2. However, distinguishing $\pi^-_{001}, \pi^-_{010}, \pi^-_{011}$ is much simpler here than before. Since $\pi^-_{001} = 0$, the operators we are discriminating between are π^-_{010}, π^-_{011}. As we saw in Region I, this corresponds to a Pauli-x measurement on the path qubit Q_0, the result of which is stored in c_3[15]. It follows that when $c_3 = 1$ ($c_3 = 0$), we take this to correspond to a measurement outcome of 010 (011).

3.4.4.3 Simulated results

These two circuits where simulated in Qiskit. The results, were plotted in Fig. 3.10 along with the analytical tradeoff [Eq. (3.51), Fig. 3.1].

In order to simulate these results, the states ρ_{ijk} had to somehow be input into the circuit. Since Qiskit operates under the paradigm of inputting pure states into quantum circuits, and since

$$\rho_{ijk} = \int |\varphi_i\varphi_j\varphi_k\rangle\langle\varphi_i\varphi_j\varphi_k| \, d\varphi_0 d\varphi_1, \tag{3.91}$$

our first worrying thought might be that we require a large number pure states to approximate ρ_{ijk}. Thankfully, however, there is a set of just six pure states, due to how they are distributed on the Bloch sphere,

[15]Note that this time, one less classical bit is required since a measurement outcome corresponding to π^-_{001} is never registered. So that we don't have to rename the classical bits corresponding to $\{\pi^+_{ijk}\}$ outcomes, we just ignore c_2 as it will be left unchanged with a value of 0.

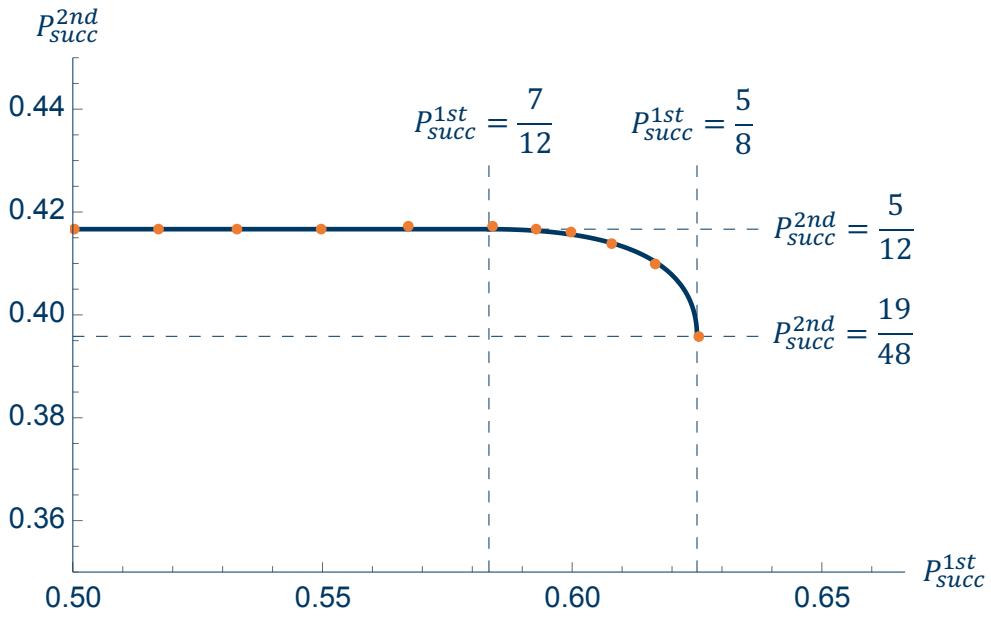

Figure 3.10: Plot of the simulated results of the quantum circuit describing the two-measurement protocol discussed in Sec. 3.3. The blue curve shows the analytical tradeoff given by Eq. (3.51) and the orange points show how the simulated success rates of the two measurements (as a quantum circuit) relate to one another for varying α, β. These simulations were carried out using the AerSimulator in Qiskit.

that can construct each ρ_{ijk} exactly:

$$T = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle, |-i\rangle\}, \tag{3.92}$$

that is, the eigenstates of the Pauli operators $\sigma_x, \sigma_y, \sigma_z$. This is true because T is what's known as a quantum 1-design, 2-design and 3-design [114]. That is,

$$\rho_0 = \int |\varphi_0\rangle\langle\varphi_0| \, d\varphi_0 = \frac{1}{6} \sum_{|v_i\rangle \in T} |v_i\rangle\langle v_i|, \tag{3.93a}$$

$$\rho_{00} = \int |\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0| \, d\varphi_0 = \frac{1}{6} \sum_{|v_i\rangle \in T} |v_i v_i\rangle\langle v_i v_i|, \tag{3.93b}$$

$$\rho_{000} = \int |\varphi_0\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0\varphi_0| \, d\varphi_0 = \frac{1}{6} \sum_{|v_i\rangle \in T} |v_i v_i v_i\rangle\langle v_i v_i v_i| \tag{3.93c}$$

respectively. Using these relations, the fact that $\rho_{0\cdots0} = \rho_{1\cdots1}$, and that $\rho_{001}, \rho_{010}, \rho_{011}$ are related by a permutation symmetry, every ρ_{ijk} can be constructed using only the pure states in T.

So, in order to simulate our tradeoff, we allowed $|\varphi_0\rangle, |\varphi_1\rangle$ to be the states in T, and for each choice, we input $|\varphi_0\varphi_0\varphi_0\rangle, |\varphi_0\varphi_0\varphi_1\rangle, |\varphi_0\varphi_1\varphi_0\rangle, |\varphi_0\varphi_1\varphi_1\rangle$ into the circuit 8192 times to approximate the measurement statistics of each of these states. Once this had been done for every element of T, we averaged over the results. We did this using the AerSimulator in Qiskit for different choices of α, β, corresponding to different success probabilities of the first and second measurements. These different α, β correspond to the different orange points in Fig. 3.10.

3.5 Discussion

To summarise, we considered a base case in the tradeoff between two sequential unsupervised quantum learning tasks. In particular, we looked at the situation in which there was initially a dataset of three

qubits that could each be in one of two unknown quantum states. Once a binary classification of varying success rate, corresponding to a quantum measurement of varying strength, had been performed on a subset of two of these qubits, the optimal classification on all three qubits was then performed. We found that, although a binary classification of two unknown qubits causes measurement disturbance which can degrade the performance of an optimal classifier on all three qubits, there is a large regime in which the performance remains unaffected. In this regime, the final measurement may be adjusted to fully mitigate the disturbance caused by the first measurement. That is, the success rate of the first classification can range from that of a guess, $P_{\text{succ}}^{\text{1st}} = 1/2$ to $P_{\text{succ}}^{\text{1st}} = 7/12$ without causing the success rate of the second classification to deviate from its optimal value of $P_{\text{succ}}^{\text{2nd}} = 5/12$. When $P_{\text{succ}}^{\text{1st}}$ is further improved, however, $P_{\text{succ}}^{\text{2nd}}$ decreases non-linearly to a success rate of 19/48 as $P_{\text{succ}}^{\text{1st}}$ increases to its optimal value of 5/8. We also demonstrated this tradeoff through a circuit implementation in Qiskit, executed using the AerSimulator.

The contents of this chapter provides an indication that sequential unsupervised classifications of quantum data can be performed. Further, depending on the strength of an earlier classification, a later classification's ability need not be compromised. Having said this, this work also highlights that there are non-trivial tradeoffs between sequential unsupervised quantum learning tasks which, although small in this base case, may be more considerable in more complicated scenarios. Here we have considered the simplest possible example of a quantum learning task in which a measurement disturbance tradeoff exists between performance on a subset of the data provided and performance on the whole dataset. We have fully characterized this tradeoff. This is a peculiarly quantum effect due to fundamental features of quantum mechanics, which is not present in classical machine learning.

This is just the first step in exploring this tradeoff in learning tasks, and more work is required to fully understand the limitations imposed by quantum mechanics on sequential learning. For example the next natural step would be to consider starting with n unknown qubits of two types and, following a classification of them, adding 1 or more extra qubits to be subsequently classified - we take steps in this direction in the following chapter. Further, one could look at the case in which there are a larger number of options of qubit (or d-dimensional qudit) to choose between. Another path to take could be the supervised analogue of the content of this chapter, with labelled qubits being given as a training set used to classify future ones. In addition, there are a range of learning paradigms, including partially or fully supervised learning, and reinforcement learning, in which similar effects may be explored.

Appendix 3.A Derivation of updated states and measurements

3.A.1 Updated prior probabilities

Assuming the outcome of the measurement on the first two qubits is $-$, the probabilities of the disturbed states $\rho_{000}^{-}, \rho_{001}^{-}, \rho_{010}^{-}, \rho_{011}^{-}$ occurring are given by $p_{000}^{-}, p_{001}^{-}, p_{010}^{-}, p_{011}^{-}$ respectively, such that

$$p_{0ij}^{-} := P(\rho_{0ij}|\pi_- \otimes \mathbb{1}). \tag{3.94}$$

Using Bayes' theorem, this can be written as

$$\begin{aligned} p_{0ij}^{-} &= \frac{P(\pi_- \otimes \mathbb{1}|\rho_{0ij})P(\rho_{0ij})}{P(\pi_- \otimes \mathbb{1})} \\ &= \frac{P(\pi_-|\rho_{0i})}{4P(\pi_-)}, \end{aligned} \tag{3.95}$$

where the second equality is obtained using the fact that $P(\rho_{0ij}) = 1/4$, and that the third qubit is acted on only by the identity and therefore does not change any of the probabilities.

So, by noting that

$$P(\pi_-|\rho_{00}) = \text{Tr}(\pi_-\rho_{00}) = \beta, \tag{3.96a}$$

$$P(\pi_-|\rho_{01}) = \text{Tr}(\pi_-\rho_{01}) = \frac{1}{4}(\alpha + 4\beta), \tag{3.96b}$$

and therefore,

$$\begin{aligned} P(\pi_-) &= P(\pi_-|\rho_{00})P(\rho_{00}) + P(\pi_-|\rho_{01})P(\rho_{01}) \\ &= \frac{1}{8}(\alpha + 8\beta), \end{aligned} \tag{3.97}$$

we find that

$$p^-_{000} = p^-_{001} = \frac{2\beta}{\alpha + 8\beta}, \tag{3.98a}$$

$$p^-_{010} = p^-_{011} = \frac{\alpha + 4\beta}{2(\alpha + 8\beta)}. \tag{3.98b}$$

3.A.2 Second measurement

Again, assuming the outcome of the first classification was $-$, recall that distinguishing ρ^-_{000} from the other states is done optimally by letting π^-_{000} be the projector onto the $s = 3/2$ space. This leads to the measurement that best distinguishes $\rho^-_{001}, \rho^-_{010}, \rho^-_{011}$ being entirely contained in the $s = 1/2$ space $\mathcal{L}(\mathcal{Q}^{(3)}_{\frac{1}{2}} \otimes \mathcal{P}^{(3)}_{\frac{1}{2}})$. Further, since the $\mathcal{L}(\mathcal{Q}^{(3)}_{\frac{1}{2}})$ component of each of $\rho^-_{001}, \rho^-_{010}, \rho^-_{011}$ is the identity, all the information about how they differ is contained in $\mathcal{L}(\mathcal{P}^{(3)}_{\frac{1}{2}})$. So we can rephrase this as a state discrimination problem of the following states:

$$|\psi^-_{001}\rangle = \frac{\mathcal{N}^-_{001}}{\sqrt{6}}|1\rangle, \tag{3.99a}$$

$$|\psi^-_{010}\rangle = \frac{\mathcal{N}^-_{010}}{\sqrt{6(\alpha + 4\beta)}}\left(\sqrt{\beta}|1\rangle - \sqrt{3(\alpha + \beta)}|0\rangle\right), \tag{3.99b}$$

$$|\psi^-_{011}\rangle = \frac{\mathcal{N}^-_{011}}{\sqrt{6(\alpha + 4\beta)}}\left(\sqrt{\beta}|1\rangle + \sqrt{3(\alpha + \beta)}|0\rangle\right), \tag{3.99c}$$

where $\mathcal{N}^-_{0ij}$ are normalisation constants required so that we can think of this as a mirror symmetric state discrimination problem. Explicitly,

$$\mathcal{N}^-_{001} = \sqrt{6}, \tag{3.100a}$$

$$\mathcal{N}^-_{010} = \sqrt{\frac{6(\alpha + 4\beta)}{4\beta + 3\alpha}} = \mathcal{N}^-_{011}. \tag{3.100b}$$

Now, in [63], the states to be discriminated are written as

$$|\psi_1\rangle = |1\rangle, \tag{3.101a}$$

$$|\psi_2\rangle = \cos\theta|1\rangle - \sin\theta|0\rangle, \tag{3.101b}$$

$$|\psi_3\rangle = \cos\theta|1\rangle + \sin\theta|0\rangle, \tag{3.101c}$$

such that $|\psi_{2,3}\rangle$ happen with probability $p_{2,3} = p$ and $|\psi_1\rangle$ with probability $p_1 = 1 - 2p$. So, we can let

$$\cos\theta = \sqrt{\frac{\beta}{4\beta + 3\alpha}}, \tag{3.102a}$$

$$\sin\theta = \sqrt{\frac{3(\alpha + \beta)}{4\beta + 3\alpha}}, \tag{3.102b}$$

and $q^-_{010}, q^-_{011} = p^-$, $q^-_{001} = 1 - 2p^-$ where

$$q^-_{0ij} = P(\rho_{0ij}|\pi_-, s = 1/2) \tag{3.103}$$

is the probability of being in the state $|\psi^-_{0ij}\rangle$, and we have added (with respect to [63]) a superscript to p to distinguish the two outcomes of the intermediate measurement.

So, using Eq. (3.103), we can find $p^- = q^-_{01j}$. Using Bayes' theorem, we find that

$$p^- = \frac{P\Big(\pi_- \otimes \mathbb{1}, s = \frac{1}{2}\Big|\rho_{01j}\Big)P(\rho_{01j})}{P\big(\pi_- \otimes \mathbb{1}, s = \frac{1}{2}\big)}. \tag{3.104}$$

Note that requiring $s = 1/2$ is equivalent to projecting the state ρ_{01j} onto the $s = 1/2$ space $\mathcal{L}(\mathcal{Q}^{(3)}_{\frac{1}{2}} \otimes \mathcal{P}^{(3)}_{\frac{1}{2}})$. Denoting this projector by $P_{\frac{1}{2}}$,

$$P\left(\pi_- \otimes \mathbb{1}, s = \frac{1}{2}\middle|\rho_{01j}\right) = P\Big(\pi_- \otimes \mathbb{1}, P_{\frac{1}{2}}\Big|\rho_{01j}\Big) = \mathrm{Tr}\Big[P_{\frac{1}{2}}\big(\sqrt{\pi_-} \otimes \mathbb{1}\big)\rho_{01j}\big(\sqrt{\pi_-} \otimes \mathbb{1}\big)^\dagger P^\dagger_{\frac{1}{2}}\Big]. \tag{3.105}$$

The denominator can be found using

$$P\left(\pi_- \otimes \mathbb{1}, s = \frac{1}{2}\right) = \sum_{ij} P(\pi_- \otimes \mathbb{1}, P_{\frac{1}{2}}|\rho_{0ij})P(\rho_{0ij}), \tag{3.106}$$

from which it follows that

$$p^- = \frac{3\alpha + 4\beta}{6(\alpha + 2\beta)}. \tag{3.107}$$

Now, according to [63], if

$$p \geq \frac{1}{2 + \cos\theta(\cos\theta + \sin\theta)}, \tag{3.108}$$

$a = 1$. Else,

$$a = \frac{p\cos\theta\sin\theta}{1 - p(2 + \cos^2\theta)}. \tag{3.109}$$

Substituting p^- for p, a_- for a and our expressions for $\sin\theta, \cos\theta$ given in Eq. (3.102), this can be restated in the following way: if

$$\alpha \geq 2\beta, \tag{3.110}$$

$a_- = 1$. Else,

$$a_- = \sqrt{\frac{\alpha + \beta}{3\beta}}. \tag{3.111}$$

When coupled with the constraints on α, β given in Eq. (3.34), we obtain

$$a_- = \begin{cases} \sqrt{\frac{\alpha+\beta}{3\beta}} & \text{if } \alpha \in [0, \min\{1-\beta, 2\beta\}], \\ 1 & \text{if } \alpha \in (2\beta, 1-\beta] \text{ with } 2\beta < 1-\beta \end{cases} \tag{3.112}$$

such that $\beta \in [0, 1]$.

Chapter 4

Measurement disturbance tradeoffs in n-qubit unsupervised classification

In this chapter, we aim to generalise some of the findings of the previous chapter to n qubits. To do this, we first learn how to perform an unsupervised binary classification on n qubits. We do this by re-deriving some of the work by Sentís et al [71]. In doing so, we'll establish the notation used throughout this chapter. After this, given a set of n qubits, we will look into how an initial classification on a subset of $n-1$ qubits affects one's ability to classify the full dataset. In particular, we investigate how successful we can be in our initial classification without affecting the optimality of a subsequent one. We find that, in the initial classification, we can learn something about the numbers of each of the states, $|\varphi_0\rangle, |\varphi_1\rangle$, without affecting the second classification. Indeed, as we will see, there are hints that nothing about their order can be deduced, although it is possible that this is due to the symmetric form of the optimal measurement on n undisturbed qubits that we use. We find that a consequence of this is that no non-trivial measurement on the first $n-m$ qubits (for $m > 1$) can be performed without affecting the success rate of a subsequent classification of the whole n-qubit dataset. We derive an analytical expression for a lower bound on the success rate achievable in this initial classification. Following this, we hypothesise a construction algorithm of the measurement that realises the upper bound - at least under the constraint that the n-qubit measurement shares the symmetries of the dataset. Before we do all of this, let's first summarise the notation used throughout this chapter.

4.1 Notation

This section is included purely to summarise the notation used over the course of this chapter. Any explanation, if necessary, of such notation occurs when it is first encountered. When classifying n qubits, our states and representations are labelled using, partitions or total spin:

$$\nu_k = (n-k, k), \tag{4.1a}$$

$$s_{\nu_k} = \frac{n-2k}{2}. \tag{4.1b}$$

When considering $n-1$ qubits, we will use

$$\mu_j = (n-1-j, j), \tag{4.2a}$$

$$s_{\mu_j} = \frac{n-1-2j}{2}. \tag{4.2b}$$

Since partitions are defined using non-negative integers, it will be implicitly assumed throughout that the subscripts of the partitions are integers - e.g. in the above, $j, k \in \mathbb{Z}$. Although it will be made clear as we go, when labeling states, measurement operators and so on, we will reserve $\sigma, \sigma', \tilde{\sigma}$ etc. for elements of S_n, whereas $\tau, \tau', \tilde{\tau}$ etc. will be used as elements of S_{n-1}. Finally, measurement operators on n qubits will be written using π, for example $\pi_{\nu_k,\sigma}$. Conversely, measurement on $n-1$ qubits will be written using ξ, for example, $\xi_{\mu_j,\tau}$. We summarise the notation in Table 4.1.

	$n-1$ qubits	n qubits
Partition	μ_j	ν_k
Spin	s_{μ_j}	s_{ν_k}
Permutation cycle	τ	σ
Permutation equivalence class	$[\tau]_{\mu_j}$	$[\sigma]_{\nu_k}$
Set of equivalence classes	C_{μ_j}	C_{ν_k}
Set of states	$R^{(n-1)}$	$R^{(n)}$
POVM elements	$\xi_{\mu_j,\tau}$	$\pi_{\nu_k,\sigma}$
POVM	$\Xi^{(n-1)}$	$\Pi^{(n)}$
Hilbert space	$\mathcal{H}^{(n-1)}$	$\mathcal{H}_n$
Reducible $SU(2)$ representation	$\left(\mathbf{Q}^{(n-1)}, \mathcal{H}^{(n-1)}\right)$	$\left(\mathbf{Q}^{(n)}, \mathcal{H}^{(n)}\right)$
Irreducible $SU(2)$ representations	$(\mathbf{q}_{\mu_j}, \mathcal{Q}_{\mu_j})$	$(\mathbf{q}_{\nu_k}, \mathcal{Q}_{\nu_k})$
Reducible symmetric group representation	$\left(\mathbf{P}^{(n-1)}, \mathcal{H}^{(n-1)}\right)$	$\left(\mathbf{P}^{(n)}, \mathcal{H}^{(n)}\right)$
Irreducible symmetric group representations	$(\mathbf{p}_{\mu_j}, \mathcal{P}_{\mu_j})$	$(\mathbf{p}_{\nu_k}, \mathcal{P}_{\nu_k})$

Table 4.1: Summary of the notation used throughout this chapter.

4.2 Unsupervised binary classification of n qubits

In this section, we re-derive a special case[1] of the work by Sentís et al [71] and write down the optimal success rate in classifying n qubits that are each in one of two unknown states $|\varphi_0\rangle, |\varphi_1\rangle$. As in the previous section, this corresponds to a quantum state discrimination problem where the states to distinguish represent each possible quantum dataset. With that, our first task is to write down these states.

4.2.1 The states

As mentioned, suppose we have n qubits that are one of two unknown pure states $|\varphi_0\rangle$, $|\varphi_1\rangle$. Define the partition of n:

$$\nu_k = (n-k, k), \tag{4.3}$$

such that $k \in \mathbb{Z}$ subject to $0 \leq k \leq n/2$, or in other words, $k \in \{0, \ldots, \lfloor n/2 \rfloor\}$. By Schur-Weyl duality, each ν_k simultaneously labels an irrep of SU(2) and S_n: $(\mathbf{q}_{\nu_k}, \mathcal{Q}_{\nu_k})$ and $(\mathbf{p}_{\nu_k}, \mathcal{P}_{\nu_k})$ respectively[2]. It turns out that these partitions can also be used to label how many of each state $|\varphi_i\rangle$ we have, where k tells us how many $|\varphi_1\rangle$ states there are. We therefore define the following states

$$\rho_{\nu_k} := \rho_{0^{n-k}1^k}, \tag{4.4}$$

where b^i means i copies of b in a row, e.g. $\rho_{0^3 1^2} := \rho_{00011}$. It turns out that we can also label our irreps and states using the total spin by imagining our qubits as spin-half particles. We do this using [115]

$$\nu_k \mapsto s_{\nu_k} = \frac{n-2k}{2}. \tag{4.5}$$

The corresponding z-component of the spin follows the normal rules

$$m_{\nu_k} \in \{-s_{\nu_k}, -s_{\nu_k}+1, \ldots, s_{\nu_k}\}. \tag{4.6}$$

This alternate labelling comes in particularly useful when we consider the sequential learning task later in this chapter.

Let's write down these states more quantitatively. First, we reiterate that the pure states $|\varphi_i\rangle$ are completely unknown to us and can therefore be located at any point on the surface of the Bloch sphere with equal likelihood. Therefore, similarly to in the two and three-qubit cases considered previously, we write

$$\rho_{\nu_k} = \int \left(|\varphi_0\rangle^{\otimes n-k} |\varphi_1\rangle^{\otimes k}\right) \left(\langle\varphi_0|^{\otimes n-k} \langle\varphi_1|^{\otimes k}\right) d\varphi_0 d\varphi_1, \tag{4.7}$$

[1] A special case in that Sentís et al took $|\varphi_0\rangle, |\varphi_1\rangle$ to be d-dimensional *qudit* states, whereas we only consider them as *qubit* states.

[2] Recall that a representation of a group G is a homomorphism $\mathbf{R}$ together with a vector space $\mathcal{V}$ such that $\mathbf{R} : G \to \text{End}(\mathcal{V})$.

which, since $|\varphi_i\rangle$ are totally independent of one another, can be rewritten as[3],

$$\begin{aligned}\rho_{\nu_k} &= \left[\int \left(|\varphi_0\rangle\langle\varphi_0|\right)^{\otimes n-k} d\varphi_0\right] \otimes \left[\int \left(|\varphi_1\rangle\langle\varphi_1|\right)^{\otimes k} d\varphi_1\right] \\ &= \rho_{0^{n-k}} \otimes \rho_{1^k}. \end{aligned} \tag{4.8}$$

Next, notice that $\mathbf{P}^{(i)}(\sigma)|\varphi_b\rangle^{\otimes i} = |\varphi_b\rangle^{\otimes i}$ for all $\sigma \in S_n$, $|\varphi_b\rangle \in \mathcal{H}^{(1)}$, for example, permuting the qubits in the state $|\varphi_0\rangle|\varphi_0\rangle|\varphi_0\rangle$ does not change the state of the system. This means that $|\varphi_b\rangle^{\otimes i} \in \mathcal{Q}_{(i)} \otimes \mathcal{P}_{(i)}$ and therefore $\rho_{b^i} \in \mathcal{L}(\mathcal{Q}_{(i)} \otimes \mathcal{P}_{(i)})$, where $(i) := (i, 0)$ is the partition labelling the totally symmetric Schur-Weyl subspace of i qubits.

Now, for all $U \in SU(2)$,

$$\mathbf{Q}^{(i)}(U)\rho_{b^i}\mathbf{Q}^{(i)\,\dagger}(U) = \rho_{b^i}. \tag{4.9}$$

To see this, as was done before, we can rewrite ρ_{b^i}, perhaps more rigorously, as

$$\int_{SU(2)} V_b^{\otimes i}|0\rangle\langle 0|V_b^{\otimes i\,\dagger} d\mu(V_b), \tag{4.10}$$

where $|0\rangle$ is some fixed pure state, and μ is the Haar measure on SU(2). This is related to Eq. (4.7) by noting that $|\varphi_b\rangle = V_b|0\rangle$ for some $V_b \in \mathrm{SU}(2)$. The reason for performing this integral with respect to the Haar measure on SU(2) is that this ensures the states $\{|\varphi_b\rangle = V_b|0\rangle \mid V_b \in \mathrm{SU}(2)\}$ are uniformly distributed on the surface of the Bloch sphere, which is what we're assuming. As we saw in Sec. 2.3.4, a property of the Haar measure is that, for any integrable function f, $\int_{\mathrm{SU}(2)} f(UV)d\mu(V) = \int_{\mathrm{SU}(2)} f(V)d\mu(V)$ for any $U \in \mathrm{SU}(2)$ [76]. It follows that

$$\begin{aligned}\mathbf{Q}^{(i)}(U)\rho_{b^i}\mathbf{Q}^{(i)\,\dagger}(U) &= U^{\otimes i}\left(\int_{SU(2)} V_b^{\otimes i}|0\rangle\langle 0|V_b^{\otimes i\,\dagger} d\mu(V_b)\right)U^{\otimes i\,\dagger} \\ &= \int_{SU(2)} (UV_b)^{\otimes i}|0\rangle\langle 0|(UV_b)^{\otimes i\,\dagger} d\mu(V_b) \\ &= \int_{SU(2)} V_b^{\otimes i}|0\rangle\langle 0|V_b^{\otimes i\,\dagger} d\mu(V_b) = \rho_{b^i}. \end{aligned} \tag{4.11}$$

Using Schur's Lemma, this, together with the fact that $\rho_{b^i} \in \mathcal{L}(\mathcal{Q}_{(i)} \otimes \mathcal{P}_{(i)})$, means that

$$\rho_{\nu_k} = \frac{1}{d_{(n-k)}d_{(k)}}\mathbb{I}_{(n-k)} \otimes \mathbb{I}_{(k)}, \tag{4.12}$$

where $d_{(i)} := \dim\big[\mathcal{Q}_{(i,0)} \otimes \mathcal{P}_{(i,0)}\big]$ ensures ρ_{ν_k} is normalised, and $\mathbb{I}_{(i)}$ is the identity operator on $\mathcal{Q}_{(i)} \otimes \mathcal{P}_{(i)}$. Notice that only the dimension of the SU(2) subspace contributes, that is, $d_{(i)} := \dim\big[\mathcal{Q}_{(i,0)}\big]$ since $\dim\big[\mathcal{P}_{(i,0)}\big] = 1$.

We can go further by recalling our alternate labelling [Eq. (4.5)], and noting that the dimension of a spin s subspace is $2s + 1$, which means that $d_{(i)} = i + 1$, and thus,

$$\rho_{\nu_k} = \frac{1}{(n-k+1)(k+1)}\mathbb{I}_{(n-k)} \otimes \mathbb{I}_{(k)}. \tag{4.13}$$

By recalling how the Hilbert space of a composite system of two particles with spins s_1, s_2 decomposes:

$$\mathcal{Q}_{s_1} \otimes \mathcal{Q}_{s_2} \cong \mathcal{Q}_{s_1+s_2} \oplus \mathcal{Q}_{s_1+s_2-1} \oplus \cdots \oplus \mathcal{Q}_{|s_1-s_2|}, \tag{4.14}$$

we can see that, using Eq. (4.5),

$$\begin{aligned}\mathcal{Q}_{(n-k)} \otimes \mathcal{Q}_{(k)} &\cong \mathcal{Q}_{(n,0)} \oplus \mathcal{Q}_{(n-1,1)} \oplus \cdots \oplus \mathcal{Q}_{(n-k,k)} \\ &= \bigoplus_{i=0}^{k} \mathcal{Q}_{\nu_i}. \end{aligned} \tag{4.15}$$

[3]With the slight abuse of notation that is changing the order of the vector spaces to pair up each vector space with its corresponding dual space.

Therefore, by noting again that $\dim[\mathcal{P}_{(i)}] = 1$, we can rewrite ρ_{ν_k} in the Schur basis as follows,

$$\rho_{\nu_k} = \frac{1}{(n-k+1)(k+1)} \bigoplus_{i=0}^{k} \mathbb{I}_{\mathcal{Q}_{\nu_i}} \otimes \Omega_{\nu_i}, \tag{4.16}$$

where, $\Omega_{\nu_i} \in \mathcal{L}(\mathcal{P}_{\nu_i})$ are pure states that we don't need to know explicitly, and $\mathbb{I}_{\mathcal{Q}_{\nu_i}}$ denotes the identity on the SU(2) invariant subspace $\mathcal{Q}_{\nu_i}$.

Next, in order to find all the possible states, all we need to do is permute the 0s and 1s in ρ_{ν_k}. To do this, we use elements from $\mathbf{P}(S_n)$, where we're taking $\mathbf{P}(S_n) := \mathbf{P}^{(n)}(S_n)$ in this section. Notice, however, that some repetition occurs. For example, in the $n = 3$ case,

$$\rho_{010} = \mathbf{P}[(23)]\rho_{001}\mathbf{P}^\dagger[(23)] = \mathbf{P}[(132)]\rho_{001}\mathbf{P}^\dagger[(132)]. \tag{4.17}$$

To remedy this, we define the following equivalence relation.

Definition 4.2.1. *For $\sigma, \sigma' \in S_n$,*

$$\sigma \sim_{\nu_k} \sigma' \iff \mathbf{P}(\sigma)\rho_{\nu_k}\mathbf{P}^\dagger(\sigma) = \mathbf{P}(\sigma')\rho_{\nu_k}\mathbf{P}^\dagger(\sigma'). \tag{4.18}$$

It can be shown that this is indeed an equivalence relation and therefore partitions S_n into equivalence classes $[\sigma]_{\nu_i}$. So, if we define

$$C_{\nu_k} = \{[\sigma]_{\nu_k} \ : \ \sigma \in S_n\} \tag{4.19}$$

to be the set of equivalence classes with respect to $\sim_{\nu_k}$, we can write down our states

$$\rho_{\nu_k,\sigma} := \mathbf{P}(\sigma)\rho_{\nu_k}\mathbf{P}^\dagger(\sigma), \tag{4.20}$$

such that σ is a representative of the equivalence class $[\sigma]_{\nu_k} \in C_{\nu_k}$. More explicitly,

$$\rho_{\nu_k,\sigma} = \frac{1}{(n-k+1)(k+1)} \bigoplus_{i=0}^{k} \mathbb{I}_{\mathcal{Q}_{\nu_i}} \otimes \Omega_{\nu_i,\sigma}, \tag{4.21}$$

where $\Omega_{\nu_i,\sigma} := \mathbf{p}_{\nu_i}(\sigma)\Omega_{\nu_i}\mathbf{p}^\dagger_{\nu_i}(\sigma)$. So the set of all possible n-qubit states is

$$R^{(n)} = \bigcup_{k=0}^{\lfloor n/2 \rfloor} \{\rho_{\nu_k,\sigma} \ : \ [\sigma]_{\nu_k} \in C_{\nu_k}\}, \tag{4.22}$$

where the condition $[\sigma]_{\nu_k} \in C_{\nu_k}$ is taken to mean that there is one state $\rho_{\nu_k,\sigma}$ for each equivalence class $[\sigma]_{\nu_k} \in C_{\nu_k}$.

4.2.2 The measurement

An optimal measurement to distinguish the states in $R^{(n)}$ is given by

$$\Pi^{(n)} = \bigcup_{k=0}^{\lfloor n/2 \rfloor} \left\{ \pi_{\nu_k,\sigma} = \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|} \mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \Omega_{\nu_k,\sigma} \ : \ [\sigma]_{\nu_k} \in C_{\nu_k} \right\}, \tag{4.23}$$

where $d_{\mathcal{P}_{\nu_i}} := \dim[\mathcal{P}_{\nu_k}]$, and $|C_{\nu_k}|$ denotes the cardinality of C_{ν_k} and therefore the number of states with $n-k$ zeros and k ones. We originally hypothesised the form of this POVM via symmetry considerations, in that it shares the symmetries of the possible states in $R^{(n)}$. We go on now to show that it is indeed an optimal POVM.

Let's first confirm that it is a valid POVM. That is, that it satisfies the conditions in Eq. (2.82). Since $\Omega_{\nu_k,\sigma}$ is a pure state, and $d_{\mathcal{P}_{\nu_k}}, |C_{\nu_k}| > 0$, it is clear that $\pi_{\nu_k,\sigma} \geq 0 \ \forall k \leq n/2$ and $[\sigma]_{\nu_k} \in C_{\nu_k}$. For the

completeness condition, first note that

$$\begin{aligned}
&\sum_{k=0}^{\lfloor n/2 \rfloor} \sum_{[\sigma]_{\nu_k} \in C_{\nu_k}} \pi_{\nu_k,\sigma} = \mathbb{I} \\
\iff &\sum_{[\sigma]_{\nu_k} \in C_{\nu_k}} \pi_{\nu_k,\sigma} = \mathbb{I}_{\nu_k}, \ \forall k \leq n/2 \\
\iff &\sum_{[\sigma]_{\nu_k} \in C_{\nu_k}} \pi_{\nu_k,\sigma} \propto \mathbb{I}_{\nu_k} \text{ and } \operatorname{Tr}\left[\sum_{[\sigma]_{\nu_k} \in C_{\nu_k}} \pi_{\nu_k,\sigma}\right] = d_{\nu_k}, \ \forall k \leq n/2. \qquad (4.24)
\end{aligned}$$

Let $k \leq n/2$ be arbitrary. We can see that, since $\pi_{\nu_k,\sigma} \in \mathcal{L}(\mathcal{Q}_{\nu_k} \otimes \mathcal{P}_{\nu_k})$ and $\mathbf{p}_{\nu_k}(\sigma')\big(\sum_{[\sigma]_{\nu_k}} \pi_{\nu_k,\sigma}\big)\mathbf{p}^\dagger_{\nu_k}(\sigma') = \sum_{[\sigma]_{\nu_k}} \pi_{\nu_k,\sigma}$, by Schur's lemma, it follows that $\sum_{[\sigma]_{\nu_k}} \pi_{\nu_k,\sigma} \propto \mathbb{I}_{\nu_k}$. Also, since $\pi_{\nu_k,\sigma} = \mathbf{p}_{\nu_k}(\sigma)\pi_{\nu_k}\mathbf{p}^\dagger_{\nu_k}(\sigma)$, by the cyclic nature of the trace along with the unitarity of $\mathbf{p}_{\nu_k}(\sigma)$, it follows that $\operatorname{Tr}\big(\sum_{[\sigma]_{\nu_k}} \pi_{\nu_k,\sigma}\big) = \sum_{[\sigma]_{\nu_k}} \operatorname{Tr}(\pi_{\nu_k}) = |C_{\nu_k}| \operatorname{Tr}\left[(d_{\mathcal{P}_{\nu_k}}/|C_{\nu_k}|)\mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \Omega_{\nu_k}\right] = d_{\mathcal{Q}_{\nu_k}} d_{\mathcal{P}_{\nu_k}} = d_{\nu_k}$. So completeness is satisfied and $\Pi^{(n)}$ is therefore a POVM.

To prove the optimality of this POVM with respect to the minimum error figure of merit, we show that $\Pi^{(n)}$ satisfies the necessary condition in Eq. (2.97):

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \sum_{[\sigma]_{\nu_k} \in C_{\nu_k}} p_{\nu_k,\sigma}\rho_{\nu_k,\sigma}\pi_{\nu_k,\sigma} - p_{\nu_j,\sigma'}\rho_{\nu_j,\sigma'} \geq 0, \ \forall j, \sigma'. \qquad (4.25)$$

Since $p_{\nu_k,\sigma} = 2^{1-n}$ is fixed for all k, σ, and using our explicit states and POVM elements in Eq. (4.16), Eq. (4.23) respectively, after some algebra, one can see that we have to show

$$\begin{aligned}
\tilde{\Gamma} := \bigoplus_{k=0}^{j} \mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \left[\frac{1}{(n-k+1)(k+1)}\mathbb{I}_{\mathcal{P}_{\nu_k}} - \frac{1}{(n-j+1)(j+1)}\Omega_{\nu_k,\sigma'}\right] \\
+ \bigoplus_{k=j+1}^{\lfloor n/2 \rfloor} \frac{1}{(n-k+1)(k+1)}\mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \mathbb{I}_{\mathcal{P}_{\nu_k}} \geq 0. \qquad (4.26)
\end{aligned}$$

To see that this is indeed the case, notice that

$$\frac{1}{(n-k+1)(k+1)} \geq 0, \ \forall k, \qquad (4.27a)$$

$$\frac{1}{(n-k+1)(k+1)} - \frac{1}{(n-j+1)(j+1)} \geq 0, \ \forall k \leq j. \qquad (4.27b)$$

From this, it follows that, for any vector $|\chi\rangle \in \mathcal{H}^{(n)}$, $\langle\chi|\tilde{\Gamma}|\chi\rangle \geq 0$, as required. We have thus shown that $\Pi^{(n)}$ is a measurement that optimally distinguishes between the states in $R^{(n)}$.

The POVM $\Pi^{(n)}$ can be thought of as a measurement with two steps. To understand this, suppose a state ρ is measured and an outcome corresponding the POVM element $\pi_{\nu_k,\sigma}$ is found. Looking back to Eq. (4.23), we can think of this event as first projecting ρ onto the partition labelled subspace $\mathcal{L}(\mathcal{Q}_{\nu_k} \otimes \mathcal{P}_{\nu_k})$. This can be thought of as measuring ρ to be the state of the dataset with $n-k$ zeros and k ones[4]. So at this stage, our best guess is that $\rho \in \{\rho_{\nu_k,\sigma'} : [\sigma']_{\nu_k} \in C_{\nu_k}\}$. The second step then corresponds to measuring the order of the states in the dataset, or in other words, it aims to distinguish between the states in $\{\rho_{\nu_k,\sigma'} : [\sigma']_{\nu_k} \in C_{\nu_k}\}$. In this example, we would conclude that $[\sigma']_{\nu_k} = [\sigma]_{\nu_k}$. To summarise this situation, a measurement outcome corresponding to $\pi_{\nu_k,\sigma}$ tells us (with minimal probability of error) that, first, ρ has $n-k$ zeros and k ones, and second, that these zeros and ones are jumbled up using some $\sigma \in [\sigma]_{\nu_k}$.

[4]Recall that $\nu_k = (n-k, k)$ labels the states with $n-k$ zeros and k ones.

n	$P_{\text{optimal}}(n)$	$P_{\text{guess}}(n)$
1	$1 = 100\%$	$1 = 100\%$
2	$5/8 = 62.5\%$	$1/2 = 50.0\%$
3	$5/12 \approx 41.7\%$	$1/4 = 25.0\%$
4	$169/576 \approx 29.3\%$	$1/8 = 12.5\%$

Table 4.2: Some examples of how this optimal unsupervised classification of quantum bits, with success rate $P_{\text{optimal}}(n)$, compares to a guess, with success rate $P_{\text{guess}}(n) = 2^{1-n}$.

4.2.3 Probability of success

We can now write down the probability of optimally (with respect to the minimum error figure of merit) distinguishing the n-qubit states in $R^{(n)}$. If each combination is equiprobable, $p = 1/2^{n-1}$, since the first state can, without loss of generality, be chosen to be $|\varphi_0\rangle$. Using Eq. (2.96), the optimal probability of success is found as follows

$$\begin{aligned} P_{\text{optimal}}(n) &= \frac{1}{2^{n-1}} \sum_{k=0}^{\lfloor n/2 \rfloor} \sum_{[\sigma]_{\nu_k} \in C_{\nu_k}} \text{Tr}(\pi_{\nu_k,\sigma} \rho_{\nu_k,\sigma}) \\ &= \frac{1}{2^{n-1}} \sum_{k=0}^{\lfloor n/2 \rfloor} \sum_{[\sigma]_{\nu_k} \in C_{\nu_k}} \text{Tr}(\pi_{\nu_k} \rho_{\nu_k}) \\ &= \frac{1}{2^{n-1}} \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k} \frac{(n-2k+1)^2}{(n-k+1)^2(k+1)}. \end{aligned} \tag{4.28}$$

Here, in the last step, we used $\text{Tr}(\mathbb{I}_{\nu_k} \otimes \Omega_{\nu_k}) = d_{\mathcal{Q}_{\nu_k}} = n - 2k + 1$, as well as Eq. (2.141) for $d_{\mathcal{P}_{\nu_k}}$.

To get some sense of this result, the probability of success for various values of n are noted in Table 4.2 and plotted in Fig. 4.1. As mentioned at the beginning of this section, the results derived here correspond to a special case of those found in Ref. [71], where the derived the optimal success rate of an unsupervised binary classification of n, *d-dimensional qudits* is found. This turns out to be

$$P^d_{\text{optimal}}(n) = \frac{1}{2^{n-1}} \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k} \frac{(d-1)(n-2k+1)^2}{(n-k+1)^2(d+k-1)}. \tag{4.29}$$

4.3 Intermediate classifications on four qubits

Before we launch into the general world of n qubits, to get an idea of what we might expect to see later on, let's consider, numerically, some intermediate measurements on a four-qubit dataset, with possible states $\{\rho_{0klm} : k, l, m \in \{0, 1\}\}$. First, let's see what happens when we follow the approach taken in the $2 \to 3$ qubit case and *weaken* the optimal measurement on three qubits $\{\pi_{0ij}\}$, given by Eq. (3.27), onto the identity $\mathbb{I} \in \mathcal{L}\big[\mathcal{H}^{(3)}\big]$. That is, let our intermediate measurement have the POVM elements

$$\xi_{000} = \alpha\pi_{000} + \beta_0\mathbb{I}, \tag{4.30a}$$
$$\xi_{001} = \alpha\pi_{001} + \beta_1\mathbb{I}, \tag{4.30b}$$
$$\xi_{010} = \alpha\pi_{010} + \beta_1\mathbb{I}, \tag{4.30c}$$
$$\xi_{011} = \alpha\pi_{011} + \beta_1\mathbb{I}, \tag{4.30d}$$

such that α, β_i are constrained so that $\{\xi_{0ij}\}$ is a valid POVM[5]. Following the general road map of the previous chapter, we can perform this first measurement on the first three qubits of the dataset, which

[5]Note that we have preserved the symmetries of the corresponding states with this measurement. Since we are not concerned with full generality at this stage, we have included this extra constraint, to reduce the complexity of the calculation.

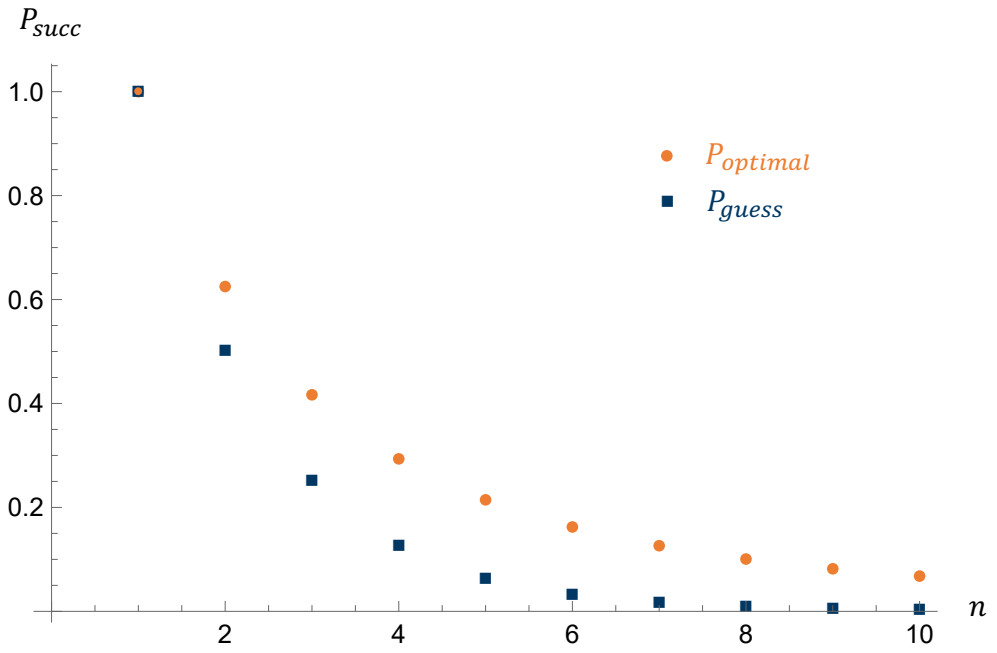

Figure 4.1: Plot showing how the success rate P_{succ} of an unsupervised binary classification on an n-qubit dataset varies with n. The orange circles correspond to the optimal success rate P_{optimal} whereas the blue squares correspond to the success rate of a guess $P_{\text{guess}}(n) = 2^{1-n}$.

updates the states $\{\rho_{0klm}\}$ as follows

$$\rho_{0klm} \to \rho_{0klm}^{0ij} = \frac{\left(\sqrt{\xi_{0ij}} \otimes \mathbb{1}\right)\rho_{0klm}\left(\sqrt{\xi_{0ij}} \otimes \mathbb{1}\right)^{\dagger}}{\text{Tr}\left(\xi_{0ij}\rho_{0klm}\right)}, \tag{4.31}$$

and then see how if affects our ability to subsequently classify all four qubits. For each choice of α, β_i, after the first measurement, we can write the second measurement as an SDP whose aim is to maximise the probability of a successful classification on all four qubits:

$$\begin{aligned} \max \quad & P_{\text{succ}}^{\text{2nd}} = \sum_{i,j,k,l,m} \text{Tr}\left(\tilde{\pi}_{0klm}^{0ij}\rho_{0klm}^{0ij}\right) \\ \text{s.t.} \quad & \sum_{k,l,m} \tilde{\pi}_{0klm}^{0ij} = \mathbb{I}, \ \forall k, \\ & \tilde{\pi}_{0klm}^{0ij} \geq 0, \end{aligned} \tag{4.32}$$

where $\left\{\tilde{\pi}_{0klm}^{0ij}\right\}_{k,l,m}$ corresponds to the POVM, distinguishing the disturbed states $\left\{\rho_{0klm}^{0ij}\right\}_{k,l,m}$, that we are maximising over. We do this numerically and plot the tradeoff between the two success rates, as shown in Fig. 4.2. Notice that there appears[6] to be no constant region in this tradeoff, and the only point at which the second classification achieves its optimal value is when the the first measurement is the identity, and $\alpha = 0$. This means that the intermediate measurement we have chosen here never allows for an optimal subsequent one (at least when $\alpha > 0$).

What if our intermediate classification was exactly the one we considered in Eq. (3.34)? We saw earlier that this allowed for the second classification on three qubits to remain at its optimal value even when the intermediate measurement became nontrivial, so one might expect, when applied to a four-qubit classification, a similar phenomenon should arise. It turns out that this is not the case. As shown in Fig. 4.3, as soon as the measurement $\{\pi_{\pm}\}$ develops a nontrivial component ($\alpha > 0$), it leads to a deviation in the success rate $P_{\text{succ}}^{\text{2nd}}(4)$ in classifying the full four-qubit dataset from its optimal value.

[6]Of course, this is not proven here, it is just a hint.

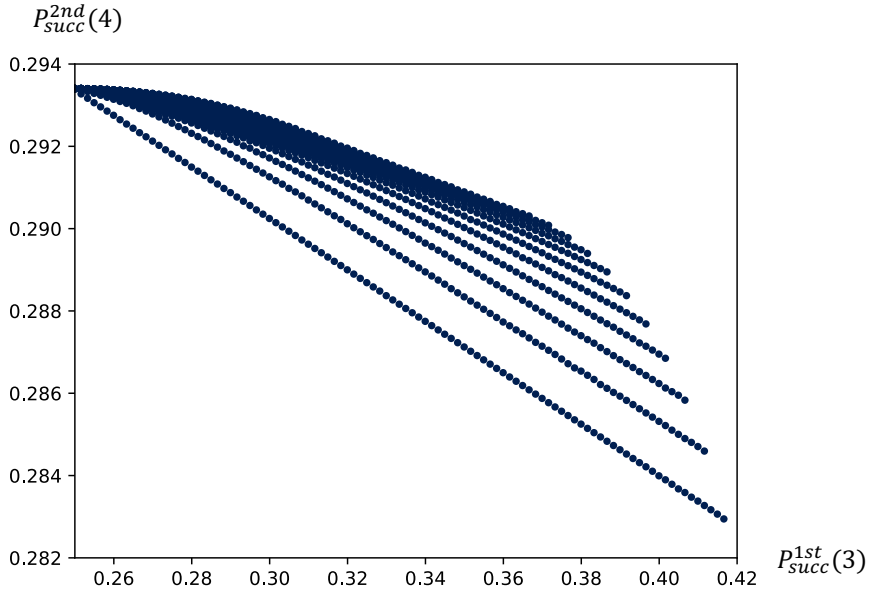

Figure 4.2: The tradeoff between the success rate $P^{\text{1st}}_{\text{succ}}(3)$ of an intermediate measurement on a three-qubit subset, given by Eq. (4.30), and the success rate $P^{\text{2nd}}_{\text{succ}}(4)$ of a subsequent classification of the full four-qubit dataset. The different lines arise due to the fact that multiple values of α, β_i give the same success rate, either in the first or second step.

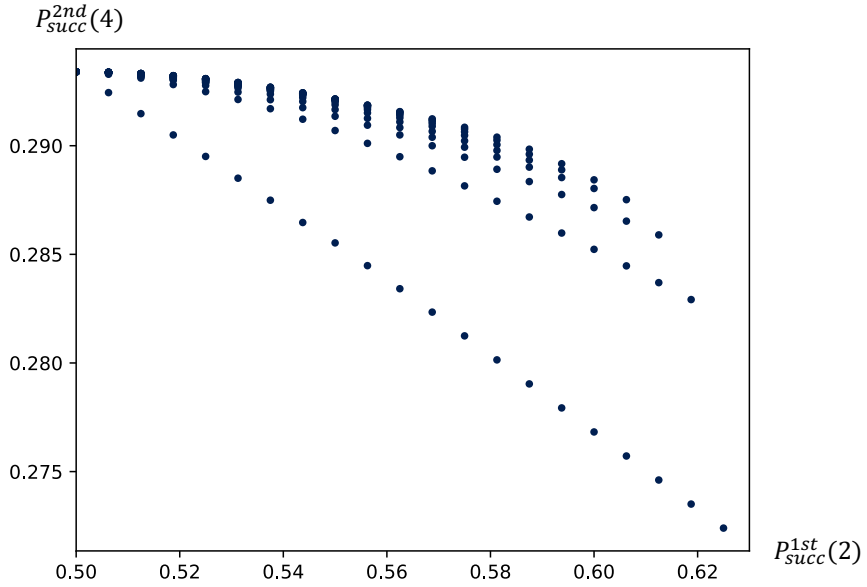

Figure 4.3: The tradeoff between the success rate $P^{\text{1st}}_{\text{succ}}(2)$ of an intermediate measurement on a two-qubit subset, given by Eq. (3.34), and the success rate $P^{\text{2nd}}_{\text{succ}}(4)$ of a subsequent classification of the full four-qubit dataset. The different lines arise due to the fact that multiple values of α, β give the same success rate, either in the first or second step.

Is there any common theme between the two cases we've considered here? One thing we can notice is that, when thinking of these intermediate classifications as measurements on the first three qubits, they tell us something about the order of the states in three-qubit subset. As we will see, this is a key observation when we generalise to n qubits.

4.4 What can we learn from an intermediate classification?

In Section 3.3, when given a quantum dataset consisting of three qubits, we saw how classifying a subset of two qubits affected our ability to classify the entire dataset. Interestingly, it was found that the first classification could be remarkably strong without affecting the success rate of the second. This naturally led us to ask the question of whether this feature generalises to an $n-1 \to n$-qubit situation. That is, we wanted to investigate how successful an initial classification on $n-1$ qubits could be without affecting the success rate of a classification on the full n-qubit dataset. In this section, we ask the question: "what can we learn from an intermediate classification?", and we get the impression that nothing about the order of the first $n-1$ qubits in the dataset can be deduced without affecting the overall optimal success rate of the second classification on n qubits[7]. Before making steps to show this in full generality, we first set up the problem in Sec. 4.4.1 and then return to the $2 \to 3$-qubit scenario in Sec. 4.4.2 in order to motivate and gain some intuition about the approach taken in the $n-1 \to n$-qubit case.

4.4.1 Problem setup

Let's set up the problem in the form that we use to derive our results. First of all, we should make clear that we will be taking $n > 2$. This is because, when $n = 2$, the intermediate measurements on $n-1 = 1$ is trivial. With that, let

$$\Xi^{(n-1)} = \{\xi_{\mu_j,\tau} : [\tau]_{\mu_j} \in C_{\mu_j},\ 0 \leq j \leq (n-1)/2\} \tag{4.33}$$

be our intermediate measurement on the first $n-1$ qubits of the n-qubit dataset we considered in the Sec. 4.2. Here, $\mu_j = (n-1-j, j)$ are the partitions labelling the $(n-1)$-qubit states, measurement operators and irreps; and C_{μ_j} are the sets of equivalence classes defined analogously to their n qubit counterparts C_{ν_k} in Def. 4.2.1 and Eq. (4.19). The purpose of $\Xi^{(n-1)}$ is to distinguish between the states in

$$R^{(n-1)} = \{\rho_{\mu_j,\tau} : [\tau]_{\mu_j} \in C_{\mu_j},\ 0 \leq j \leq (n-1)/2\}, \tag{4.34}$$

where, similarly to the n-qubit case,

$$\rho_{\mu_j,\tau} = \frac{1}{(n-j)(j+1)} \bigoplus_{i=0}^{j} \mathbb{I}_{\mathcal{Q}_{\mu_i}} \otimes \Omega_{\mu_i,\tau}. \tag{4.35}$$

To understand this notation, we define irreducible representations of SU(2) and S_{n-1} on $n-1$ qubits as $(\mathbf{q}_{\mu_j}, \mathcal{Q}_{\mu_j})$ and $(\mathbf{p}_{\mu_j}, \mathcal{P}_{\mu_j})$ respectively. So, analogously to the n-qubit case in Eq. (4.16), $\mathbb{I}_{\mathcal{Q}_{\mu_i}}$ is the identity operator on $\mathcal{Q}_{\mu_i}$ and $\Omega_{\mu_i,\tau} = \mathbf{p}_{\mu_i}(\tau)\Omega_{\mu_i}\mathbf{p}^{\dagger}_{\mu_i}(\tau) \in \mathcal{L}(\mathcal{P}_{\mu_i})$ are pure states.

Returning to the n-qubit picture, we first perform the measurement

$$\Xi^{(n)} := \{\xi_{\mu_j,\tau} \otimes \mathbb{1} : [\tau]_{\mu_j} \in C_{\mu_j},\ 0 \leq j \leq (n-1)/2\} \tag{4.36}$$

on an n-qubit quantum dataset prepared in some state in $R^{(n)}$, given in Eq. (4.22). Following this, supposing a measurement outcome of (μ_j, τ) is found, a second measurement $\{\pi^{\mu_j,\tau}_{\nu_k,\sigma}\}_{k,\sigma}$ is performed to try and distinguish the (now disturbed) states $\{\rho^{\mu_j,\tau}_{\nu_k,\sigma}\}_{k,\sigma}$, such that

$$\rho^{\mu_j,\tau}_{\nu_k,\sigma} := \frac{\left(\sqrt{\xi_{\mu_j,\tau}} \otimes \mathbb{1}\right)\rho_{\nu_k,\sigma}\left(\sqrt{\xi_{\mu_j,\tau}} \otimes \mathbb{1}\right)^{\dagger}}{\mathrm{Tr}\left[(\xi_{\mu_j,\tau} \otimes \mathbb{1})\rho_{\nu_k,\sigma}\right]}. \tag{4.37}$$

[7] Assuming the optimal POVM, given in Eq. (4.23), is unique - at least in its elements' $\mathcal{P}_{\nu_k}$ components.

The success rate of the second measurement is given by

$$P_{\text{succ}}^{\text{2nd}} = \sum_{j=0}^{\lfloor (n-1)/2 \rfloor} \sum_{[\tau]_{\mu_j} \in C_{\mu_j}} \sum_{k=0}^{\lfloor n/2 \rfloor} \sum_{[\sigma]_{\nu_k} \in C_{\nu_k}} P(\rho_{\nu_k,\sigma}^{\mu_j,\tau}) \operatorname{Tr}(\pi_{\nu_k,\sigma}^{\mu_j,\tau} \rho_{\nu_k,\sigma}^{\mu_j,\tau})$$
$$= \frac{1}{2^{n-1}} \sum_j \sum_{[\tau]_{\mu_j}} \sum_k \sum_{[\sigma]_{\nu_k}} \operatorname{Tr}\left[\pi_{\nu_k,\sigma}^{\mu_j,\tau} \Big(\sqrt{\xi_{\mu_j,\tau}} \otimes \mathbb{1} \Big) \rho_{\nu_k,\sigma} \Big(\sqrt{\xi_{\mu_j,\tau}} \otimes \mathbb{1} \Big)^\dagger \right], \tag{4.38}$$

which, using the cyclical property of the trace, can be rewritten as

$$P_{\text{succ}}^{\text{2nd}} = \frac{1}{2^{n-1}} \sum_j \sum_{[\tau]_{\mu_j}} \sum_k \sum_{[\sigma]_{\nu_k}} \operatorname{Tr}\left[\Big(\sqrt{\xi_{\mu_j,\tau}} \otimes \mathbb{1} \Big)^\dagger \pi_{\nu_k,\sigma}^{\mu_j,\tau} \Big(\sqrt{\xi_{\mu_j,\tau}} \otimes \mathbb{1} \Big) \rho_{\nu_k,\sigma} \right]. \tag{4.39}$$

Note that since $\{\pi_{\nu_k,\sigma}^{\mu_j,\tau}\}_{k,\sigma}$ is a POVM for every j, τ, it follows that

$$\left\{ \pi_{\nu_k,\sigma} := \sum_j \sum_{[\tau]_{\mu_j}} \Big(\sqrt{\xi_{\mu_j,\tau}}^\dagger \otimes \mathbb{1} \Big) \pi_{\nu_k,\sigma}^{\mu_j,\tau} \Big(\sqrt{\xi_{\mu_j,\tau}} \otimes \mathbb{1} \Big) \right\}_{k,\sigma}, \tag{4.40}$$

is also one. Therefore, $P_{\text{succ}}^{\text{2nd}}$ takes its optimal value, given by Eq. (4.28), if and only if $\{\pi_{\nu_k,\sigma}\}$ make up an optimal POVM classifying the n-qubit dataset.

Now, defining the Kraus operators

$$A_{\nu_k,\sigma}^{\mu_j,\tau} := \sqrt{\pi_{\nu_k,\sigma}^{\mu_j,\tau}} \Big(\sqrt{\xi_{\mu_j,\tau}} \otimes \mathbb{1} \Big), \tag{4.41}$$

it follows that

$$\pi_{\nu_k,\sigma} = \sum_j \sum_{[\tau]_{\mu_j}} A_{\nu_k,\sigma}^{\mu_j,\tau\,\dagger} A_{\nu_k,\sigma}^{\mu_j,\tau}. \tag{4.42}$$

Further, Eq. (4.41) implies that

$$\sum_k \sum_{[\sigma]_{\nu_k}} A_{\nu_k,\sigma}^{\mu_j,\tau\,\dagger} A_{\nu_k,\sigma}^{\mu_j,\tau} = \sum_k \sum_{[\sigma]_{\nu_k}} \Big(\sqrt{\xi_{\mu_j,\tau}} \otimes \mathbb{1} \Big)^\dagger \pi_{\nu_k,\sigma}^{\mu_j,\tau} \Big(\sqrt{\xi_{\mu_j,\tau}} \otimes \mathbb{1} \Big). \tag{4.43}$$

So, by requiring the completeness of $\{\pi_{\nu_k,\sigma}^{\mu_j,\tau}\}_{k,\sigma}$, this leads to

$$\xi_{\mu_k,\tau} \otimes \mathbb{1} = \sum_k \sum_{[\sigma]_{\nu_j}} A_{\nu_k,\sigma}^{\mu_j,\tau\,\dagger} A_{\nu_k,\sigma}^{\mu_j,\tau}. \tag{4.44}$$

We can therefore note the aim of our approach: To find positive operators $B_{\nu_k,\sigma}^{\mu_j,\tau} := A_{\nu_k,\sigma}^{\mu_j,\tau\,\dagger} A_{\nu_k,\sigma}^{\mu_j,\tau}$ that maximise

$$P_{\text{succ}}^{\text{1st}} = \frac{1}{2^{n-2}} \sum_j \sum_{[\tau]_{\mu_j}} \operatorname{Tr}(\xi_{\mu_j,\tau} \rho_{\mu_j,\tau}), \tag{4.45}$$

whilst satisfying

$$\xi_{\mu_j,\tau} \otimes \mathbb{1} = \sum_{k=0}^{\lfloor n/2 \rfloor} \sum_{[\sigma]_{\nu_k} \in C_{\nu_k}} B_{\nu_k,\sigma}^{\mu_j,\tau}, \tag{4.46a}$$

$$\pi_{\nu_k,\sigma} = \sum_{j=0}^{\lfloor (n-1)/2 \rfloor} \sum_{[\tau]_{\mu_j} \in C_{\mu_j}} B_{\nu_k,\sigma}^{\mu_j,\tau}, \tag{4.46b}$$

for some fixed POVM $\Pi = \{\pi_{\nu_k,\sigma}\}$, that optimally classifies the undisturbed n-qubit dataset. To make the results that we derive completely general, we would allow Π to be any optimal POVM on the n-qubits, but we leave this to future work.

4.4.1.1 Aside: a more general problem

Notice that this formulation allows us to, at least numerically, solve a more general problem. Suppose we have some non-degenerate optimal measurement $\{\pi_k\}$ that distinguishes the states in $R = \{\rho_k\}$ with probability $P_{\text{succ}}^{\text{general}} = \sum_k p_k \operatorname{Tr}(\pi_k \rho_k)$, such that p_i is the probability of the state ρ_i being prepared. Then, what is the best intermediate measurement $\{\xi_j\}$, to distinguish the states $R' = \{\rho_j\} \subseteq R$, that we can perform without affecting $P_{\text{succ}}^{\text{general}}$? It is likely that this problem can be solved efficiently because we can formulate it as a semidefinite programme (SDP) [49, 50].

To do this, first note that we're allowing R' to be a subset of R, meaning that we do not necessarily distinguish all the states in R during our first classification. To account for this, suppose we do not wish to distinguish the states $\{\rho_{j_1}, \dots, \rho_{j_m} \mid m < |R|\}$, let us define $\tilde{\rho_j} := \sum_{i=1}^{m} p_{j_i} \rho_{j_i}$. Then our aim is really for our first measurement $\{\xi_j\}$ to distinguish the states $\{\tilde{\rho}_j\}$. Indeed, the goal is to maximise $P_{\text{intermediate}} = \sum_j \operatorname{Tr}(\xi_j \tilde{\rho}_j)$ subject to the conditions

$$\xi_j = \sum_k B_k^j, \tag{4.47a}$$

$$\pi_k = \sum_j B_k^j, \tag{4.47b}$$

where $B_k^j \geq 0$. This can be rewritten as the primal problem of an SDP as follows.

$$\begin{aligned} &\max \sum_{j,k} \operatorname{Tr}(B_k^j \tilde{\rho}_j) \\ &\text{s.t.} \ \sum_j B_k^j = \pi_k, \ \forall k, \\ &\quad B_k^j \geq 0. \end{aligned} \tag{4.48}$$

SDPs can often be solved efficiently numerically [50], so this could be a practical way of investigating this problem. It would also be interesting to see if, similarly to how the Holevo conditions for minimum error quantum state discrimination can be found analytically using SDP methods [50], conditions could be derived for this problem. However, we leave this to future work.

4.4.2 Returning to three qubits

Let's now return to the $2 \to 3$-qubit situation and derive the POVM that best classifies the first two qubits *without* affecting the subsequent, overall success rate in classifying the full three-qubit dataset. Indeed, let us do so using our new, partition based notation so that we can go on to generalise these results with some intuition. First, let $\tilde{\sigma} = (123) \in S_3$, so that we can write the four possible three-qubit states representing our entire quantum dataset using the partition notation (with the old notation also included for comparison):

$$\rho_{\nu_0} = \frac{1}{4}\mathbb{I}_{\mathcal{Q}_{\nu_0}} \otimes \Omega_{\nu_0} \quad \sim \quad \rho_{000} = \frac{1}{4}\mathbb{I}_{\frac{3}{2}}, \tag{4.49a}$$

$$\rho_{\nu_1} = \frac{1}{6}\Big(\mathbb{I}_{\mathcal{Q}_{\nu_0}} \otimes \Omega_{\nu_0}\Big) \oplus \Big(\mathbb{I}_{\mathcal{Q}_{\nu_1}} \otimes \Omega_{\nu_1}\Big) \quad \sim \quad \rho_{001} = \frac{1}{6}\mathbb{I}_{\frac{3}{2}} + \frac{1}{6}\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{4.49b}$$

$$\rho_{\nu_1,\tilde{\sigma}} = \frac{1}{6}\Big(\mathbb{I}_{\mathcal{Q}_{\nu_0}} \otimes \Omega_{\nu_0}\Big) \oplus \Big(\mathbb{I}_{\mathcal{Q}_{\nu_1}} \otimes \Omega_{\nu_1,\tilde{\sigma}}\Big) \quad \sim \quad \rho_{010} = \frac{1}{6}\mathbb{I}_{\frac{3}{2}} + \frac{1}{24}\mathbb{I}_{\frac{1}{2}} \otimes \big(|1\rangle - \sqrt{3}|0\rangle\big)\big(\langle 1| - \sqrt{3}\langle 0|\big), \tag{4.49c}$$

$$\rho_{\nu_1,\tilde{\sigma}^2} = \frac{1}{6}\Big(\mathbb{I}_{\mathcal{Q}_{\nu_0}} \otimes \Omega_{\nu_0}\Big) \oplus \Big(\mathbb{I}_{\mathcal{Q}_{\nu_1}} \otimes \Omega_{\nu_1,\tilde{\sigma}^2}\Big) \quad \sim \quad \rho_{011} = \frac{1}{6}\mathbb{I}_{\frac{3}{2}} + \frac{1}{24}\mathbb{I}_{\frac{1}{2}} \otimes \big(|1\rangle + \sqrt{3}|0\rangle\big)\big(\langle 1| + \sqrt{3}\langle 0|\big). \tag{4.49d}$$

Note that since $(\mathbf{p}_{\nu_0}, \mathcal{P}_{\nu_0})$ is the trivial irrep of S_3, $\Omega_{\nu_0,\sigma} = \Omega_{\nu_0,\sigma^2} = \Omega_{\nu_0}, \ \forall \sigma \in S_3$.

Now, suppose we perform an intermediate measurement $\{\xi_{\mu_j,\tau} \equiv \xi_{\mu_j}\}$ that distinguishes the two-qubit

states[8]

$$\rho_{\mu_0} = \frac{1}{3}\mathbb{I}_{\mathcal{Q}_{\mu_0}} \otimes \Omega_{\mu_0} \qquad \sim \quad \rho_{00} = \frac{1}{3}\mathbb{I}_1, \tag{4.50a}$$

$$\rho_{\mu_1} = \frac{1}{4}\Big(\mathbb{I}_{\mathcal{Q}_{\mu_0}} \otimes \Omega_{\mu_0}\Big) \oplus \Big(\mathbb{I}_{\mathcal{Q}_{\mu_1}} \otimes \Omega_{\mu_1}\Big) \quad \sim \quad \rho_{01} = \frac{1}{4}\mathbb{I}_1 \oplus \mathbb{I}_0, \tag{4.50b}$$

where $\xi_{\mu_0} \sim \xi_{00}$, $\xi_{\mu_1} \sim \xi_{01}$. As we have discussed before, we can think of this as the measurement $\{\xi_{\mu_j} \otimes \mathbb{1}\}$ on the three-qubit states in Eq. (4.49). Tailoring the message of the previous subsection to this scenario, our aim is to find positive operators $B^{\mu_j}_{\nu_k,\sigma}$ that maximise

$$P^{\text{1st}}_{\text{succ}} = \frac{1}{2}\operatorname{Tr}(\xi_{\mu_0}\rho_{\mu_0} + \xi_{\mu_1}\rho_{\mu_1}) \quad \sim \quad P^{\text{1st}}_{\text{succ}} = \frac{1}{2}\operatorname{Tr}(\xi_{00}\rho_{00} + \xi_{01}\rho_{01}), \tag{4.51}$$

whilst satisfying

$$\xi_{\mu_j} \otimes \mathbb{1} = \sum_{k=0}^{1}\sum_{[\sigma]_{\nu_k}} B^{\mu_j}_{\nu_k,\sigma} \quad \sim \quad \xi_{0u} \otimes \mathbb{1} = B^{0u}_{000} + B^{0u}_{001} + B^{0u}_{010} + B^{0u}_{011}, \tag{4.52a}$$

$$\pi_{\nu_k,\sigma} = \sum_{j=0}^{1} B^{\mu_j}_{\nu_k,\sigma} \qquad \sim \qquad \pi_{0vw} = B^{00}_{0vw} + B^{01}_{0vw}, \tag{4.52b}$$

for all $j,k \in \{0,1\}$, $[\sigma]_{\nu_k} \in C_{\nu_k}$, $u,v,w \in \{0,1\}$.

Let's now deduce more about the form of the intermediate measurement. First of all, as it will be shown explicitly in Sec. 4.4.3, we can take

$$\xi_{\mu_j} = \big(\mathbb{I}_{\mathcal{Q}_{\mu_0}} \otimes \Theta^{(\mu_j)}_{\mu_0}\big) \oplus \big(\mathbb{I}_{\mathcal{Q}_{\mu_1}} \otimes \Theta^{(\mu_j)}_{\mu_1}\big) \quad \sim \quad \xi_{0u} = \Big(\theta^{(0u)}_1\mathbb{I}_1\Big) \oplus \Big(\theta^{(0u)}_0\mathbb{I}_0\Big), \tag{4.53}$$

where $j,u \in \{0,1\}$, $\Theta^{(\mu_j)}_{\mu_i} \in \mathcal{L}(\mathcal{P}_{\mu_i})$ are positive operators, $\theta^{(0u)}_{s_{\mu_i}} \geq 0$ can be taken to be real numbers[9], such that the subscript s_{μ_i} denotes the total spin of the corresponding two-qubit subspace labelled by μ_i. Further, in order to ensure the completeness of $\{\xi_{\mu_j}\} \sim \{\xi_{0u}\}$, we require

$$\sum_{j=0}^{1} \Theta^{(\mu_j)}_{\mu_i} = \mathbb{I}_{\mathcal{P}_{\mu_i}} \quad \sim \quad \theta^{(00)}_{s_{\mu_i}} + \theta^{(01)}_{s_{\mu_i}} = 1, \tag{4.54}$$

for all $i \in \{0,1\}$. In words, ξ_{μ_j} can take this form because the probabilities associated with the first and second measurements require the *outcomes* of the first measurement to be invariant under SU(2), a feature coming from the commutativity of ρ_{μ_j} with $\mathbf{Q}^{(2)}[\mathrm{SU}(2)]$. Now, let's think back to spin addition which says that $\mathcal{Q}_s \otimes \mathcal{Q}_{\frac{1}{2}} \cong \mathcal{Q}_{s+\frac{1}{2}} \oplus \mathcal{Q}_{s-\frac{1}{2}}$. We can rewrite this in partition notation as $\mathcal{Q}_{\mu_i} \otimes \mathcal{Q}_{(1,0)} \cong \mathcal{Q}_{\nu_i} \oplus \mathcal{Q}_{\nu_{i+1}}$ which, along with Ref. [72], motivates the following[10]:

$$\xi_{\mu_j} \otimes \mathbb{1} = \bigoplus_{k=0}^{1} \mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \Big(\big[\Theta^{(\mu_j)}_{\mu_k} \otimes |0\rangle\langle 0|\big] \oplus \big[\Theta^{(\mu_j)}_{\mu_{k-1}} \otimes |1\rangle\langle 1|\big]\Big)$$

$$\sim \quad \xi_{0u} \otimes \mathbb{1} = \Big(\theta^{(0u)}_1\mathbb{I}_{\frac{3}{2}}\Big) \oplus \Big(\mathbb{I}_{\frac{1}{2}} \otimes \big[\theta^{(0u)}_1|1\rangle\langle 1| + \theta^{(0u)}_0|0\rangle\langle 0|\big]\Big), \tag{4.55}$$

written in the Schur basis. Here, if μ_{k-1} is undefined, like when $k=0$, we take $\Theta^{(\mu_j)}_{\mu_{k-1}} = 0$.

Next, we look at Eq. (4.52b) to find out something about the positive operators $B^{\mu_j}_{\nu_k,\sigma}$. It is at this point that we fix a specific form of the optimal POVM on three undisturbed qubits. Namely, $\Pi^{(3)} = \{\pi_{\nu_k,\sigma}\}$

[8] The independence of $\tau \in S_2$ comes from the two-qubit states being invariant under permutation of qubits.

[9] Since $\Theta^{(\mu_j)}_{\mu_0}, \Theta^{(\mu_j)}_{\mu_1}$ are both one-dimensional. Indeed, $\Theta^{(\mu_j)}_{\mu_i}$ can also be taken to be positive real numbers, however, we have written them in the full tensor product form to make the generalisation clearer when we come to it.

[10] Again, more detail will be provided in Sec 4.4.3.

given by Eq. (3.27) or, more generally, Eq. (4.23). Writing this measurement in partition notation (using $\tilde{\sigma} = (123) \in S_3$ again),

$$\pi_{\nu_0} = \mathbb{I}_{\mathcal{Q}_{\nu_0}} \otimes \Omega_{\nu_0} \quad \sim \quad \pi_{000} = \mathbb{I}_{\frac{3}{2}}, \tag{4.56a}$$

$$\pi_{\nu_1} = \frac{2}{3}\mathbb{I}_{\mathcal{Q}_{\nu_1}} \otimes \Omega_{\nu_1} \quad \sim \quad \pi_{001} = \frac{2}{3}\mathbb{I}_{\frac{1}{2}} \otimes |1\rangle\langle 1|, \tag{4.56b}$$

$$\pi_{\nu_1,\tilde{\sigma}} = \frac{2}{3}\mathbb{I}_{\mathcal{Q}_{\nu_1}} \otimes \Omega_{\nu_1,\tilde{\sigma}} \quad \sim \quad \pi_{010} = \frac{1}{6}\mathbb{I}_{\frac{1}{2}} \otimes \big(|1\rangle - \sqrt{3}|0\rangle\big)\big(\langle 1| - \sqrt{3}\langle 0|\big), \tag{4.56c}$$

$$\pi_{\nu_1,\tilde{\sigma}^2} = \frac{2}{3}\mathbb{I}_{\mathcal{Q}_{\nu_1}} \otimes \Omega_{\nu_1,\tilde{\sigma}^2} \quad \sim \quad \pi_{011} = \frac{1}{6}\mathbb{I}_{\frac{1}{2}} \otimes \big(|1\rangle + \sqrt{3}|0\rangle\big)\big(\langle 1| + \sqrt{3}\langle 0|\big). \tag{4.56d}$$

Since $\Omega_{\nu_k,\sigma}$ are pure states, this means that $B^{\mu_j}_{\nu_k,\sigma}$ have the form

$$B^{\mu_j}_{\nu_0} = D^{\mu_j}_{\nu_0} \otimes \Omega_{\nu_0} \quad \sim \quad B^{0u}_{000} = D^{0u}_{000}, \tag{4.57a}$$

$$B^{\mu_j}_{\nu_1} = D^{\mu_j}_{\nu_1} \otimes \Omega_{\nu_1} \quad \sim \quad B^{0u}_{001} = D^{0u}_{001} \otimes |1\rangle\langle 1|, \tag{4.57b}$$

$$B^{\mu_j}_{\nu_1,\tilde{\sigma}} = D^{\mu_j}_{\nu_1,\tilde{\sigma}} \otimes \Omega_{\nu_1,\tilde{\sigma}} \quad \sim \quad B^{0u}_{010} = \frac{1}{4}D^{0u}_{010} \otimes \big(|1\rangle - \sqrt{3}|0\rangle\big)\big(\langle 1| - \sqrt{3}\langle 0|\big), \tag{4.57c}$$

$$B^{\mu_j}_{\nu_1,\tilde{\sigma}^2} = D^{\mu_j}_{\nu_1,\tilde{\sigma}^2} \otimes \Omega_{\nu_1,\tilde{\sigma}^2} \quad \sim \quad B^{0u}_{011} = \frac{1}{4}D^{0u}_{011} \otimes \big(|1\rangle + \sqrt{3}|0\rangle\big)\big(\langle 1| + \sqrt{3}\langle 0|\big), \tag{4.57d}$$

such that $D^{\mu_j}_{\nu_k,\sigma} \in \mathcal{L}(\mathcal{Q}_{\nu_k})$ are positive operators (likewise, $D^{0u}_{0vw} \geq 0$).

To finish off the derivation of the optimal success rate we can achieve in this first classification, we follow two paths. Along the first, we use our old notation along with a slightly more brute force, but explicit approach. Along the second path, we move over to our new notation and use a moderately sized sledgehammer to crack the same nut. We will see that this latter approach will be more useful in generalising to n qubits.

4.4.2.1 Optimal value using old notation

Let us first see how we can obtain the upper bound of $P^{\text{1st}}_{\text{succ}}$ in our old notation. To do this, let's compare

$$\begin{aligned}\xi_{0u} \otimes \mathbb{1} = D^{0u}_{000} + D^{0u}_{001} \otimes |1\rangle\langle 1| \\ + \frac{1}{4}D^{0u}_{010} \otimes \big(|1\rangle - \sqrt{3}|0\rangle\big)\big(\langle 1| - \sqrt{3}\langle 0|\big) + \frac{1}{4}D^{0u}_{011} \otimes \big(|1\rangle + \sqrt{3}|0\rangle\big)\big(\langle 1| + \sqrt{3}\langle 0|\big)\end{aligned} \tag{4.58}$$

with Eq. (4.55). Since $\mathbb{I}_{\frac{3}{2}}, D^{0u}_{000} \in \mathcal{L}(\mathcal{Q}_{\frac{3}{2}})$ and $\mathbb{I}_{\frac{1}{2}}, D^{0u}_{001}, D^{0u}_{010}, D^{0u}_{011} \in \mathcal{L}(\mathcal{Q}_{\frac{1}{2}})$, it follows that

$$\theta^{(0u)}_1 \mathbb{I}_{\frac{3}{2}} = D^{0u}_{000}, \tag{4.59a}$$

$$\theta^{(0u)}_1 \mathbb{I}_{\frac{1}{2}} = D^{0u}_{001} + \frac{1}{4}D^{0u}_{010} + \frac{1}{4}D^{0u}_{011}, \tag{4.59b}$$

$$\theta^{(0u)}_0 \mathbb{I}_{\frac{1}{2}} = \frac{3}{4}\big(D^{0u}_{010} + D^{0u}_{011}\big), \tag{4.59c}$$

$$0 = \frac{\sqrt{3}}{4}\big(D^{0u}_{010} - D^{0u}_{011}\big), \tag{4.59d}$$

where Eq. (4.59b) comes from the $|1\rangle\langle 1|$ component of Eq. (4.58); Eq. (4.59c) from the $|0\rangle\langle 0|$ component; and Eq. (4.59d) from the $|0\rangle\langle 1|$ or $|1\rangle\langle 0|$ component. This system of equations can be simplified to

$$D^{0u}_{000} = \theta^{(0u)}_1 \mathbb{I}_{\frac{3}{2}}, \tag{4.60a}$$

$$D^{0u}_{001} = \left[\theta^{(0u)}_1 - \frac{1}{3}\theta^{(0u)}_0\right]\mathbb{I}_{\frac{1}{2}}, \tag{4.60b}$$

$$D^{0u}_{010} = D^{0u}_{011} = \frac{2}{3}\theta^{(0u)}_0 \mathbb{I}_{\frac{1}{2}}. \tag{4.60c}$$

Now, using Eq. (4.51), Eq. (4.53) and Eq. (4.54), we find that

$$P_{\text{succ}}^{\text{1st}} = \frac{1}{2} + \frac{1}{8}\theta_1^{(00)} - \frac{1}{8}\theta_0^{(00)}. \tag{4.61}$$

Our task is to maximise this quantity. Being planar, we look to the extreme values of $\theta_1^{(00)}, \theta_0^{(00)}$ to do so - namely, the maximum of $\theta_1^{(00)}$ and the minimum of $\theta_0^{(00)}$. Looking back to Eq. (4.54), along with Eq. (4.60), note that, requiring positivity of D_{0vw}^{0u} means that

$$\theta_1^{(00)}, \big[1 - \theta_1^{(00)}\big] \geq 0, \tag{4.62a}$$

$$\big[3\theta_1^{(00)} - \theta_0^{(00)}\big], \big[2 + \theta_0^{(00)} - 3\theta_1^{(00)}\big] \geq 0, \tag{4.62b}$$

$$\theta_0^{(00)}, \big[1 - \theta_0^{(00)}\big] \geq 0. \tag{4.62c}$$

This implies that $\theta_1^{(00)} \leq \big(\theta_0^{(00)} + 2\big)/3$ and thus,

$$P_{\text{succ}}^{\text{1st}} \leq \frac{7}{12} - \frac{1}{12}\theta_0^{(00)}. \tag{4.63}$$

So, since $\theta_0^{(00)} \geq 0$, we finally have that

$$P_{\text{succ}}^{\text{1st}} \leq \frac{7}{12}, \tag{4.64}$$

with $7/12$ occurring when $\theta_0^{(00)} = 0$ and $\theta_1^{(00)} = 2/3$, and thus

$$\xi_{00} = \frac{2}{3}\mathbb{I}_1, \tag{4.65a}$$

$$\xi_{01} = \left[\frac{1}{3}\mathbb{I}_1\right] \oplus \mathbb{I}_0. \tag{4.65b}$$

4.4.2.2 Optimal value using new notation

Let's now derive this upper bound using the new partition notation. We first note that $\Omega_{\nu_1} = \Omega_{\mu_0} \otimes |1\rangle\langle 1|$, which means that $\Omega_{\nu_1,\sigma} = \mathbf{p}_{\nu_1}(\sigma)(\Omega_{\mu_0} \otimes |1\rangle\langle 1|)\mathbf{p}_{\nu_1}^\dagger(\sigma)$. Once again taking $\tilde{\sigma} = (123)$, we can therefore write

$$\begin{aligned}
\xi_{\mu_j} \otimes \mathbb{1} &= B_{\nu_0}^{\mu_j} + B_{\nu_1}^{\mu_j} + B_{\nu_1,\tilde{\sigma}}^{\mu_j} + B_{\nu_1,\tilde{\sigma}^2}^{\mu_j} \\
&= D_{\nu_0}^{\mu_j} \otimes \Omega_{\nu_0} + D_{\nu_1}^{\mu_j} \otimes \big(\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big) \\
&\qquad + D_{\nu_1,\tilde{\sigma}}^{\mu_j} \otimes \mathbf{p}_{\nu_1}(\tilde{\sigma})\big(\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big)\mathbf{p}_{\nu_1}^\dagger(\tilde{\sigma}) + D_{\nu_1,\tilde{\sigma}^2}^{\mu_j} \otimes \mathbf{p}_{\nu_1}(\tilde{\sigma}^2)\big(\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big)\mathbf{p}_{\nu_1}^\dagger(\tilde{\sigma}^2),
\end{aligned} \tag{4.66}$$

which must agree with Eq. (4.55).

We can see immediately that the first term $D_{\nu_0}^{\mu_j} \otimes \Omega_{\nu_0} \in \mathcal{L}(\mathcal{Q}_{\nu_0} \otimes \mathcal{P}_{\nu_0})$ has the correct block diagonal form[11] of Eq. (4.55), so let's focus on the remaining, $\mathcal{L}(\mathcal{Q}_{\nu_0} \otimes \mathcal{P}_{\nu_0})$ terms. These can be rewritten as:

$$\begin{aligned}
B_{\nu_1}^{\mu_j} + B_{\nu_1,\tilde{\sigma}}^{\mu_j} + B_{\nu_1,\tilde{\sigma}^2}^{\mu_j} = &\sum_{[\tau \in S_2]_{\nu_1}} D_{\nu_1,\tau}^{\mu_j} \otimes \mathbf{p}_{\nu_1}(\tau)\big(\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big)\mathbf{p}_{\nu_1}^\dagger(\tau) \\
&+ \sum_{[\sigma \in S_3 \backslash S_2]_{\nu_1}} D_{\nu_1,\sigma}^{\mu_j} \otimes \mathbf{p}_{\nu_1}(\sigma)\big(\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big)\mathbf{p}_{\nu_1}^\dagger(\sigma),
\end{aligned} \tag{4.67}$$

where $[\sigma \in X]_{\nu_1} := \{\sigma' \in X \subset S_3 \mid \sigma' \sim_{\nu_1} \sigma\}$, such that $\sim_{\nu_1}$ is the equivalence relation on three-qubit states defined in Def. 4.2.1[12]. Next, we can see that the first sum in the above expression is in the block diagonal form we are looking for, since

$$\sum_{[\tau \in S_2]_{\nu_1}} D_{\nu_1,\tau}^{\mu_j} \otimes \mathbf{p}_{\nu_1}(\tau)\big(\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big)\mathbf{p}_{\nu_1}^\dagger(\tau) = D_{\nu_1}^{\mu_j} \otimes \big(\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big). \tag{4.68}$$

[11] By block diagonal, we mean a matrix that is made of square matrices along its diagonal. If these square matrices are constant, we will call the whole matrix block constant.

[12] To make Eq. (4.67) clear, the first sum has one term since $S_2 = \{e, (12)\}$ and $[e]_{\nu_1} \equiv [(12)]_{\nu_1}$, whereas the second sum has two terms since $S_3 \backslash S_2 = \{(123), (132), (13), (23)\}$ and $[(123)]_{\nu_1} \equiv [(23)]_{\nu_1} \not\equiv [(132)]_{\nu_1} \equiv [(13)]_{\nu_1}$.

For the remaining sum, recalling the derivation of Eq. (4.60), we found that in order to achieve the block diagonal form (that is, with no cross terms: $|0\rangle\langle 1|$ or $|1\rangle\langle 0|$), we required $D^{0u}_{010} = D^{0u}_{011}$. This corresponds, here, to requiring $D^{\mu_j}_{\nu_1,\sigma} = D^{\mu_j}_{\nu_1,\sigma'}$, $\forall \sigma, \sigma' \in S_3\backslash S_2$. The question we will have to answer later is whether this is also the case in the more general setting. That is, in order for the sum over $[\sigma \in S_n\backslash S_{n-1}]_{\nu_k}$, to be block diagonal, does $D^{\mu_j}_{\nu_k,\sigma} = D^{\mu_j}_{\nu_k,\sigma'}$ have to be true $\forall \sigma, \sigma' \in S_n\backslash S_{n-1}$?

So, equating the two forms of $\xi_{\mu_j} \otimes \mathbb{1}$, given in Eq. (4.55) and Eq. (4.66), so far we have

$$\begin{aligned}\Big(\mathbb{I}_{\mathcal{Q}_{\nu_0}} \otimes \big[\Theta^{(\mu_j)}_{\mu_0} \otimes |0\rangle\langle 0|\big]\Big) \oplus \Big(\mathbb{I}_{\mathcal{Q}_{\nu_1}} \otimes \big[(\Theta^{(\mu_j)}_{\mu_1} \otimes |0\rangle\langle 0|) \oplus (\Theta^{(\mu_j)}_{\mu_0} \otimes |1\rangle\langle 1|)\big]\Big) \\ = \Big(D^{\mu_j}_{\nu_0} \otimes \Omega_{\nu_0}\Big) \oplus \Big(D^{\mu_j}_{\nu_1} \otimes \big[\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big] + D^{\mu_j}_{\nu_1,\tilde{\sigma}} \otimes \sum_{[\sigma \in S_3\backslash S_2]_{\nu_1}} \mathbf{p}_{\nu_1}(\sigma)\big[\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big]\mathbf{p}^\dagger_{\nu_1}(\sigma)\Big). \quad (4.69)\end{aligned}$$

Now, since $\mathcal{P}_{\nu_0}, \mathcal{P}_{\mu_0}$ are both one-dimensional, we can write $\Omega_{\nu_0} = \mathbb{I}_{\mathcal{P}_{\nu_0}}$ and $\Theta^{(\mu_j)}_{\mu_0} = \theta^{(\mu_j)}_{\mu_0}\mathbb{I}_{\mathcal{P}_{\mu_0}}$ such that $\theta^{(\mu_j)}_{\mu_0} \geq 0$. Further, since $\mathcal{P}_{\nu_0} = \mathcal{P}_{\mu_0} \otimes \{|0\rangle\}$, it follows that $\Omega_{\nu_0} = \mathbb{I}_{\mathcal{P}_{\mu_0}} \otimes |0\rangle\langle 0|$. We can therefore deduce that

$$D^{\mu_j}_{\nu_0} = \theta^{(\mu_j)}_{\mu_0}\mathbb{I}_{\mathcal{Q}_{\nu_0}}. \quad (4.70)$$

Next, notice that

$$\frac{2}{3}\sum_{[\sigma]_{\nu_1}} \mathbf{p}_{\nu_1}(\sigma)\big(\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big)\mathbf{p}^\dagger_{\nu_1}(\sigma) = \mathbb{I}_{\mathcal{P}_{\nu_1}} = \big(\mathbb{I}_{\mathcal{P}_{\mu_1}} \otimes |0\rangle\langle 0|\big) \oplus \big(\mathbb{I}_{\mathcal{P}_{\mu_0}} \otimes |1\rangle\langle 1|\big), \quad (4.71)$$

which follows from Schur's lemma, and the $2/3$ coefficient can be confirmed by taking the trace of both sides. Recalling that $\Omega_{\mu_0} = \mathbb{I}_{\mathcal{P}_{\mu_0}}$, it follows that

$$\frac{2}{3}\sum_{[\sigma \in S_3\backslash S_2]_{\nu_1}} \mathbf{p}_{\nu_1}(\sigma)\big(\Omega_{\mu_0} \otimes |1\rangle\langle 1|\big)\mathbf{p}^\dagger_{\nu_1}(\sigma) = \Big(\mathbb{I}_{\mathcal{P}_{\mu_1}} \otimes |0\rangle\langle 0|\Big) \oplus \Big(\frac{1}{3}\mathbb{I}_{\mathcal{P}_{\mu_0}} \otimes |1\rangle\langle 1|\Big). \quad (4.72)$$

We can see explicitly at this stage, that every $\mathcal{P}_{\mu_i}$ component of ξ_{μ_j} is proportional to $\mathbb{I}_{\mathcal{P}_{\mu_i}}$. This means nothing about the order of the first two qubits can be deduced in the first classification without affecting the overall success rate of the second classification[13]. Using the above expression, along with the $\mathcal{L}(\mathcal{Q}_{\nu_1} \otimes \mathcal{P}_{\nu_1})$ terms in Eq. (4.69), we have that

$$\begin{aligned}\mathbb{I}_{\mathcal{Q}_{\nu_1}} \otimes \big[(\Theta^{(\mu_j)}_{\mu_1} \otimes |0\rangle\langle 0|) \oplus (\Theta^{(\mu_j)}_{\mu_0} \otimes |1\rangle\langle 1|)\big] \\ = D^{\mu_j}_{\nu_1} \otimes (\mathbb{I}_{\mathcal{P}_{\mu_0}} \otimes |1\rangle\langle 1|) + \frac{3}{2}D^{\mu_j}_{\nu_1,\tilde{\sigma}} \otimes \Big[\Big(\mathbb{I}_{\mathcal{P}_{\mu_1}} \otimes |0\rangle\langle 0|\Big) \oplus \Big(\frac{1}{3}\mathbb{I}_{\mathcal{P}_{\mu_0}} \otimes |1\rangle\langle 1|\Big)\Big] \quad (4.73)\end{aligned}$$

which implies

$$\mathbb{I}_{\mathcal{Q}_{\nu_1}} \otimes \Theta^{(\mu_j)}_{\mu_1} = \frac{3}{2}D^{\mu_j}_{\nu_1,\tilde{\sigma}} \otimes \mathbb{I}_{\mathcal{P}_{\mu_1}}, \quad (4.74a)$$

$$\mathbb{I}_{\mathcal{Q}_{\nu_1}} \otimes \Theta^{(\mu_j)}_{\mu_0} = \Big(D^{\mu_j}_{\nu_1} + \frac{1}{2}D^{\mu_j}_{\nu_1,\tilde{\sigma}}\Big) \otimes \mathbb{I}_{\mathcal{P}_{\mu_0}}. \quad (4.74b)$$

Taking the partial trace over the $\mathcal{P}_{\mu_1}$ subspace in Eq. (4.74a) tells us that $D^{\mu_j}_{\nu_1,\tilde{\sigma}} = \frac{2}{3}\operatorname{Tr}\big[\Theta^{(\mu_j)}_{\mu_1}\big]\mathbb{I}_{\mathcal{Q}_{\nu_1}}$. Substituting this back into the same equation and taking the partial trace over the $\mathcal{Q}_{\nu_1}$ subspace this time, tells us that $\Theta^{(\mu_j)}_{\mu_1} = \operatorname{Tr}\big[\Theta^{(\mu_j)}_{\mu_1}\big]\mathbb{I}_{\mathcal{P}_{\mu_1}}$. So defining $\theta^{(\mu_j)}_{\mu_1} = \operatorname{Tr}\big[\Theta^{(\mu_j)}_{\mu_1}\big] \geq 0$, it follows that[14] $\Theta^{(\mu_j)}_{\mu_1} = \theta^{(\mu_j)}_{\mu_1}\mathbb{I}_{\mathcal{P}_{\mu_1}}$ and thus $D^{\mu_j}_{\nu_1,\tilde{\sigma}} = \frac{2}{3}\theta^{(\mu_j)}_{\mu_1}\mathbb{I}_{\mathcal{Q}_{\nu_1}}$.

[13] This, however, is a trivial observation in this scenario, since the *two* qubit datasets are invariant under a change of order.

[14] The fact that $\Theta^{(\mu_j)}_{\mu_1}$ has this form may seem like a trivial result since $\dim \mathcal{P}_{\mu_1} = 1$, but this working is included to help us understand what happens when $\dim \mathcal{P}_{\mu_i} \neq 1$, as is generically the case when $n - 1 > 2$.

So combining everything we've found, and substituting $D^{\mu_j}_{\nu_1,\tilde{\sigma}} = \frac{2}{3}\theta^{(\mu_j)}_{\mu_1}\mathbb{I}_{\mathcal{Q}_{\nu_1}}$ into Eq. (4.74b), we finally have

$$D^{\mu_j}_{\nu_0} = \theta^{(\mu_j)}_{\mu_0}\mathbb{I}_{\mathcal{Q}_{\nu_0}}, \tag{4.75a}$$

$$D^{\mu_j}_{\nu_1} = \left[\theta^{(\mu_j)}_{\mu_0} - \frac{1}{3}\theta^{(\mu_j)}_{\mu_1}\right]\mathbb{I}_{\mathcal{Q}_{\nu_1}}, \tag{4.75b}$$

$$D^{\mu_j}_{\nu_1,\tilde{\sigma}} = D^{\mu_j}_{\nu_1,\tilde{\sigma}^2} = \frac{2}{3}\theta^{(\mu_j)}_{\mu_1}\mathbb{I}_{\mathcal{Q}_{\nu_1}}. \tag{4.75c}$$

Notice that this is exactly what we found in Eq. (4.60) when using our old notation. So the final upper bound $P^{\text{1st}}_{\text{succ}} = 7/12$, and corresponding intermediate measurement

$$\xi_{\mu_0} = \frac{2}{3}\mathbb{I}_{\mu_0}, \tag{4.76a}$$

$$\xi_{\mu_1} = \left[\frac{1}{3}\mathbb{I}_{\mu_0}\right] \oplus \mathbb{I}_{\mu_1}, \tag{4.76b}$$

are found in exactly the same way from here on, using $\theta^{(0j)}_1 \to \theta^{(\mu_j)}_{\mu_0},\ \theta^{(0j)}_0 \to \theta^{(\mu_j)}_{\mu_1}$.

4.4.3 Qubit order cannot be deduced in an intermediate classification

In the previous subsection, we saw that requiring the overall final measurement to be the optimal one on three qubits, given by Eq. (3.27) [Eq. (4.23) more generally], constrained our intermediate measurement. We found that the best intermediate measurement that achieves this only told us something about the number of each type of state and nothing about their order. This is an obvious realisation for a classification on two qubits, as the possible states of the system are invariant under permutations of the qubits. However, as we noted in Sec. 4.3 when considering intermediate measurements on a four-qubit dataset, it seems that this phenomenon is true as we generalise to larger quantum datasets. Here, we make steps towards showing that this is the case more generally. That is, in order for our overall classification on n qubits to be given by the optimal measurement found in Eq. (4.23), an intermediate measurement on the first $n-1$ qubits cannot reveal anything about their order. For easy access, we summarise what we show in this subsection as a theorem.

Theorem 4.4.1. *Suppose the optimal binary classification on an undisturbed n-qubit dataset is given by the POVM in Eq. (4.23) (rewritten here):*

$$\Pi^{(n)} = \bigcup_{k=0}^{\lfloor n/2 \rfloor}\left\{\pi_{\nu_k,\sigma} = \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|}\mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \Omega_{\nu_k,\sigma} \ : \ [\sigma]_{\nu_k} \in C_{\nu_k}\right\}, \tag{4.23}$$

and suppose Conjecture 4.A.1 holds. Then, in order for a subesquent classification on the full n-qubit dataset to achieve it's optimal success rate, an intermediate measurement $\{\xi_{\mu_j,\tau}\}$ on the first $n-1$ qubits must have the form

$$\xi_{\mu_j,\tau} = \bigoplus_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \theta^{(\mu_j)}_{\mu_i}\mathbb{I}_{\mu_i}, \tag{4.77}$$

where $0 \leq \theta^{(\mu_j)}_{\mu_i} \in \mathbb{R}$ and $\mathbb{I}_{\mu_i}$ is the identity operator on $\mathcal{Q}_{\mu_i} \otimes \mathcal{P}_{\mu_i}$. In other words, nothing about the order of the first $n-1$ qubits in the dataset can be deduced without negatively impacting a subsequent classification of the full dataset.

Before we show this, let's recap some of things we have found so far. Suppose the optimal measurement on our undisturbed dataset of n qubits is given by $\Pi^{(n)} = \{\pi_{\nu_k,\sigma}\}$, written explicitly in Eq. (4.23), and let $\{\xi_{\mu_j,\tau}\}$ be our intermediate measurement on the first $n-1$ qubits of the dataset. We saw that in order for the overall success rate of the second classification to remain at its optimal value, the conditions found in

Eq. (4.46), rewritten here for convenience, should be satisfied:

$$\xi_{\mu_j,\tau}\otimes\mathbb{1}=\sum_{k=0}^{\lfloor n/2\rfloor}\sum_{[\sigma]_{\nu_k}\in C_{\nu_k}}B^{\mu_j,\tau}_{\nu_k,\sigma}, \tag{4.78a}$$

$$\pi_{\nu_k,\sigma}=\sum_{j=0}^{\lfloor (n-1)/2\rfloor}\sum_{[\tau]_{\mu_j}\in C_{\mu_j}}B^{\mu_j,\tau}_{\nu_k,\sigma}. \tag{4.78b}$$

Let's now steps towards deducing the required form of $\{\xi_{\mu_j,\tau}\}$, with the aim of showing that nothing about the order of the first $n-1$ qubits can be learnt using this intermediate measurement.

4.4.3.1 Intermediate classification can be taken to be SU(2) invariant

We begin by showing that we are free to let each $\xi_{\mu_j,\tau}$ commute with $\mathbf{Q}^{(n-1)}[\mathrm{SU}(2)]$. We achieve this via the following lemma.

Lemma 4.4.1. *The measurement statistics of, and disturbance caused by the POVM $\{\xi_{\mu_j,\tau}\}$ are the same regardless of whether the operators $\xi_{\mu_j,\tau}$ have an SU(2) dependence or not.*

Proof. Suppose for now that $\xi_{\mu_j,\tau}$ does have some SU(2) dependence. That is, there is some $U\in\mathrm{SU}(2)$ such that

$$\xi^U_{\mu_j,\tau}:=\mathbf{Q}^{(n-1)}(U)\xi_{\mu_j,\tau}\mathbf{Q}^{(n-1)^\dagger}(U). \tag{4.79}$$

The SU(2) invariance of $\rho_{\mu_j,\tau}$ means that

$$\begin{aligned}P\big(\xi^U_{\mu_j,\tau}|\rho_{\mu_{j'},\tau'}\big)&=\mathrm{Tr}\left(\xi^U_{\mu_j,\tau}\rho_{\mu_{j'},\tau'}\right)=\mathrm{Tr}\left[\mathbf{Q}^{(n-1)}(U)\xi_{\mu_j,\tau}\mathbf{Q}^{(n-1)^\dagger}(U)\rho_{\mu_{j'},\tau'}\right]\\&=\mathrm{Tr}\left[\xi_{\mu_j,\tau}\mathbf{Q}^{(n-1)}(U^{-1})\rho_{\mu_{j'},\tau'}\mathbf{Q}^{(n-1)^\dagger}(U^{-1})\right]=\mathrm{Tr}(\xi_{\mu_j,\tau}\rho_{\mu_{j'},\tau'})=P(\xi_{\mu_j,\tau}|\rho_{\mu_{j'},\tau'}),\end{aligned} \tag{4.80}$$

for all j,j',τ,τ', from which it follows that the measurement statistics do not have an SU(2) dependence.

To see that $\xi^U_{\mu_j,\tau}$ (minimally) disturbs the measured state in the same way as $\xi_{\mu_j,\tau}$, note that $\xi^U_{\mu_j,\tau}=\mathbf{Q}^{(n-1)}(U)\sqrt{\xi_{\mu_j,\tau}}^\dagger\sqrt{\xi_{\mu_j,\tau}}\mathbf{Q}^{(n-1)^\dagger}(U)$ meaning that $\sqrt{\xi^U_{\mu_j,\tau}}=\sqrt{\xi_{\mu_j,\tau}}\mathbf{Q}^{(n-1)^\dagger}(U)$. Thus,

$$\Big(\sqrt{\xi^U_{\mu_j,\tau}}\otimes\mathbb{1}\Big)\rho_{\nu_k,\sigma}\Big(\sqrt{\xi^U_{\mu_j,\tau}}\otimes\mathbb{1}\Big)^\dagger=\Big(\sqrt{\xi_{\mu_j,\tau}}\otimes\mathbb{1}\Big)\rho_{\nu_k,\sigma}\Big(\sqrt{\xi_{\mu_j,\tau}}\otimes\mathbb{1}\Big)^\dagger. \tag{4.81}$$

□

Due to the property of the disturbance proven here, it follows that the success rate of the second classification, given in Eq. (4.38), is the same regardless of whether the intermediate measurement is invariant under SU(2) or not. Therefore, for every applicable j,τ, we are free to allow

$$\mathbf{Q}^{(n-1)}(U)\xi_{\mu_j,\tau}\mathbf{Q}^{(n-1)^\dagger}(U)=\xi_{\mu_j,\tau},\ \forall U\in\mathrm{SU}(2), \tag{4.82}$$

which, by Schur's Lemma, means we can write

$$\xi_{\mu_j,\tau}=\bigoplus_{i=0}^{\lfloor\frac{n-1}{2}\rfloor}\mathbb{I}_{\mathcal{Q}_{\mu_i}}\otimes\Theta^{(\mu_j,\tau)}_{\mu_i}, \tag{4.83}$$

such that $0\leq\Theta^{(\nu_j,\tau)}_{\mu_i}\in\mathcal{L}(\mathcal{P}_{\mu_i})$ and $\sum_{j,[\tau]_{\nu_j}}\Theta^{(\mu_j,\tau)}_{\mu_i}=\mathbb{I}_{\mathcal{P}_{\mu_i}},\ \forall i$.

Before we move on, in order to be able to impose the conditions in Eq. (4.78), note that

$$\begin{aligned}\xi_{\mu_j,\tau}\otimes\mathbb{1}&=\bigoplus_{i=0}^{\lfloor\frac{n-1}{2}\rfloor}\left(\mathbb{I}_{\mathcal{Q}_{\nu_i}}\otimes\left[\Theta^{(\mu_j,\tau)}_{\mu_i}\otimes|0\rangle\langle 0|\right]\right)\oplus\left(\mathbb{I}_{\mathcal{Q}_{\nu_{i+1}}}\otimes\left[\Theta^{(\mu_j,\tau)}_{\mu_i}\otimes|1\rangle\langle 1|\right]\right),\\&=\bigoplus_{i=0}^{\lfloor\frac{n}{2}\rfloor}\mathbb{I}_{\mathcal{Q}_{\nu_i}}\otimes\left(\left[\Theta^{(\mu_j,\tau)}_{\mu_i}\otimes|0\rangle\langle 0|\right]\oplus\left[\Theta^{(\mu_j,\tau)}_{\mu_{i-1}}\otimes|1\rangle\langle 1|\right]\right),\end{aligned} \tag{4.84}$$

where, if μ_i or μ_{i-1} doesn't exist, we take $\Theta_{\mu_i}^{(\mu_j,\tau)} = 0$ or $\Theta_{\mu_{i-1}}^{(\mu_j,\tau)} = 0$ respectively[15].

4.4.3.2 Intermediate classification is S_n invariant

Now, let's move on and make steps to show that nothing about the order of the first $n-1$ qubits can be deduced in the intermediate classification. First, let's fix $\{\pi_{\nu_k,\sigma}\}$ to be given by the optimal POVM in Eq. (4.23), so that

$$\pi_{\nu_k,\sigma} = \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|}\mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \Omega_{\nu_k,\sigma}, \tag{4.85}$$

for every $k \leq n/2$, $[\sigma]_{\nu_k} \in C_{\nu_k}$. Thinking back to Eq. (4.78), since $\pi_{\nu_k,\sigma} \in \mathcal{L}(\mathcal{Q}_{\nu_k} \otimes \mathcal{P}_{\nu_k})$ and $\Omega_{\nu_k,\sigma}$ is a pure state, it follows that $B_{\nu_k,\sigma}^{\mu_j,\tau} \in \mathcal{L}(\mathcal{Q}_{\nu_k} \otimes \mathcal{P}_{\nu_k})$ and

$$B_{\nu_k,\sigma}^{\mu_j,\tau} = D_{\nu_k,\sigma}^{\mu_j,\tau} \otimes \Omega_{\nu_k,\sigma}, \tag{4.86}$$

such that $0 \leq D_{\nu_k,\sigma}^{\mu_j,\tau} \in \mathcal{L}(\mathcal{Q}_{\nu_k})$ and $\sum_{j,[\tau]_{\mu_j}} D_{\nu_k,\sigma}^{\mu_j,\tau} = \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|}\mathbb{I}_{\mathcal{Q}_{\nu_k}}$. Using all of this, along with Eq. (4.78a) and the orthogonality of the subspaces $\mathcal{L}(\mathcal{Q}_{\nu_k} \otimes \mathcal{P}_{\nu_k})$, it follows that

$$\mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \left(\left[\Theta_{\mu_k}^{(\mu_j,\tau)} \otimes |0\rangle\langle 0|\right] \oplus \left[\Theta_{\mu_{k-1}}^{(\mu_j,\tau)} \otimes |1\rangle\langle 1|\right] \right) = \sum_{[\sigma]_{\nu_k}} D_{\nu_k,\sigma}^{\mu_j,\tau} \otimes \Omega_{\nu_k,\sigma} \tag{4.87}$$

for all $k \leq n/2$. Let's consider a lemma.

Lemma 4.4.2. *Let*

$$\mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \left(\left[\Theta_{\mu_k}^{(\mu_j,\tau)} \otimes |0\rangle\langle 0|\right] \oplus \left[\Theta_{\mu_{k-1}}^{(\mu_j,\tau)} \otimes |1\rangle\langle 1|\right] \right) = \sum_{[\sigma]_{\nu_k}} D_{\nu_k,\sigma}^{\mu_j,\tau} \otimes \Omega_{\nu_k,\sigma}, \tag{4.88}$$

then, if Conjecture 4.A.1 holds, $\Theta_{\mu_k}^{(\mu_j,\tau)} = \theta_{\mu_k}^{(\mu_j,\tau)}\mathbb{I}_{\mathcal{P}_{\mu_k}}$, for all $0 \leq k < n/2$ such that $\theta_{\mu_i}^{(\mu_j,\tau)} := Tr\left[\Theta_{\mu_i}^{(\mu_j,\tau)}\right]/d_{\mathcal{P}_{\mu_i}}$ are positive real numbers.

Proof. We prove this by induction, but before we do, note that, except for when $k = 0$, where $\Omega_{\nu_0,\sigma} \equiv \Omega_{\mu_0} \otimes |0\rangle\langle 0| \equiv \mathbb{I}_{\mathcal{P}_{\mu_0}} \otimes |0\rangle\langle 0|$, we have that $\Omega_{\nu_k} = \Omega_{\mu_{k-1}} \otimes |1\rangle\langle 1|$ [72]. Now, let us first consider $k = 0$. Here, Eq. (4.88) is

$$\mathbb{I}_{\mathcal{Q}_{\nu_0}} \otimes \left[\Theta_{\mu_0}^{(\mu_j,\tau)} \otimes |0\rangle\langle 0|\right] = \sum_{[\sigma]_{\nu_k}} D_{\nu_0,\sigma}^{\mu_j,\tau} \otimes \Omega_{\nu_0,\sigma} \equiv D_{\nu_0,\sigma}^{\mu_j,\tau} \otimes \left[\mathbb{I}_{\mathcal{P}_{\mu_0}} \otimes |0\rangle\langle 0|\right]. \tag{4.89}$$

By tracing out the $\mathcal{P}_{\nu_0}$ component, and defining $\theta_{\mu_0}^{(\mu_j,\tau)} = \mathrm{Tr}\left[\Theta_{\mu_0}^{(\mu_j,\tau)}\right]/d_{\mathcal{P}_{\mu_0}}$, it follows that $D_{\nu_0,\sigma}^{\mu_j,\tau} = \theta_{\mu_0}^{(\mu_j,\tau)}\mathbb{I}_{\mathcal{Q}_{\nu_0}}$, and thus, $\Theta_{\mu_0}^{(\mu_j,\tau)} = \theta_{\mu_0}^{(\mu_j,\tau)}\mathbb{I}_{\mathcal{P}_{\mu_0}}$.

Now assume the lemma is true for arbitrary $k = i-1 > 0$. That is, assume

$$\Theta_{\mu_{i-1}}^{(\mu_j,\tau)} = \theta_{\mu_{i-1}}^{(\mu_j,\tau)}\mathbb{I}_{\mathcal{P}_{\mu_{i-1}}}. \tag{4.90}$$

Therefore, when $k = i$, Eq. (4.88) is

$$\mathbb{I}_{\mathcal{Q}_{\nu_i}} \otimes \left(\left[\Theta_{\mu_i}^{(\mu_j,\tau)} \otimes |0\rangle\langle 0|\right] \oplus \left[\theta_{\mu_{i-1}}^{(\mu_j,\tau)}\mathbb{I}_{\mathcal{P}_{\mu_{i-1}}} \otimes |1\rangle\langle 1|\right] \right) = \sum_{[\sigma]_{\nu_i}} D_{\nu_i,\sigma}^{\mu_j,\tau} \otimes \Omega_{\nu_i,\sigma}. \tag{4.91}$$

Note that the right hand side of this can be rewritten as

$$\begin{aligned}\sum_{[\sigma]_{\nu_i}} D_{\nu_i,\sigma}^{\mu_j,\tau} \otimes \Omega_{\nu_i,\sigma} = &\sum_{[\sigma\in S_{n-1}]_{\nu_i}} D_{\nu_i,\sigma}^{\mu_j,\tau} \otimes \left[\mathbf{p}_{\nu_i}(\sigma)\left(\Omega_{\mu_{i-1}} \otimes |1\rangle\langle 1|\right)\mathbf{p}_{\nu_i}^\dagger(\sigma)\right] \\ &+ \sum_{[\sigma\in S_n\setminus S_{n-1}]_{\nu_i}} D_{\nu_i,\sigma}^{\mu_j,\tau} \otimes \left[\mathbf{p}_{\nu_i}(\sigma)\left(\Omega_{\mu_{i-1}} \otimes |1\rangle\langle 1|\right)\mathbf{p}_{\nu_i}^\dagger(\sigma)\right],\end{aligned} \tag{4.92}$$

[15]For example, when $i = 0$, μ_{i-1} doesn't exist and we take $\Theta_{\mu_{-1}}^{(\mu_j,\tau)} = 0$. Likewise, for even n, where $\nu_{n/2}$ exists but $\mu_{n/2}$ does not, we take $\Theta_{\mu_{n/2}}^{(\mu_j,\tau)} = 0$.

where $[\sigma \in X]_{\nu_i} := \{\sigma' \in S_n \mid \sigma' \sim_{\nu_i} \sigma,\ \sigma \in X \subset S_n\}$ such that $\sim_{\nu_i}$ is the equivalence relation on n-qubit states defined in Def. 4.2.1. Noting that $[\sigma \in S_{n-1}]_{\nu_i}$ only permute the first $n-1$ qubits non-trivially, we can see that the first term on the right hand side is of the correct, block diagonal form of Eq. (4.88):

$$\sum_{[\sigma\in S_{n-1}]_{\nu_i}} D^{\mu_j,\tau}_{\nu_i,\sigma} \otimes \Big[\mathbf{p}_{\nu_i}(\sigma)\big(\Omega_{\mu_{i-1}} \otimes |1\rangle\langle 1|\big)\mathbf{p}^\dagger_{\nu_i}(\sigma)\Big] = \mathbb{I}_{\mathcal{Q}_{\nu_i}} \otimes \Big(\big[\Theta^{(\mu_j,\tau)}_{\mu_{i-1}} - \tilde{\Theta}^{(\mu_j,\tau)}_{\mu_{i-1}}\big] \otimes |1\rangle\langle 1|\Big), \tag{4.93}$$

where $\tilde{\Theta}^{(\mu_j,\tau)}_{\mu_{i-1}}$ is some positive operator satisfying $\Theta^{(\mu_j,\tau)}_{\mu_{i-1}} \geq \tilde{\Theta}^{(\mu_j,\tau)}_{\mu_{i-1}} \geq 0$. The reason as to why the $\mathcal{Q}_{\nu_i}$ component should be proportional to $\mathbb{I}_{\mathcal{Q}_{\nu_i}}$ comes from the fact that the $[\sigma \in S_n \backslash S_{n-1}]_{\nu_i}$ sum in Eq. (4.91) must have a $\mathcal{Q}_{\nu_i}$ component proportional to $\mathbb{I}_{\mathcal{Q}_{\nu_i}}$. This is on account of this sum containing *all* of the $\mathcal{L}\big(\mathcal{P}_{\mu_i} \otimes \{|0\rangle\}\big)$ terms.

The last question we have to answer is what set of matrices $\{D^{\mu_j,\tau}_{\nu_i,\sigma}\}_{[\sigma\in S_n\backslash S_{n-1}]_{\nu_i}}$ allow

$$\begin{aligned} Y^{\mu_j,\tau}_{\nu_i,\tilde{\sigma}} := \sum_{[\sigma\in S_n\backslash S_{n-1}]_{\nu_i}} D^{\mu_j,\tau}_{\nu_i,\sigma} \otimes \Big[\mathbf{p}_{\nu_i}(\sigma)\big(\Omega_{\mu_{i-1}} \otimes |1\rangle\langle 1|\big)\mathbf{p}^\dagger_{\nu_i}(\sigma)\Big] \\ = \mathbb{I}_{\mathcal{Q}_{\nu_i}} \otimes \left(\Big[\Theta^{(\mu_j,\tau)}_{\mu_i} \otimes |0\rangle\langle 0|\Big] \oplus \Big[\tilde{\Theta}^{(\mu_j,\tau)}_{\mu_{i-1}} \otimes |1\rangle\langle 1|\Big]\right) \end{aligned} \tag{4.94}$$

to be true? We conjecture that the elements in $\{D^{\mu_j,\tau}_{\nu_i,\sigma}\}_{[\sigma\in S_n\backslash S_{n-1}]_{\nu_i}}$ must all be equal[16]. Let's write the representative of this set as $D^{\mu_j,\tau}_{\nu_i,\tilde{\sigma}}$, where $\tilde{\sigma} = (12\cdots n) \in S_n \backslash S_{n-1}$. With this in mind, we can rewrite $Y^{\mu_j,\tau}_{\nu_i,\tilde{\sigma}}$ as

$$Y^{\mu_j,\tau}_{\nu_i,\tilde{\sigma}} = D^{\mu_j,\tau}_{\nu_i,\tilde{\sigma}} \otimes \left[\sum_{[\sigma\in S_n\backslash S_{n-1}]_{\nu_i}} \mathbf{p}_{\nu_i}(\sigma)\big(\Omega_{\mu_{i-1}} \otimes |1\rangle\langle 1|\big)\mathbf{p}^\dagger_{\nu_i}(\sigma)\right], \tag{4.95}$$

from which we can see that $Y^{\mu_j,\tau}_{\nu_i,\tilde{\sigma}}$ commutes with $\mathbf{P}^{(n-1)}(S_{n-1}) \otimes \mathbb{1}$. It therefore follows, via Schur's lemma, that

$$Y^{\mu_j,\tau}_{\nu_i,\tilde{\sigma}} = D^{\mu_j,\tau}_{\nu_i,\tilde{\sigma}} \otimes \Big(\big[a\mathbb{I}_{\mathcal{P}_{\mu_i}} \otimes |0\rangle\langle 0|\big] \oplus \big[b\mathbb{I}_{\mathcal{P}_{\mu_{i-1}}} \otimes |1\rangle\langle 1|\big]\Big), \tag{4.96}$$

where a, b are some positive real numbers.

Although not necessary for this argument, the explicit values of a and b will be used later on, so we derive them here. To do so, note that

$$\frac{d_{\mathcal{P}_{\nu_i}}}{|C_{\nu_i}|}\sum_{[\sigma]_{\nu_i}} \mathbf{p}_{\nu_i}(\sigma)\big(\Omega_{\mu_{i-1}} \otimes |1\rangle\langle 1|\big)\mathbf{p}^\dagger_{\nu_i}(\sigma) = \mathbb{I}_{\mathcal{P}_{\nu_i}} \equiv \big(\mathbb{I}_{\mathcal{P}_{\mu_i}} \otimes |0\rangle\langle 0|\big) \oplus \big(\mathbb{I}_{\mathcal{P}_{\mu_{i-1}}} \otimes |1\rangle\langle 1|\big), \tag{4.97}$$

as was deduced in Sec. 4.2.2. Using Schur's lemma, note also that

$$\frac{d_{\mathcal{P}_{\nu_i}}}{|C_{\nu_i}|}\sum_{[\sigma\in S_{n-1}]_{\nu_i}} \mathbf{p}_{\nu_i}(\sigma)\big(\Omega_{\mu_{i-1}} \otimes |1\rangle\langle 1|\big)\mathbf{p}^\dagger_{\nu_i}(\sigma) = c_i\big(\mathbb{I}_{\mathcal{P}_{\mu_{i-1}}} \otimes |1\rangle\langle 1|\big), \tag{4.98}$$

since the left hand side is invariant under S_{n-1}. To find c_i, first note that, when $i = 0$, $\Omega_{\mu_{i-1}} = 0$ and $\mathbb{I}_{\mathcal{P}_{\mu_{i-1}}} = 0$, so we define $c_0 = 0$. Next, we can see that the left hand side has $\binom{n-1}{i-1} = \frac{(n-1)!}{(n-i)!(i-1)!}$ terms in the sum. This can be understood be recalling that the state $\rho_{\mu_{i-1}}$ has $i-1$ ones which have $n-1$ positions to choose between. The fact that there is an nth qubit means that each of these choices is distinct[17].

[16] We rewrite this conjecture in Appendix 4.A to allow for easy access to this open problem.

[17] This differs slightly from how we count permutations when considering the full dataset. For example, suppose we have a situation in which we're looking at the first four qubits of a dataset, two of which are labelled by ones. If these qubits constitute the full dataset, permuting the first four qubits results in $\frac{1}{2}\binom{4}{2} = 3$ states overall: $\rho_{0011} = \rho_{1100}$, $\rho_{0101} = \rho_{1010}$, $\rho_{1001} = \rho_{0110}$. However, if they are part of a five qubit dataset, permuting the first four qubits results in $\binom{4}{2} = 6$ states overall: $\rho_{0011b}, \rho_{1100b}, \rho_{0101b}, \rho_{1010b}, \rho_{1001b}, \rho_{0110b}$, where $b \in \{0, 1\}$.

This is because $\mathbf{p}_{\nu_i}(\sigma)$ only acts on the first $n-1$ qubits for $[\sigma \in S_{n-1}]_{\nu_i}$ and therefore, $\mathbf{p}_{\nu_i}(\sigma) \equiv [\mathbf{p}_{\mu_{i-1}}(\sigma) \otimes |1\rangle\langle 1|] \oplus [\mathbf{p}_{\mu_i}(\sigma) \otimes |0\rangle\langle 0|]$ for $[\sigma \in S_{n-1}]_{\nu_i}$. So, with this in mind, we can take the trace to deduce that

$$c_i = \begin{cases} 0, & i = 0, \\ \frac{d_{\mathcal{P}_{\nu_i}}}{|C_{\nu_i}| d_{\mathcal{P}_{\mu_{i-1}}}} \frac{(n-1)!}{(n-i)!(i-1)!}, & i > 0. \end{cases} \tag{4.99}$$

Using this and rearranging Eq. (4.97), we can rewrite $Y_{\nu_i}^{\mu_j,\tau}$ more concretely as

$$Y_{\nu_i,\tilde{\sigma}}^{\mu_j,\tau} = D_{\nu_i,\tilde{\sigma}}^{\mu_j,\tau} \otimes \left[\left(\frac{|C_{\nu_i}|}{d_{\mathcal{P}_{\nu_i}}} \mathbb{I}_{\mathcal{P}_{\mu_i}} \otimes |0\rangle\langle 0| \right) \oplus \left(\left[\frac{|C_{\nu_i}|}{d_{\mathcal{P}_{\nu_i}}} - \frac{(n-1)!}{d_{\mathcal{P}_{\mu_{i-1}}}(n-i)!(i-1)!} \right] \mathbb{I}_{\mathcal{P}_{\mu_{i-1}}} \otimes |1\rangle\langle 1| \right) \right], \tag{4.100}$$

where, as discussed for similar operators, $\mathbb{I}_{\mathcal{P}_{\mu_{i-1}}} = 0$ when $i = 0$.

So, substituting what we have found back into Eq. (4.91), and focusing on the $\mathbb{I}_{\mathcal{Q}_{\nu_i}} \otimes \left[\Theta_{\mu_i}^{(\mu_j,\tau)} \otimes |0\rangle\langle 0| \right]$ component, we see that

$$\mathbb{I}_{\mathcal{Q}_{\nu_i}} \otimes \left[\Theta_{\mu_i}^{(\mu_j,\tau)} \otimes |0\rangle\langle 0| \right] = D_{\nu_i,\tilde{\sigma}}^{\mu_j,\tau} \otimes \left[\frac{|C_{\nu_i}|}{d_{\mathcal{P}_{\nu_i}}} \mathbb{I}_{\mathcal{P}_{\mu_i}} \otimes |0\rangle\langle 0| \right]. \tag{4.101}$$

Similarly to as we did in the $k = 0$ case, tracing out the $\mathcal{P}_{\nu_i}$ component, and defining $d_{\mathcal{P}_{\mu_i}} \theta_{\mu_i}^{(\mu_j,\tau)} = \mathrm{Tr}\left[\Theta_{\mu_i}^{(\mu_j,\tau)} \right]$ results in

$$D_{\nu_i,\tilde{\sigma}}^{\mu_j,\tau} = \frac{d_{\mathcal{P}_{\nu_i}}}{|C_{\nu_i}|} \theta_{\mu_i}^{(\mu_j,\tau)} \mathbb{I}_{\mathcal{Q}_{\nu_i}}, \tag{4.102}$$

and therefore

$$\Theta_{\mu_i}^{(\mu_j,\tau)} = \theta_{\mu_i}^{(\mu_j,\tau)} \mathbb{I}_{\mathcal{P}_{\mu_i}}, \tag{4.103}$$

as required. This concludes our argument (pending a proof of Conjecture 4.A.1). □

If true, what we have deduced from this working is that

$$\xi_{\mu_j,\tau} = \bigoplus_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \theta_{\mu_i}^{(\mu_j,\tau)} \mathbb{I}_{\mu_i}, \tag{4.104}$$

where $\mathbb{I}_{\mu_i}$ is the identity on $\mathcal{L}(\mathcal{Q}_{\mu_i} \otimes \mathcal{P}_{\mu_i})$ and $\theta_{\mu_i}^{(\mu_j,\tau)} \geq 0$. This means that $\xi_{\mu_j,\tau}$ are invariant under S_{n-1} and thus, cannot tell us anything about the order of the qubits in the quantum dataset, only something about how many of each type there are. Further, since $P(\xi_{\mu_j,\tau}|\rho_{\mu_{j'},\tau'}) = P(\xi_{\mu_j,\tau}|\rho_{\mu_{j'},\tau''}),\ \forall \tau', \tau''$, we are free to weight $\theta_{\mu_i}^{(\mu_j,\tau)}$ so that, for each choice of i, j, they are equal:

$$\xi_{\mu_j,\tau} = \bigoplus_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \theta_{\mu_i}^{(\mu_j)} \mathbb{I}_{\mu_i}. \tag{4.105}$$

Intermediate classification on $n-m$ qubits

Can we say anything about what one can learn in an intermediate classification on the first $n-m$ qubits (such that $m > 1$) of an n-qubit dataset? Lemma 4.4.2 implies that neither the order nor the number of each type of state can be deduced if we want to preserve the optimal success rate of the final n-qubit classification. To see this, consider the example of $n = 4$, with possible states

$$R^{(4)} = \{\rho_{0000}, \rho_{0001}, \rho_{0010}, \rho_{0100}, \rho_{0111}, \rho_{0011}, \rho_{0101}, \rho_{0110}\}. \tag{4.106}$$

Let

$$\Xi^{(2)} = \{\xi_{00}, \xi_{01}\} \tag{4.107}$$

be a POVM that distinguishes $R^{(2)} = \{\rho_{00}, \rho_{01}\}$ with a higher success rate than a guess. Zooming out to the full data set, ξ_{00} is associated with the states $\rho_{0000}, \rho_{0001}, \rho_{0010}, \rho_{0011}$, whereas ξ_{01} is associated with $\rho_{0100}, \rho_{0111}, \rho_{0101}, \rho_{0110}$. Now, we can think of $\Xi^{(2)}$ instead as a three-qubit measurement

$$\Xi^{(3)} = \{\xi_{00} \otimes \mathbb{1}, \xi_{01} \otimes \mathbb{1}\}. \tag{4.108}$$

But notice that this measurement distinguishes ρ_{0010} from ρ_{0100}, ρ_{0111}, and ρ_{0011} from ρ_{0101}, ρ_{0110}, or in other words, it distinguishes ρ_{001} from ρ_{010}, ρ_{011}. Thus, $\Xi^{(3)}$ says something about the order of the first three qubits, which isn't allowed according to Lemma 4.4.2.

More generally, let $m > 1$ and $\lambda_k = (n-m-k, k)$ be a partition of $n-m$. Suppose we have a POVM

$$\Xi^{(n-m)} = \{\xi_{\lambda_k,\tau} \mid 0 \leq k \leq (n-m)/2, [\tau]_{\lambda_k} \in C_{\lambda_k}\}, \tag{4.109}$$

with elements satisfying $\xi_{\lambda_k,\tau} = \xi_{\lambda_k}\ \forall k \leq (n-m)/2,\ \tau \in S_{n-m}$, that distinguishes the states in the set

$$R^{(n-m)} = \{\rho_{\lambda_k,\tau} \mid 0 \leq k \leq (n-m)/2, [\tau]_{\lambda_k} \in C_{\lambda_k}\} \tag{4.110}$$

non-trivially. Then, although

$$\mathrm{Tr}\left[\xi_{\lambda_k,\tau}\rho_{\lambda_j,\tau'}\right] = \mathrm{Tr}\left[\xi_{\lambda_k}\rho_{\lambda_j,\tau}\right] \tag{4.111}$$

for all j, k, τ, τ', and thus tells us nothing about the order of the first $n-m$ qubits, since $\Xi^{(n-m)}$ is a non-trivial measurement, there must exist some k, j', satisfying $k \neq j'$, such that

$$\mathrm{Tr}\left[\xi_{\lambda_k}\rho_{\lambda_k}\right] \neq \mathrm{Tr}\left[\xi_{\lambda_k}\rho_{\lambda_{j'}}\right]. \tag{4.112}$$

Assuming $k < j'$ for the remainder of this discussion (since an analogous argument holds for $j' < k$), it follows that there exists some j, satisfying $k \leq j \leq j'-1$, such that

$$\mathrm{Tr}\left[\xi_{\lambda_k}\rho_{\lambda_j}\right] \neq \mathrm{Tr}\left[\xi_{\lambda_k}\rho_{\lambda_{j+1}}\right]. \tag{4.113}$$

Now, we can think of $\Xi^{(n-m)}$ as an $(n-1)$-qubit measurement:

$$\Xi^{(n-1)} = \left\{\tilde{\xi}_{\lambda_k,\tau} = \xi_{\lambda_k,\tau} \otimes \mathbb{1}^{\otimes m-1} \mid \xi_{\lambda_k,\tau} \in \Xi^{(n-m)}\right\}. \tag{4.114}$$

Let's consider the $(n-1)$-qubit state $\rho_{\mu_{m+j}}$ whose first $n-m-j-1$ qubits are all labelled by zero, and whose last $m+j$ qubits are labelled by ones[18]. Defining the 2-cycle $\tilde{\tau} := \big([n-1][n-m-j-1]\big) \in S_{n-1}$, which swaps the $(n-1)$th qubit with the $(n-m-j-1)$th qubit. Since the $(n-1)$th qubit of $\rho_{\mu_{m+1}}$ is labelled by a one, whereas the $(n-m-j-1)$th qubit of this state is labelled by a zero, it follows that

$$\mathrm{Tr}\left[\xi_{\lambda_k}\rho_{\lambda_j}\right] = \mathrm{Tr}\left[\tilde{\xi}_{\mu_{m+k}}\rho_{\mu_{m+j}}\right], \tag{4.115a}$$

$$\mathrm{Tr}\left[\xi_{\lambda_k}\rho_{\lambda_{j+1}}\right] = \mathrm{Tr}\left[\tilde{\xi}_{\mu_{m+k}}\rho_{\mu_{m+j},\tilde{\tau}}\right]. \tag{4.115b}$$

Therefore, by Eq. (4.113),

$$\mathrm{Tr}\left[\tilde{\xi}_{\mu_{m+k}}\rho_{\mu_{m+j}}\right] \neq \mathrm{Tr}\left[\tilde{\xi}_{\mu_{m+k}}\rho_{\mu_{m+j},\tilde{\tau}}\right], \tag{4.116}$$

which, by Lemma 4.4.2 is not allowed as this would mean something about the order of the first $n-1$ qubits can be learned. So, Lemma 4.4.2 implies that a non-trivial intermediate measurement on the first $n-m$ qubits (for $m > 1$) will always impact one's ability subsequently classify the whole n-qubit dataset.

4.5 Constructing an intermediate measurement

Let us now go a little further and deduce the constraints that the $\theta^{(\mu_j)}_{\mu_i}$ of Eq. (4.105) are subject to so that Eq. (4.78) is valid. Using what we've found so far,

$$\begin{aligned}\mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \left(\left[\theta^{(\mu_j)}_{\mu_k}\mathbb{I}_{\mathcal{P}_{\mu_k}} \otimes |0\rangle\langle 0|\right] \oplus \left[\theta^{(\mu_j)}_{\mu_{k-1}}\mathbb{I}_{\mathcal{P}_{\mu_{k-1}}} \otimes |1\rangle\langle 1|\right]\right) &= \sum_{[\sigma \in S_{n-1}]_{\nu_k}} D^{\mu_j,\tau}_{\nu_k,\sigma} \otimes \Omega_{\nu_k,\sigma} \\ + \theta^{(\mu_j)}_{\mu_k}\mathbb{I}_{\mathcal{Q}_{\nu_k}} \otimes \left[\left(\mathbb{I}_{\mathcal{P}_{\mu_k}} \otimes |0\rangle\langle 0|\right) \oplus \left(\left[1 - \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|}\frac{(n-1)!}{d_{\mathcal{P}_{\mu_{k-1}}}(n-k)!(k-1)!}\right]\mathbb{I}_{\mathcal{P}_{\mu_{k-1}}} \otimes |1\rangle\langle 1|\right)\right],\end{aligned} \tag{4.117}$$

[18] We are using the same definition of μ_i as before: $\mu_i = (n-1-i, i)$.

which means that

$$\sum_{[\sigma\in S_{n-1}]_{\nu_k}} D^{\mu_j,\tau}_{\nu_k,\sigma}\otimes\Omega_{\nu_k,\sigma} = \left(\theta^{(\mu_j)}_{\mu_{k-1}} - \left[1-\frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|}\frac{(n-1)!}{d_{\mathcal{P}_{\mu_{k-1}}}(n-k)!(k-1)!}\right]\theta^{(\mu_j)}_{\mu_k}\right)\mathbb{I}_{\mathcal{Q}_{\nu_k}}\otimes\left(\mathbb{I}_{\mathcal{P}_{\mu_{k-1}}}\otimes|1\rangle\langle 1|\right). \quad (4.118)$$

We conjecture[19] that for this to be true, $D^{\mu_j,\tau}_{\nu_k,\sigma} = D^{\mu_j,\tau}_{\nu_k,\sigma'},\ \forall\sigma,\sigma'\in S_{n-1}$. Tracing out over $\mathcal{P}_{\nu_k}$ then gives us an expression for $D^{\mu_j,\tau}_{\nu_k,\sigma}$, which, since $\mathbb{I}_{\mathcal{P}_{\mu_{k-1}}} = 0$ when $k=0$, has separate expressions for $k=0$ and $k>0$. Including what we found earlier with regards to $D^{\mu_j,\tau}_{\nu_k,\tilde{\sigma}}$ for completeness, we have that

$$D^{\mu_j,\tau}_{\nu_k,\sigma} = \begin{cases} 0, & k=0, \\ \left(\frac{d_{\mathcal{P}_{\mu_{k-1}}}(n-k)!(k-1)!}{(n-1)!}\left[\theta^{(\mu_j)}_{\mu_{k-1}} - \theta^{(\mu_j)}_{\mu_k}\right] + \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\mu_k}|}\theta^{(\mu_j)}_{\mu_k}\right)\mathbb{I}_{\mathcal{Q}_{\mu_k}}, & k>0, \end{cases} \quad (4.119a)$$

$$D^{\mu_j,\tau}_{\nu_k,\tilde{\sigma}} = \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|}\theta^{(\mu_j)}_{\mu_k}\mathbb{I}_{\mathcal{Q}_{\nu_k}}. \quad (4.119b)$$

Now, recall that when we introduced $D^{\mu_j,\tau}_{\nu_k,\sigma}$ in Eq. (4.86), we noted the following were required:

$$D^{\mu_j,\tau}_{\nu_k,\sigma} \geq 0, \quad (4.120a)$$

$$\sum_j\sum_{[\tau]_{\mu_j}} D^{\mu_j,\tau}_{\nu_k,\sigma} = \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|}\mathbb{I}_{\mathcal{Q}_{\nu_k}}, \quad (4.120b)$$

for all $k \leq n/2$. This second condition implies that $D^{\mu_j,\tau}_{\nu_k,\sigma} \leq \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|}\mathbb{I}_{\mathcal{Q}_{\nu_k}}$, which means that $\theta^{(\mu_j)}_{\mu_k} \leq 1$ (unless $\sigma\in S_{n-1},\ k=0$, in which case $D^{\mu_j,\tau}_{\mu_k,\sigma}=0,\ \forall j,\tau.$). Note, however, that the condition $\theta^{(\mu_j)}_{\nu_k}\leq 1$ is superseded by the requirement that $\sum_j\sum_{[\tau]_{\mu_j}}\theta^{(\mu_j)}_{\mu_k} = 1$ for all k, which means that $\theta^{(\mu_j)}_{\mu_k} \leq 1/|C_{\mu_j}|$.

Let's summarise what we have found. The final form of the intermediate measurement is

$$\xi_{\mu_j,\tau} = \bigoplus_{k=0}^{\lfloor\frac{n-1}{2}\rfloor}\theta^{(\mu_j)}_{\mu_k}\mathbb{I}_{\mu_k}, \quad (4.121)$$

subject to $\sum_j |C_{\mu_j}|\,\theta^{(\mu_j)}_{\mu_k} = 1,\ \theta^{(\mu_j)}_{\mu_k}\geq 0,\ \forall\, 0\leq j,k<n/2$. And the bounds that the $\theta^{(\mu_j)}_{\mu_k}$ reside within are dictated by

$$0 \leq \frac{d_{\mathcal{P}_{\mu_{k-1}}}(n-k)!(k-1)!}{(n-1)!}\left[\theta^{(\mu_j)}_{\mu_{k-1}} - \theta^{(\mu_j)}_{\mu_k}\right] + \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|}\theta^{(\mu_j)}_{\mu_k} \leq \frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|},\ \ \forall\, 0<k<\frac{n}{2}, \quad (4.122a)$$

$$0 \leq \theta^{(\mu_j)}_{\mu_k} \leq \frac{1}{|C_{\mu_j}|},\ \ \forall\, 0\leq k<\frac{n}{2}, \quad (4.122b)$$

for any $0\leq j\leq n/2$. Finally, to complete this discussion, due to the non-existence of μ_k when $k<0$ or $k\geq n/2$, we should reiterate that, for all j,

$$\theta^{(\mu_j)}_{\mu_k} = 0,\ \forall\, k<0 \text{ or } k\geq\frac{n}{2}. \quad (4.123)$$

4.5.1 A lower bound

Let's now derive an analytical lower bound $P^{\text{1st}}_{\text{lower}}$ for the optimal success rate $P^{\text{1st}}_{\text{succ}}$ of the first classification. To do this, we constrain $\{\xi_{\mu_j,\tau}\}$ to be made of operators of the form

$$\xi_{\mu_j,\tau} = \alpha_j\mathbb{I}_{\mu_j} + \beta_j\mathbb{I}, \quad (4.124)$$

[19] Rewritten as Conjecture 4.A.2 in Appendix 4.A for convenience.

for all $[\tau]_{\mu_j} \in C_{\mu_j}$, where $\mathbb{I}_{\mu_j} = \mathbb{I}_{\mathcal{Q}_{\mu_j}} \otimes \mathbb{I}_{\mathcal{P}_{\mu_j}}$ as always, and $\mathbb{I}$ is the identity on the entire $(n-1)$-qubit Hilbert space $\mathcal{H}^{(n-1)}$. In order for this to be a valid POVM, positivity and completeness are required: for positivity, $\alpha_j + \beta_j, \beta_j \geq 0$. And for completeness, after some algebra, we obtain the following conditions:

$$\alpha_j = \frac{1}{|C_{\mu_j}|}\left(1 - \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} |C_{\mu_i}|\beta_i\right) \tag{4.125a}$$

$$\alpha_{j'} = \frac{|C_{\mu_j}|}{|C_{\mu_{j'}}|}\alpha_j, \tag{4.125b}$$

where the second follows from the first.

Now, using $\rho_{\mu_j,\tau}$ given in Eq. (4.35), along with the fact that $\mathrm{Tr}\left[\xi_{\mu_j,\tau}\rho_{\mu_j,\tau}\right] = \mathrm{Tr}\left[\xi_{\mu_j}\rho_{\mu_j}\right]$, $\forall\tau$, after some algebra,

$$\begin{aligned} P^{\mathrm{1st}}_{\mathrm{lower}} &= \frac{1}{2^{n-2}} \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{[\tau]_{\mu_j} \in C_{\mu_j}} \mathrm{Tr}\left[\xi_{\mu_j,\tau}\rho_{\mu_j,\tau}\right] \\ &= 2^{2-n} \sum_j \sum_{[\tau]_{\mu_j}} \left[\beta_j |C_{\mu_j}| + \alpha_j |C_{\mu_j}| \frac{n-2j}{(n-j)(j+1)}\right]. \end{aligned} \tag{4.126}$$

Looking back to the conditions in Eq. (4.125), note that $\sum_j \beta_j |C_{\mu_j}| = 1 - \alpha_0 |C_{\mu_0}|$, and $\alpha_0 |C_{\mu_0}| = \alpha_j |C_{\mu_j}|$, $\forall j$. Therefore, using $|C_{\mu_0}| = 1$, we have that

$$P^{\mathrm{1st}}_{\mathrm{lower}} = 2^{2-n}\left(1 - \alpha_0\left[1 - \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \frac{n-2j}{(n-j)(j+1)}\right]\right). \tag{4.127}$$

Since the sum in the above expression is greater than 1 for $n > 2$ (an assumption on n made at the start of Sec. 4.4.1), and because $P^{\mathrm{1st}}_{\mathrm{lower}}$ is linear with respect to α_0, we can see that maximising $P^{\mathrm{1st}}_{\mathrm{lower}}$ is done by maximising α_0. To do this, we look to our bounds: Eq. (4.122).

First, note that $\xi_{\mu_j,\tau}$ in Eq. (4.124) relate to the general operators in Eq. (4.121) [Eq. (4.105)] via the following:

$$\theta^{(\mu_j)}_{\mu_{i=j}} = \alpha_j + \beta_j, \tag{4.128a}$$

$$\theta^{(\mu_j)}_{\mu_{i\neq j}} = \beta_j. \tag{4.128b}$$

In particular, since we are interested in maximising α_0, we focus on $\theta^{(\mu_0)}_{\mu_i}$. Recalling that our conditions Eq. (4.122a,b), tailored to this situation, depend on both $\theta^{(\mu_0)}_{\mu_k}$ and $\theta^{(\mu_0)}_{\mu_{k-1}}$ means that we must look at the $k = 0, 1$ cases. If we were to consider $k \geq 2$ (if such ks exist), $\theta^{(\mu_0)}_{\mu_k} = \theta^{(\mu_0)}_{\mu_{k-1}} = \beta_0$ meaning that Eq. (4.122a) is superseded by Eq. (4.122b), and thus, no extra constraints on α_0 are found. First, for $k = 0$, note that Eq. (4.122a) does not apply (for reasons stemming from μ_{k-1} not existing here), and so all we find in this case comes from Eq. (4.122b): $0 \leq \alpha_0 + \beta_0 \leq 1/|C_{\mu_0}|$. Second, when $k = 1$, we find that

$$0 \leq \alpha_0 \frac{d_{\mathcal{P}_{\mu_0}}(n-1)!(1-1)!}{(n-1)!} + \beta_0 \frac{d_{\mathcal{P}_{\nu_1}}}{|C_{\nu_1}|} \leq \frac{d_{\mathcal{P}_{\nu_1}}}{|C_{\nu_1}|}, \tag{4.129}$$

and finally, due to the positivity of $\xi_{\mu_0,\tau}$, we saw earlier that $\beta_0 \geq 0$.

All together, we have found that

$$0 \leq \alpha_0 + \beta_0 \leq \frac{1}{|C_{\mu_0}|}, \tag{4.130a}$$

$$0 \leq \alpha_0 d_{\mathcal{P}_{\mu_0}} + \beta_0 \frac{d_{\mathcal{P}_{\nu_1}}}{|C_{\nu_1}|} \leq \frac{d_{\mathcal{P}_{\nu_1}}}{|C_{\nu_1}|}, \tag{4.130b}$$

$$0 \leq \beta_0. \tag{4.130c}$$

$n-1$	$P^{\text{1st}}_{\text{lower}}$	$P^{\text{1st}}_{\text{optimal}}$	$P^{\text{1st}}_{\text{guess}}$
2	58.33%	62.5%	50%
3	31.25%	41.67%	25%
4	17.36%	29.34%	12.5%

Table 4.3: Success rates of an intermediate measurement on an $(n-1)$-qubit dataset corresponding to the lower bound $P^{\text{1st}}_{\text{lower}}$ derived in Eq. (4.133). Also included is the success rate $P^{\text{1st}}_{\text{optimal}}$ of the optimal measurement on $n-1$ qubits, as well as that of a guess $P^{\text{1st}}_{\text{guess}}$, again on $n-1$ qubits.

So, to make α_0 as large as possible, we should first minimise β_0, letting $\beta_0 = 0$. With that, in order to satisfy all of the above conditions,

$$\alpha_0 \leq \min\left\{\frac{d_{\mathcal{P}_{\nu_1}}}{|C_{\nu_1}|}, 1\right\}, \tag{4.131}$$

where we have used $d_{\mathcal{P}_{\mu_0}} = 1$. Noting that $|C_{\nu_1}| = \binom{n}{1} = n$ when $n > 2$, and using Eq. (2.141) for the dimension $d_{\mathcal{P}_{\nu_1}}$, it follows that $\frac{d_{\mathcal{P}_{\nu_1}}}{|C_{\nu_1}|} = \frac{n-1}{n}$ which is less than 1. We therefore have that

$$\alpha_0 \leq \frac{n-1}{n}, \tag{4.132}$$

and thus, the best value of $P^{\text{1st}}_{\text{lower}}$, achievable with the form of intermediate measurement given in Eq. (4.124) is

$$P^{\text{1st}}_{\text{lower}} = 2^{2-n}\left(1 - \frac{n-1}{n}\left[1 - \sum_{j=0}^{\lfloor\frac{n-1}{2}\rfloor}\frac{n-2j}{(n-j)(j+1)}\right]\right). \tag{4.133}$$

In Table 4.3 and Figure 4.4 we provide some examples to see how this strategy compares to that of a guess as well the corresponding optimal strategy.

4.5.2 An algorithm for an improved intermediate measurement

The previous subsection proved that an intermediate measurement could be constructed that would, on the one hand, provide us with more information about an $(n-1)$-qubit subset than a blind guess, whilst, on the other hand, allow for a subsequent, optimal classification on the entire n-qubit dataset to be achieved. But, in order to do so, we restricted the vast majority of the POVM elements' [Eq. (4.124)] degrees of freedom. This prompts the question that is the subject of this subsection: can we do better?

It turns out that we can. Having said, this, the method used does not allow us to write down a closed form analytic equation for the success rate for arbitrary n. Equation (4.122a) hints at why this is the case: namely, the weights of adjacent invariant subspaces are related, recursively, to one another. It therefore seems that there is no closed form relating $\theta^{(\mu_j)}_{\mu_k}, \theta^{(\mu_{j'})}_{\mu_{k'}}$ for arbitrary k, k', j, j'. We can, however, write down an algorithm to construct, what we hypothesise, is the optimal intermediate measurement that preserves the optimal n-qubit POVM.

The construction algorithm we propose is motivated by an optimal measurement that distinguishes datasets purely based on the number of each data type, and not their order. Such an optimal measurement can be described with the POVM elements

$$\hat{\xi}_{\mu_j,\tau} = \frac{1}{|C_{\mu_j}|}\mathbb{I}_{\mu_j}, \tag{4.134}$$

which, when compared to Eq. (4.105) corresponds to maximising $\theta^{(\mu_j)}_{\mu_j}$ and minimising $\theta^{(\mu_j)}_{\mu_{k\neq j}}$[20]. Note that, although these operators are oblivious to the order of the qubits in the dataset, due to how the problem has

[20]This minimisation, when considering $\{\hat{\xi}_{\mu_j,\tau}\}$ as a standalone measurement, corresponds to putting $\theta^{(\mu_j)}_{\mu_{k\neq j}} = 0$, since the only lower bound for $\theta^{(\mu_j)}_{\mu_i}$ corresponds to the positivity of $\hat{\xi}_{\mu_j,\tau}$: $\theta^{(\mu_j)}_{\mu_i} \geq 0,\ \forall i, j$.

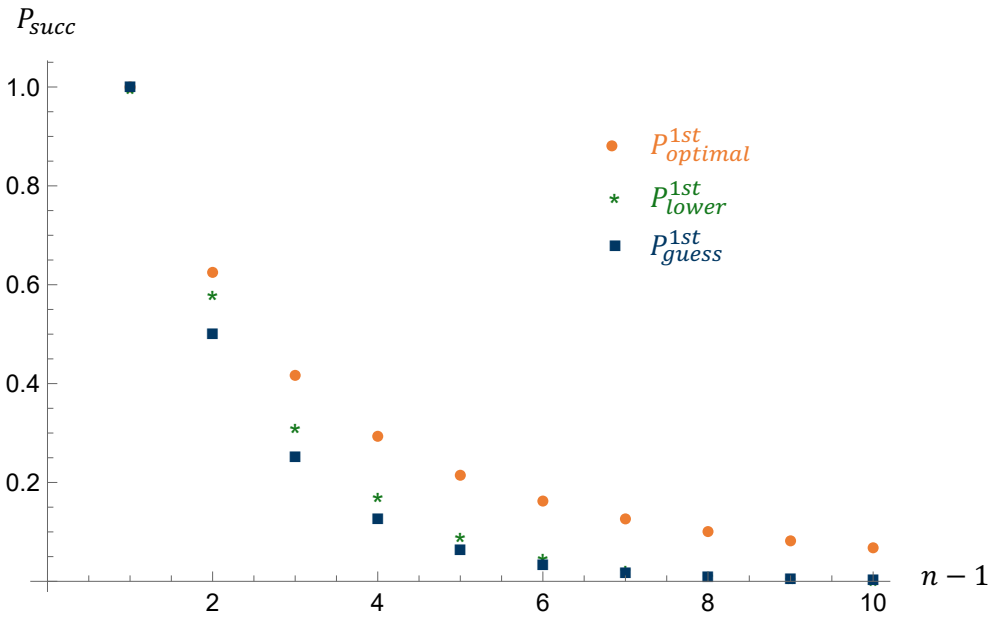

Figure 4.4: Plot showing how the success rate P_{succ} of an unsupervised binary classification on an the first $n-1$ qubits of an n-qubit dataset varies with n. The orange circles correspond to the optimal success rate $P^{\text{1st}}_{\text{optimal}}$ on these first $n-1$ qubits, the green stars to the success rate $P^{\text{1st}}_{\text{lower}}$ of our "lower bound" measurement, and the blue squares correspond to the success rate of a guess $P^{\text{1st}}_{\text{guess}}(n-1) = 2^{2-n}$.

been formulated (i.e. requiring a measurement outcome for each possible dataset), following their optimal strategy for figuring out how many zeros and ones there are, they make a random guess with regards to the order of these zeros and ones. Now, we have the added task of ensuring that our measurement on $n-1$ qubits doesn't stop us from doing the best we can in classifying n qubits. As we saw, this meant that the coefficients of our $(n-1)$-qubit measurement should be related to one another via Eq. (4.122). So, our strategy for constructing our intermediate measurement can be summarised by the following goal: maximising $\theta^{(\mu_j)}_{\mu_j}$ and minimising $\theta^{(\mu_j)}_{\mu_{k\neq j}}$, whilst satisfying Eq. (4.122).

Recall the form of the states that we are distinguishing between using $\Xi^{(n-1)} = \{\xi_{\mu_j,\tau}\}$, rewritten here for convenience:

$$\rho_{\mu_j,\tau} = \frac{1}{(n-j)(j+1)} \bigoplus_{i=0}^{j} \mathbb{I}_{\mathcal{Q}_{\mu_i}} \otimes \Omega_{\mu_i,\tau}. \tag{4.135}$$

The first thing to notice when constructing $\Xi^{(n-1)}$ is that $\rho_{\mu_j,\tau}$ does not have any $\mathcal{Q}_{\mu_i} \otimes \mathcal{P}_{\mu_i}$ components when $i > j$. Therefore, there is no reason for $\xi_{\mu_j,\tau}$ to have these components either. So we can update the elements of $\Xi^{(n-1)}$ to

$$\xi_{\mu_j,\tau} = \bigoplus_{i=0}^{j} \theta^{(\mu_j)}_{\mu_i} \mathbb{I}_{\mu_i}. \tag{4.136}$$

Let's now see how we maximise $\theta^{(\mu_j)}_{\mu_j}$.

Defining $N = \lfloor (n-1)/2 \rfloor$ for convenience and readability, notice that the *only* element that has a $\mathcal{Q}_{\mu_N} \otimes \mathcal{P}_{\mu_N}$ component is $\xi_{\mu_N,\tau}$. This means that $\theta^{(\mu_N)}_{\mu_N}$ can take it's maximum possible value of $1/|C_{\mu_N}|$. Now, like mentioned, we want to minimise contributions to $\xi_{\mu_N,\tau}$ from all the other subspaces $\mathcal{Q}_{\mu_{i<N}} \otimes \mathcal{P}_{\mu_{i<N}}$. The limit to how low we can go is dictated by Eq. (4.122a) which, when rearranged says that

$$\theta^{(\mu_j)}_{\mu_{i-1}} \geq \left(1 - \frac{d_{\mathcal{P}_{\nu_i}}}{|C_{\nu_i}|} \frac{(n-1)!}{d_{\mathcal{P}_{\mu_{i-1}}} (n-i)!(i-1)!}\right) \theta^{(\mu_j)}_{\mu_i}. \tag{4.137}$$

$n-1$	$P^{\text{1st}}_{\text{improved}}$	$P^{\text{1st}}_{\text{lower}}$	$P^{\text{1st}}_{\text{optimal}}$	$P^{\text{1st}}_{\text{guess}}$
2	58.3%	58.3%	62.5%	50%
3	31.25%	31.25%	41.67%	25%
4	17.41%	17.36%	29.34%	12.5%

Table 4.4: Intermediate classification success rates for various values of $n-1$, corresponding to the lower bound $P^{\text{1st}}_{\text{lower}}$ derived in Eq. (4.133), an improved bound $P^{\text{1st}}_{\text{improved}}$ found via Algorithm 1. The optimal and guess success rates, $P^{\text{1st}}_{\text{optimal}}$, $P^{\text{1st}}_{\text{guess}}$ respectively, are also included for comparison.

Using $|C_{\nu_i}| = \binom{n}{i}$ (because $i < n/2$), along with Eq. (2.141) we take the value of $\theta^{(\mu_j)}_{\mu_{i-1}}$ to be

$$\theta^{(\mu_j)}_{\mu_{i-1}} = \frac{\theta^{(\mu_j)}_{\mu_i}}{n-2i+2}. \tag{4.138}$$

After this, the smallest allowed value for $\theta^{(\mu_j)}_{\mu_{i-2}}$ can be found in the same way, and so on. For fixed j, we can therefore write down the smallest $\theta^{(\mu_j)}_{\mu_i}$ for any $i < j$ as follows:

$$\theta^{(\mu_j)}_{\mu_{i<j}} = \theta^{(\mu_j)}_{\mu_j} \prod_{l=1}^{j-i} \frac{1}{n-2(j-l)}. \tag{4.139}$$

We therefore have access to every $\theta^{(\mu_N)}_{\mu_i}$ that makes up $\xi_{\mu_N,\tau}$. This allows us to find $\xi_{\mu_{N-1},\tau}$. To do this, first recall that $\theta^{(\mu_N)}_{\mu_{N-1}} = 0$. Next, to find the largest possible $\theta^{(\mu_{N-1})}_{\mu_{N-1}}$, we put $\theta^{(\mu_j)}_{\mu_{N-1}} = 0,\ \forall j < N-1$, and use the completeness of $\Xi^{(n-1)}$:

$$\sum_{j=0}^{N} |C_{\mu_j}| \theta^{(\mu_j)}_{\mu_i} = 1,\ \forall 0 \leq i \leq N, \tag{4.140}$$

to find

$$\begin{aligned}
\theta^{(\mu_{N-1})}_{\mu_{N-1}} &= \frac{1}{|C_{\mu_{N-1}}|}\left(1 - \sum_{j\neq N-1} |C_{\mu_j}| \theta^{(\mu_j)}_{\mu_{N-1}}\right) \\
&= \frac{1}{|C_{\mu_{N-1}}|}\left(1 - \sum_{j> N-1} |C_{\mu_j}| \theta^{(\mu_j)}_{\mu_{N-1}}\right) \\
&= \frac{1}{|C_{\mu_{N-1}}|}\left(1 - |C_{\mu_N}| \theta^{(\mu_N)}_{\mu_{N-1}}\right) \\
&= \frac{1}{|C_{\mu_{N-1}}|} \frac{n-2N+1}{n-2N+2},
\end{aligned} \tag{4.141}$$

where $\theta^{(\mu_N)}_{\mu_{N-1}}$ was found using Eq. (4.138) or Eq. (4.139). From here, the other components of $\xi_{\mu_{N-1},\tau}$ are found using Eq. (4.139), after which the process is repeated to find $\xi_{\mu_{N-2},\tau}$ and beyond.

Algorithm 1 summarises the steps taken to construct $\Xi^{(n-1)}$, and Fig. 4.5 presents a visual representation of the method used. Table 4.4 compares the success rates $P^{\text{1st}}_{\text{guess}}, P^{\text{1st}}_{\text{lower}}, P^{\text{1st}}_{\text{improved}}$, where $P^{\text{1st}}_{\text{improved}}$ denotes the success rate of the first classification when the intermediate measurement is constructed using Algorithm 1. Note that the first instance in which Algorithm 1 outperforms Eq. (4.133) occurs when $n = 5$. Now, to gain some more intuition for how the algorithm works, let us consider some examples.

Example: $2 \to 3$ qubits

In this scenario, $n = 3$ and therefore, $N = 1$. Here, $\Xi^{(2)}$ is made up of the following operators:

$$\xi_{\mu_0} = \left[\theta^{(\mu_0)}_{\mu_0}\mathbb{I}_{\mu_0}\right] \oplus \left[\theta^{(\mu_0)}_{\mu_1}\mathbb{I}_{\mu_1}\right], \tag{4.144a}$$

$$\xi_{\mu_1} = \left[\theta^{(\mu_1)}_{\mu_0}\mathbb{I}_{\mu_0}\right] \oplus \left[\theta^{(\mu_1)}_{\mu_1}\mathbb{I}_{\mu_1}\right]. \tag{4.144b}$$

Algorithm 1 Construction of an intermediate measurement $\Xi^{(n-1)}$.

1: **let:** $\theta_{\mu_i}^{(\mu_j)} = 0,\ \forall i > j$.
2: **let:**

$$\theta_{\mu_N}^{(\mu_N)} = \frac{1}{|C_{\mu_N}|}, \tag{4.142a}$$

$$\theta_{\mu_j}^{(\mu_N)} = \theta_{\mu_N}^{(\mu_N)} \prod_{l=1}^{N-j} \big[n - 2(N-l)\big]^{-1}, \quad \forall j < N. \tag{4.142b}$$

3: **for** $i \in \{1, \ldots, N\}$:
4: find $\theta_{\mu_{N-i}}^{(\mu_{N-i})},\ \theta_{\mu_j}^{(\mu_{N-i})},\ \forall 0 \leq j < N-i$, such that

$$\theta_{\mu_{N-i}}^{(\mu_{N-i})} = \frac{1}{|C_{\mu_{N-i}}|}\Big(1 - \sum_{l>N-i} |C_{\mu_l}| \theta_{\mu_{N-i}}^{(\mu_l)}\Big), \tag{4.143a}$$

$$\theta_{\mu_j}^{(\mu_{N-i})} = \theta_{\mu_{N-i}}^{(\mu_{N-i})} \prod_{l=1}^{N-i-j} \big[n - 2(N-i-l)\big]^{-1}. \tag{4.143b}$$

As per *Step 1* of Algorithm 1, we set $\theta_{\mu_1}^{(\mu_0)} = 0$. *Step 2* then tells us that $\theta_{\mu_1}^{(\mu_1)} = 1/|C_{\mu_1}| = 1$, and therefore

$$\begin{aligned} \theta_{\mu_0}^{(\mu_1)} &= \theta_{\mu_1}^{(\mu_1)} \prod_{l=1}^{1} \big[3 - 2(1-l)\big]^{-1}, \\ &= \frac{1}{3}. \end{aligned} \tag{4.145}$$

Finally, *Steps 3 & 4* result in

$$\begin{aligned} \theta_{\mu_0}^{(\mu_0)} &= \frac{1}{|C_{\mu_0}|}\Big[1 - |C_{\mu_1}| \theta_{\mu_0}^{(\mu_1)}\Big], \\ &= \frac{2}{3}. \end{aligned} \tag{4.146}$$

The intermediate POVM $\Xi^{(2)}$ is therefore made up of the following

$$\xi_{\mu_0} = \frac{2}{3}\mathbb{I}_{\mu_0}, \tag{4.147a}$$

$$\xi_{\mu_1} = \left[\frac{1}{3}\mathbb{I}_{\mu_0}\right] \oplus \mathbb{I}_{\mu_1}, \tag{4.147b}$$

which is exactly what we found in Eq. (3.52)[21] and Eq. (4.76). It also coincides with the success rate derived in Sec. (4.5.1).

Example: $4 \to 5$ qubits

Let's now consider the case of $n = 5$, which is the first instance of this algorithm performing better than the results found in Sec. 4.5.1. Here, we have $N = 2, |C_{\mu_0}| = 1, |C_{\mu_1}| = 4, |C_{\mu_2}| = 3$.

Step 1:

$$\begin{aligned} \theta_{\mu_0}^{(\mu_1)} &= \theta_{\mu_0}^{(\mu_2)} = 0, \\ \theta_{\mu_1}^{(\mu_2)} &= 0. \end{aligned}$$

[21] Albeit with different notation.

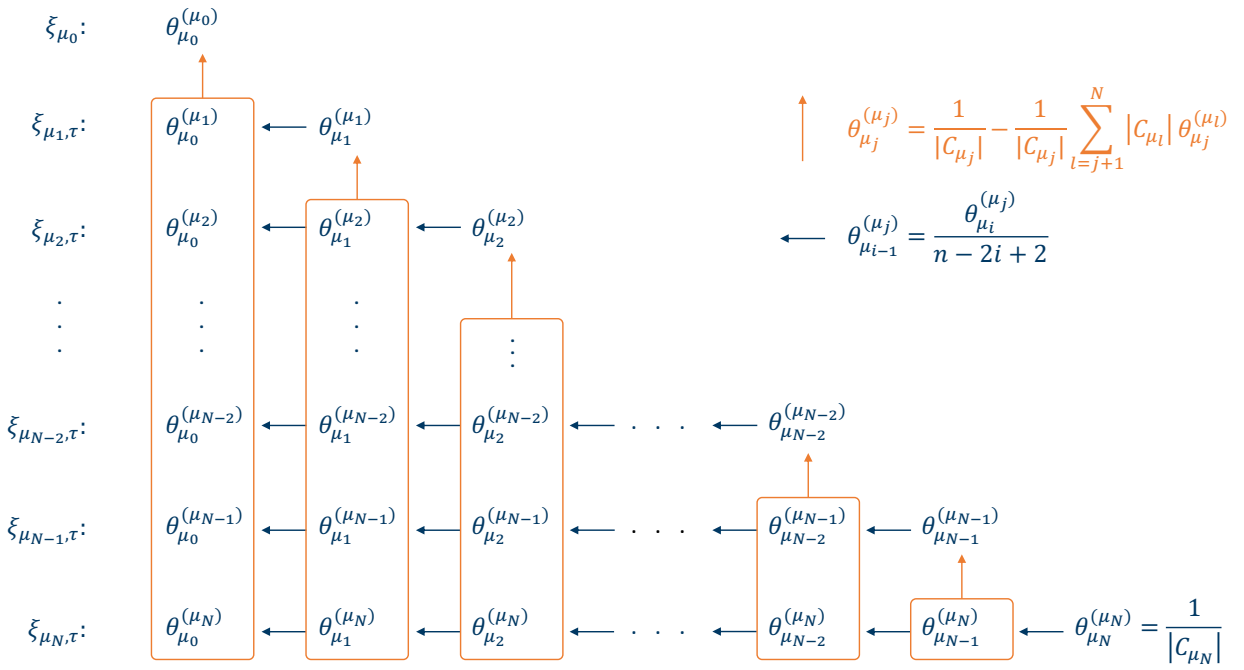

Figure 4.5: Schematic of Algorithm 1. The blue arrows, going from right to left, indicate that the weights of each component in $\xi_{\mu_j,\tau}$ can be related, recursively, by Eq. (4.138). The orange arrows, going from bottom to top, along with the orange boxes, depict how the coefficients $\theta_{\mu_j}^{(\mu_j)}$ are found: using Eq. (4.143a) (written in a slightly different, but equivalent, form in this figure). With that, the weighted sum in this expression is represented by the orange boxes.

Step 2:

$$\begin{aligned}
\theta_{\mu_2}^{(\mu_2)} &= \frac{1}{|C_{\mu_2}|} = \frac{1}{3}, \\
\implies \theta_{\mu_1}^{(\mu_2)} &= \theta_{\mu_2}^{(\mu_2)} \prod_{l=1}^{1} \left[5 - 2(2-l)\right]^{-1} = \frac{1}{9}, \\
\text{and } \theta_{\mu_0}^{(\mu_2)} &= \theta_{\mu_2}^{(\mu_2)} \prod_{l=1}^{2} \left[5 - 2(2-l)\right]^{-1} = \frac{1}{45}.
\end{aligned}$$

Steps 3 & 4 ($i = 1$):

$$\begin{aligned}
\theta_{\mu_1}^{(\mu_1)} &= \frac{1}{|C_{\mu_1}|}\left[1 - |C_{\mu_2}|\theta_{\mu_1}^{(\mu_2)}\right] = \frac{1}{6}, \\
\implies \theta_{\mu_1}^{(\mu_0)} &= \theta_{\mu_1}^{(\mu_1)} \prod_{l=1}^{1} \left[5 - 2(2-1-l)\right]^{-1} = \frac{1}{30}.
\end{aligned}$$

Steps 3 & 4 ($i = 2$):

$$\theta_{\mu_0}^{(\mu_0)} = \frac{1}{|C_{\mu_0}|}\left[1 - |C_{\mu_1}|\theta_{\mu_0}^{(\mu_1)} - |C_{\mu_2}|\theta_{\mu_0}^{(\mu_2)}\right] = \frac{4}{5}.$$

Putting this all together, our measurement $\Xi^{(4)}$ is made up of the following

$$\xi_{\mu_0} = \frac{4}{5}\mathbb{I}_{\mu_0}, \tag{4.148a}$$

$$\xi_{\mu_1,\tau} = \frac{1}{30}\mathbb{I}_{\mu_0} \oplus \frac{1}{6}\mathbb{I}_{\mu_1}, \tag{4.148b}$$

$$\xi_{\mu_2,\tau} = \frac{1}{45}\mathbb{I}_{\mu_0} \oplus \frac{1}{9}\mathbb{I}_{\mu_1} \oplus \frac{1}{3}\mathbb{I}_{\mu_2}, \tag{4.148c}$$

which, after a little algebra, and using Eq. (4.45), results in

$$P_{\text{improved}}^{\text{1st}} = \frac{47}{270} \approx 17.41\% > 17.36\% \approx P_{\text{lower}}^{\text{1st}}. \tag{4.149}$$

4.6 Discussion

Intuitively, the unsupervised classification of quantum data is, at least to me, not a trivial problem. Unlike their classical counterpart, since completely unknown, there is a continuum of possible states for each datum to occupy (e.g. for qubits, any point on the Bloch sphere). Therefore, considering each data point individually tells us nothing, either about them, or the structure of the dataset as a whole. Remarkably, as we saw in Sec. 4.2, and as was noted in Refs. [71, 92], despite our complete ignorance of the state of each individual datum, when considering the quantum dataset as a whole, information about its structure could be learnt: namely, the number of each type of quantum state, as well as their order. However, free lunches being non-existent, we saw how the act of learning about a dataset induced disturbance in the quantum state representing it. This led us to ask the question: how well can we classify an $(n-1)$-qubit subset of an n-qubit dataset, without affecting a subsequent, overall classification on the entire dataset?

Interestingly, we found picked up on some hints that suggested that, in order to preserve the second classification, we couldn't learn anything about the order of the states in the $(n-1)$-qubit subset. It appeared that all this first (or intermediate) classification could therefore tell us was something about how many of each type of state there were (being a binary classification, this meant how many zeroes and ones there were). We made steps to prove this result, but did not manage to prove Conjecture 4.A.1. We saw that, if true, a consequence of this is that no non-trivial classification can be performed on the first $n-m$ qubits (for $m > 1$) without affecting one's ability to subsequently classify the entire n-qubit dataset. It would be

interesting to see how this property generalises: given a fixed measurement Π which shares its symmetries with a set of quantum states R, does an intermediate measurement on R with a different goal have to be ignorant with regards to these symmetries if we don't want to affect the success rate of Π? We leave this question for future work. Other than this general observation, in this chapter, we saw that constraining our intermediate measurement allowed for us to write down a closed form, analytical expression for the success rate of the $(n-1)$-qubit classification: $P^{\text{1st}}_{\text{lower}}$. Corresponding to a constrained measurement, we were forced to view this only as a lower bound to the optimal value. Indeed, it was confirmed that this was a lower bound when we constructed an intermediate measurement whose success rate would first beat $P^{\text{1st}}_{\text{lower}}$ when $n = 5$. In order to do so, we wrote down an algorithm to construct such a measurement, and hypothesised that the resulting measurement is the best one can do in this scenario. A proof that this is true is absent from this thesis, so we can only take this construction to correspond to an improved lower bound of the success rate. We donate the proof (or disproof) to future works.

Appendix 4.A Unproven result

We note here, for convenience, a result that needs to be proven to complete the proof of Lemma 4.4.2. This would allow us to be sure that, when classifying $n-1$ qubits, nothing can be learnt about their order without affecting a subsequent classification on the entire n-qubit dataset.

Conjecture 4.A.1. *The expression*

$$\sum_{[\sigma\in S_n\backslash S_{n-1}]_{\nu_k}} D^{\mu_j,\tau}_{\nu_k,\sigma}\otimes\Big[\mathbf{p}_{\nu_k}(\sigma)\big(\Omega_{\mu_{k-1}}\otimes|1\rangle\langle 1|\big)\mathbf{p}^\dagger_{\nu_k}(\sigma)\Big] = \mathbb{I}_{\mathcal{Q}_{\nu_k}}\otimes\left(\Big[\Theta^{(\mu_j,\tau)}_{\mu_k}\otimes|0\rangle\langle 0|\Big]\oplus\Big[\tilde{\Theta}^{(\mu_j,\tau)}_{\mu_{k-1}}\otimes|1\rangle\langle 1|\Big]\right) \quad (4.150)$$

holds only if $D^{\mu_j,\tau}_{\nu_k,\sigma} = D^{\mu_j,\tau}_{\nu_k,\sigma'},\ \forall\sigma,\sigma'\in S_n\backslash S_{n-1}$.

Further, the following conjecture is used to derive bounds that allow us to explicitly construct intermediate measurements.

Conjecture 4.A.2. *The expression*

$$\sum_{[\sigma\in S_{n-1}]_{\nu_k}} D^{\mu_j,\tau}_{\nu_k,\sigma}\otimes\Omega_{\nu_k,\sigma} = \left(\theta^{(\mu_j)}_{\mu_{k-1}} - \left[1-\frac{d_{\mathcal{P}_{\nu_k}}}{|C_{\nu_k}|}\frac{(n-1)!}{d_{\mathcal{P}_{\mu_{k-1}}}(n-k)!(k-1)!}\right]\theta^{(\mu_j)}_{\mu_k}\right)\mathbb{I}_{\mathcal{Q}_{\nu_k}}\otimes\big(\mathbb{I}_{\mathcal{P}_{\mu_{k-1}}}\otimes|1\rangle\langle 1|\big). \quad (4.151)$$

holds only if $D^{\mu_j,\tau}_{\nu_k,\sigma} = D^{\mu_j,\tau}_{\nu_k,\sigma'}\propto\mathbb{I}_{\mathcal{Q}_{\nu_k}},\ \forall\sigma,\sigma'\in S_{n-1}$.

These conjectures appear to be related to the question of whether $\{\Omega_{\nu_k,\sigma}\}_{[\sigma]_{\nu_k}}$ is a set of linearly independent operators. To see this, suppose $\{\Omega_{\nu_k,\sigma}\}_{[\sigma]_{\nu_k}}$ are linearly independent. Then there exists a set of operators $\{E_{\nu_k,\sigma}\}_{[\sigma]_{\nu_k}}$ such that $\text{Tr}(E_{\nu_i,\sigma'}\Omega_{\nu_i,\sigma}) = \delta_{\sigma'\sigma},\ \forall\sigma,\sigma'$, from which the above conjectures follow. This is one possible direction we could explore these conjectures via. But we leave this for future work.

Chapter 5

Indefinite causal key distribution

The contents of this chapter are published as a preprint [116].

5.1 Introduction

In our everyday, classical world, we are used to events occurring in a well defined order: A happens before B or vice versa. Remarkably, it appears that, in the quantum world, events can happen in a (controlled) superposition of orders [11–13]. This phenomenon has been termed indefinite causal order (ICO) and, aside from the foundational interest in this topic, a number of applications have been proposed that often show an advantage, or interesting difference, when compared to their definite causal counterparts [11, 117–124]. Such differences usually present themselves in situations where the relevant operations are incompatible (that is, when such operations do not commute with one another). This has allowed for far reaching proposals: from increasing the capacity of noisy channels [120–122] to violating fundamental quantum metrological limits [119]. Motivated by this relation to non-commuting operations, we explore here whether it can aid in another such application, this time in the well established field of quantum key distribution (QKD).

QKD is concerned with the scenario in which two parties, conventionally named Alice and Bob, would like to share a private key (a string of 0s and 1s) in such a way that they are confident an eavesdropping third party, called Eve, has not been listening in. There have been a number of protocols proposed [4, 125–132], the first of which being by Charles Bennett and Giles Brassard in 1984 (BB84) [4]. The security of these protocols comes from the fact that Eve can be detected. This is possible because, when Eve is present, due to the quantum phenomenon of measurement disturbance, a non-zero probability of error in Bob's key, with respect to Alice's, is induced. So, if one could somehow detect these errors induced by Eve, it could be concluded that an eavesdropper had been listening in. The way that these errors are normally detected is by having Alice and Bob publicly compare a subset of their respective raw keys. Now public information, this subset is subsequently discarded regardless of whether they conclude Eve is there or not.

To our knowledge, this public comparison is a feature of all QKD protocols so far proposed[1]. In this chapter, we consider how one might adapt the simplest QKD scheme: the BB84 protocol, to an indefinite regime. In doing so, we find that we can determine whether eavesdroppers are there or not *without* having to publicly compare a subset of the distributed key. We also provide some understanding of the security of such a protocol by proving that it is secure against a class of individual attacks. It is natural to ask whether this "private" detection is a consequence of ICO or if it is allowed by other features of quantum mechanics. Indeed, we find a protocol that occurs in a well defined order which allows for this same phenomenon. To do this, however, an extra instance of Alice's operation seems to be required, a property consistent with other discussions of indefinite versus definite causal orderings [11]. As we will see, although there is the potential for some more subtle differences between the two main schemes of this chapter, we ultimately conclude that ICO may not offer an advantage to QKD.

[1]There has been work in error correction and privacy amplification without publicly declaring any of the key (that is, the publicly shared information is put through various hash functions) [133]. However, being based on classical post-processing techniques, this is different from what we find here.

In Sec. 5.2 we briefly discuss the general background theory of the two topics of importance in this chapter: indefinite causal order and quantum key distribution. In Sec. 5.3.1, we describe how a key can be distributed between Alice and Bob in an indefinite causal order when no eavesdropper is present. In Sec. 5.3.2 we introduce a single eavesdropper to gain some intuition of their effects. One eavesdropper location being insufficient to prove the security of this protocol, in Sec. 5.4, a second and final eavesdropper is introduced, and we gain some intuition about the security of this protocol by considering a class of individual attacks by the eavesdroppers. Following this, in Sec. 5.5 we briefly discuss whether this phenomenon is truly a consequence of indefinite causal order, and whether there are any alternate differences between the definite and indefinite cases. Finally, in Sec. 5.6, the findings are summarised along with a discussion of the implementability and practicality of this ICO QKD protocol.

5.2 Background theory

5.2.1 Indefinite causal order

Suppose two parties, Alice and Bob, hope to act on some state ρ sequentially with the respective operations $\mathcal{A}, \mathcal{B}$ (or more generally, sets of operations, i.e. instruments) defined using the Kraus operators $\{A_i\}, \{B_j\}$, respectively. Normally, at least from a classical perspective, this happens, as depicted in Fig. 5.1, in a *definite* order: either Alice before Bob,

$$\rho \to \sum_i A_i \, \rho \, A_i^\dagger \to \sum_{i,j} B_j A_i \, \rho \, A_i^\dagger B_j^\dagger, \tag{5.1}$$

or Bob before Alice,

$$\rho \to \sum_j B_j \, \rho \, B_j^\dagger \to \sum_{i,j} A_i B_j \, \rho \, B_j^\dagger A_i^\dagger. \tag{5.2}$$

In quantum mechanics, however, the order in which Alice and Bob act on ρ can be indefinite - a phenomenon known as indefinite causal order (ICO). Take the quantum switch for example[2], where an extra, *control* qubit in the state ω dictates the order in which Alice and Bob act on ρ. Much like a classical switch, if we turn it *on* and set $\omega = |1\rangle\langle 1|$, then Alice acts before Bob. Conversely, if we switch it *off* and let $\omega = |0\rangle\langle 0|$, then Bob would go before Alice. However, since ω is a quantum state, it can be in a superposition of $|0\rangle$ and $|1\rangle$, meaning that Alice and Bob can act on ρ in a *controlled superposition* of orders.

Let us write this down mathematically. As mentioned, if the control qubit is in the state $\omega = |1\rangle\langle 1|$, then Alice acts on the target qubit using $\mathcal{A}$ before Bob acts on it with $\mathcal{B}$, and if $\omega = |0\rangle\langle 0|$, then $\mathcal{B}$ occurs before $\mathcal{A}$. Following the notation of Ref. [122], we can therefore write the quantum switch as the following operation

$$\rho \to \mathcal{S}_\omega(\mathcal{A}, \mathcal{B})(\rho) = \sum_{i,j} S_{ij} \, (\rho \otimes \omega) \, S_{ij}^\dagger, \tag{5.3}$$

where the Kraus operators $\{S_{ij}\}$ are defined as

$$S_{ij} = A_i B_j \otimes |0\rangle\langle 0| + B_j A_i \otimes |1\rangle\langle 1| \tag{5.4}$$

This is depicted in Fig. 5.1(c).

5.2.2 Quantum key distribution

Aside from being in an indefinite causal order with one another, Alice and Bob also like sharing private keys with each other to use for various cryptographic tasks. In quantum communications, this is often done (for example in original implementation: BB84) by having Alice prepare qubits in states that correspond to the 0s and 1s of the private key and sending them to Bob to be measured. Indeed, in BB84, Alice and Bob respectively prepare and measure, independently and randomly, in one of two mutually unbiased bases. In this work, we will use the Pauli x and z-bases: $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ respectively. If Alice (Bob) prepared

[2]This is just one example of indefinite causal order, but by far the most understood, and it is what we use throughout this chapter. For more general discussions, see e.g. Ref. [134].

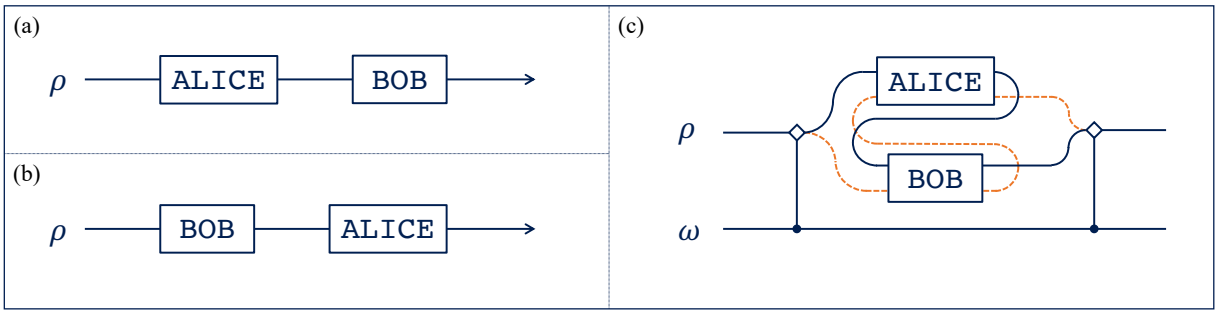

Figure 5.1: Quantum mechanics allows for more freedom in the ordering of events: (a) Alice can act on a state ρ before Bob, (b) Bob before Alice, or (c) in a superposition of both orders, controlled on some quantum state ω.

(measured) the qubit to be in the state $|0\rangle$ or $|+\rangle$, she (he) will have a corresponding key bit of 0. Likewise, if $|1\rangle, |-\rangle$ the corresponding key bit will be 1. Once Bob has measured the qubit Alice sent him, the two parties publicly discuss which bases they chose. If they chose different bases, there is only a 50% chance of them agreeing on the key bit value, so they discard the corresponding key bit. If, however, they chose the same basis, when no eavesdroppers are present, Bob's measurement result is guaranteed to correspond to the state prepared by Alice, assuming noiseless and lossless transmission, as we will do throughout. Therefore, Alice and Bob can use the corresponding ordered set of key bit values as their shared key.

To make this protocol secure, notice that when an eavesdropper, Eve, intercepts the transmission from Alice to Bob and tries to learn the key bit value being shared, she disturbs the quantum state being sent with non-zero probability. This means that, even if Alice and Bob agree on the basis chosen, there is a non-zero probability that they disagree on the state of the qubit, which implies that there is a chance of an error in Bob's key with respect to Alice's. To detect these errors, Alice and Bob take a subset of their sifted keys and compare them *publicly*. Since it has to be done publicly, this subset must subsequently be discarded, regardless of whether errors, and therefore Eve, were detected or not. Let us now see how this protocol can be adapted to an indefinite causal ordered setting.

5.3 Quantum key distribution in an indefinite causal order

5.3.1 Indefinite causal key distribution with no eavesdroppers

In BB84, Alice would prepare the qubits to be sent to Bob in a certain state. When considering an indefinite causal ordered scheme, Alice is simultaneously sending and receiving the qubit from Bob, so having one party prepare the state makes little sense. To avoid this, *both Alice and Bob* measure the qubit being used, which, because of how states are updated following projective measurements, allows them to both be the preparer and measurer of the shared qubit. This method has similarities to how the key is generated in protocols like E91 [125]. Taking this approach, the key would be made up of the results of a projective measurement on some qubit in the state ρ, but only when Alice and Bob agree they had performed the *same* projective measurement. This is because, once one party performs this measurement, ρ collapses to the measurement operator corresponding to the measurement outcome obtained. Due to the projective nature of the measurement, a subsequent measurement performed by the other party in the same basis necessarily results in the same measurement outcome (assuming noiseless and lossless channels).

Thinking of the key generation in this way, we can consider a scheme in which a key is distributed in an indefinite causal order. Here, we send a state ρ to two parties, Alice and Bob, in a controlled superposition of two orders: Alice before Bob and Bob before Alice. As shown in Fig. 5.2, this superposition is controlled by the two-level state ω: if $\omega = |0\rangle\langle 0|$, ρ travels around the loop in one direction, if $\omega = |1\rangle\langle 1|$, ρ travels around the loop in the opposite direction, and if $\omega = |\varphi\rangle\langle\varphi|$ is in some superposition of $|0\rangle$ and $|1\rangle$, ρ travels

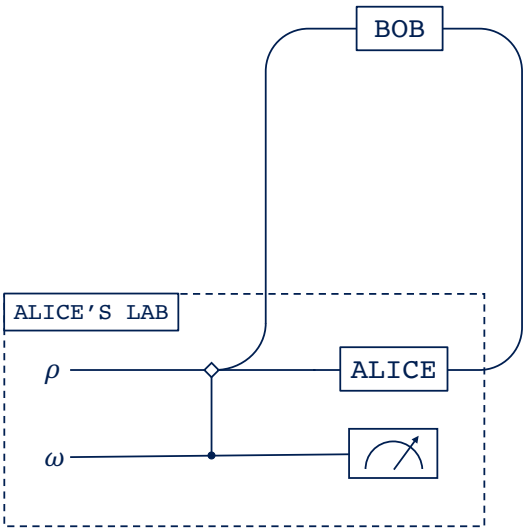

Figure 5.2: Indefinite causal key distribution with no eavesdroppers. A key is shared between Alice and Bob by sending a state ρ to them in a superposition of orders controlled by the state ω. Alice and Bob perform projective measurements randomly in either the Pauli x or z-basis. After discarding cases in which Alice and Bob measured in different bases, they are left with identical keys. Regardless of the initial state ω of the control qubit, ω never changes when there are no eavesdroppers, a phenomenon we see not to be true when an eavesdropper is introduced.

around the loop in a superposition of both directions[3]. Alice and Bob then both make a random choice to measure either in the Pauli z-basis: $\{|0\rangle, |1\rangle\}$, or x-basis: $\{|+\rangle, |-\rangle\}$. We can therefore think of Alice and Bob as acting on the state by each putting it through separate copies of the quantum channel $\mathcal{A}$, defined by the Kraus operators

$$A_0 = \frac{1}{\sqrt{2}}|0\rangle\langle 0|, \tag{5.5a}$$

$$A_1 = \frac{1}{\sqrt{2}}|1\rangle\langle 1|, \tag{5.5b}$$

$$A_+ = \frac{1}{\sqrt{2}}|+\rangle\langle +|, \tag{5.5c}$$

$$A_- = \frac{1}{\sqrt{2}}|-\rangle\langle -|, \tag{5.5d}$$

where the factors of $1/\sqrt{2}$ arise because we are assuming Alice and Bob are both equally likely to measure in the x or z-basis[4]. For convenience, define the set containing the Kraus operator indices by $I := \{0, 1, +, -\}$. It should be made clear that Alice and Bob are not just putting ρ through some quantum channel, they are indeed performing the stated measurements. They could, for example, store their measurement results in a four dimensional ancillary register R (available only in their respective laboratories) initially in the state $|m_0\rangle^R$. The corresponding Kraus operators that would achieve this would have the form $A'_i = |i\rangle\langle i| \otimes |m_i\rangle^R\langle m_0|^R/\sqrt{2}$, where $|m_i\rangle$ encode the four possible measurement outcomes $i \in I$ in orthogonal states: $\langle m_i|m_j\rangle = \delta_{ij}$. Having said this, since these ancillary systems factor out, we can take A_i to have the form given in Eq. (5.5).

Following their measurements, Alice and Bob then publicly discuss the basis they chose for each measurement and only keep the measurement outcomes in which they measured ρ in the same basis. Assuming no errors occur between Alice and Bob's measurements, their keys, made up of the measurement outcomes they

[3]Note that Fig. 5.2 is purely a schematic and we are assuming that Alice and Bob's channels do not depend on the direction the state is traversing the loop.

[4]This is not always the case, often, one basis is taken to be heavily biased over the other [135].

kept, should be identical. In what follows, similarly to what we discussed earlier, a measurement outcome of 0 and + will correspond to a 0 in the key. Likewise, 1 and − correspond to a 1 in the key.

Let's see in more detail out what happens to the state ρ when it is put through the setup in Fig. 5.2. Following [122], the channel that ρ goes through, is given by

$$\mathcal{S}_\omega(\mathcal{A},\mathcal{A})(\rho) = \sum_{i,j\in I} S_{ij}\rho\otimes\omega S_{ij}^\dagger, \tag{5.6}$$

where

$$S_{ij} = A_iA_j\otimes|0\rangle\langle 0| + A_jA_i\otimes|1\rangle\langle 1|. \tag{5.7}$$

After some algebra and index relabelling, it can be shown that Eq. (5.6) can be rewritten as follows:

$$\mathcal{S}_\omega(\mathcal{A},\mathcal{A})(\rho) = \frac{1}{4}\sum_{i,j\in I}\left(\{A_i,A_j\}\rho\{A_i,A_j\}^\dagger\otimes\omega + [A_i,A_j]\rho[A_i,A_j]^\dagger\otimes\sigma_z\omega\sigma_z\right) \tag{5.8}$$

where σ_z is the z Pauli operator.

Now, recall that, after public discussion, Alice and Bob only keep the cases in which they performed a measurement in the same basis. Therefore, following this discussion, the state becomes

$$\mathcal{S}_\omega(\mathcal{A},\mathcal{A})(\rho)\to\frac{1}{2}\sum_{S\in B}\sum_{i,j\in S}\left(\{A_i,A_j\}\rho\{A_i,A_j\}^\dagger\otimes\omega + [A_i,A_j]\rho[A_i,A_j]^\dagger\otimes\sigma_z\omega\sigma_z\right), \tag{5.9}$$

where the prefactor is found by requiring normalisation, $B=\{\{0,1\},\{+,-\}\}$, and S labels the elements of B. Noting the form of A_k given in Eq. (5.5), the terms in these sums have the following properties

$$\begin{aligned}\{A_i,A_j\} &= \sqrt{2}A_i\delta_{ij},\\ [A_i,A_j] &= 0,\end{aligned} \tag{5.10}$$

for all i,j from the same basis, where δ_{ij} is the Kronecker delta. This confirms that Alice and Bob must agree on their measurement outcomes. Overall, we have that

$$\mathcal{S}_\omega(\mathcal{A},\mathcal{A})(\rho)\to\sum_{i\in I}A_i\rho A_i^\dagger\otimes\omega. \tag{5.11}$$

So, when there are no eavesdroppers present, the control state ω stays in its original state and this situation is ultimately no different from that when the causal order is definite. Let us introduce an eavesdropper to see what changes.

5.3.2 Introducing an eavesdropper

Notice that, unlike in BB84, there are two places an eavesdropper can reside (see Fig. 5.4). Having said this, to gain some intuition as to how eavesdroppers change things, let us first consider introducing just a single eavesdropper, Eve, between Alice and Bob as shown in Fig. 5.3. For simplicity[5], denote the channel corresponding to Eve's measurement by $\mathcal{E}$, defined by the Kraus operators $\{E_i\}$. As before, allowing a state ρ to be acted on by Alice, Eve and Bob in an indefinite causal order controlled by ω, the channel ρ passes through is given by

$$\mathcal{S}_\omega(\mathcal{A},\mathcal{E},\mathcal{A})(\rho) = \sum_{i,j,k} S_{ijk}\rho\otimes\omega S_{ijk}^\dagger, \tag{5.12}$$

where

$$\begin{aligned}S_{ijk} :=& A_iE_jA_k\otimes|0\rangle\langle 0| + A_kE_jA_i\otimes|1\rangle\langle 1|\\ =&\frac{1}{2}\{A_i,E_j,A_k\}\otimes\mathbb{1} + \frac{1}{2}[A_k,E_j,A_i]\otimes\sigma_z\end{aligned} \tag{5.13}$$

[5]More generally, Eve has access to a quantum instrument. This is discussed in more detail in Appendix 5.A

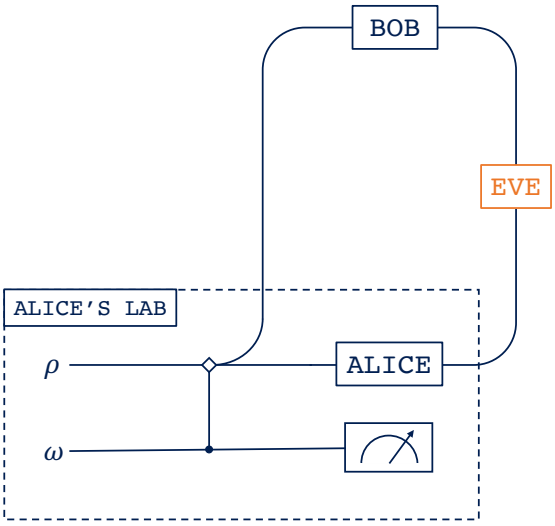

Figure 5.3: Indefinite causal key distribution with a single eavesdropper, Eve, between Alice and Bob.

such that

$$\{A_i, E_j, A_k\} := A_i E_j A_k + A_k E_j A_i, \tag{5.14a}$$
$$[A_i, E_j, A_k] := A_i E_j A_k - A_k E_j A_i. \tag{5.14b}$$

Note that E_j is always in the middle since Eve is in between Alice and Bob. After some algebra, and following the basis comparison,

$$\mathcal{S}_\omega(\mathcal{A}, \mathcal{E}, \mathcal{A})(\rho) \to \frac{1}{2} \sum_j \sum_{S \in B} \sum_{i,k \in S} \left(\{A_i, E_j, A_k\} \rho \{A_i, E_j, A_k\}^\dagger \otimes \omega + [A_i, E_j, A_k] \rho [A_i, E_j, A_k]^\dagger \otimes \sigma_z \omega \sigma_z \right). \tag{5.15}$$

From this, we can see that, as before, the ω terms survive. But more interestingly, notice that the $\sigma_z \omega \sigma_z$ terms can survive too. For example, suppose Alice and Bob measure in the z-basis and Eve measures in the x-basis, then it is possible for Alice to obtain an outcome of 0, and Bob an outcome of 1. This combination allows for $[A_0, E_\pm, A_1] \neq 0$.

We may therefore hypothesise that if Eve attempts to extract information about the state when in between Alice and Bob, she induces a nonzero $\sigma_z \omega \sigma_z$ term. So, if we were to let $\omega = |+\rangle\langle+|$ (and therefore $\sigma_z \omega \sigma_z = |-\rangle\langle-|$), if someone were to perform the measurement $\{|+\rangle\langle+|, |-\rangle\langle-|\}$ on the control state ω, and obtain an outcome of $-$, they could conclude that there was an eavesdropper in between Alice and Bob. To reiterate, since Alice can keep and measure the control qubit, this would mean that no subset of the distributed key need be publicly compared and then discarded to determine the presence of Eve. Let us now gain some understanding about how robust this hypothesis is.

5.4 Security against individual attacks

Let's see what happens when two eavesdroppers, Eve and Yves, are introduced. There being more than one eavesdropper allows for cooperative strategies. In this work, we consider *individual* attacks, where eavesdroppers work together, but on each distributed state separately [131]. The most general of these individual attacks allow for the eavesdroppers to utilise both quantum and classical correlations between their operations. However, being more involved mathematically, we leave this scenario, which we will often call the "correlated case", for Appendix 5.A. Our protocol is summarised in Protocol 5.1.

In this section, we consider a subclass of these individual eavesdropping strategies where Eve and Yves's ancilliary systems (that they use to aid in their attack) are separable, and we prove the security of the

1. Alice prepares the state $\rho = \mathbb{1}/2$ to be distributed along with a control qubit state $\omega = |+\rangle\langle+|$ that remains in her lab.
2. The state ρ is distributed to Alice and Bob's measuring devices in an indefinite causal order, controlled on ω.
3. Alice and Bob measure ρ in either the x or z-basis, chosen randomly with probability 1/2. Measurement outcomes $0, +$ correspond to a key bit 0, and outcomes $1, -$ correspond to a key bit of 1.
4. Alice and Bob compare the bases they chose and only keep the cases in which they agree.
5. For each state ρ distributed, Alice measures the corresponding control qubit state ω in the x-basis. If an outcome $+$ is obtained, carry on. If an outcome $-$ is found, Alice concludes eavesdroppers are present after which, she either aborts the key distribution, or she and Bob go ahead with privacy amplification and error correction (not discussed in this work).

Protocol 5.1: Summary of the proposed indefinite causal key distribution protocol.

protocol against them. Investigation into the full security proof of this protocol is beyond the scope of this work. This being said, the attacks considered in this section provide us with some useful understanding about the security of this protocol. The methods used follow closely those used in [129] where the authors consider a two-way deterministic quantum communications protocol in which quantum states are sent back and forth between Alice and Bob. Although they are working in a definite causal order, in this protocol, the eavesdropper has access to the state at two different points, which is why the same techniques used can be applied to our protocol.

5.4.1 Problem setup

In the scenario we consider, we assume that Alice and Bob would like their shared key to contain, on average, equal numbers of 0s and 1s. Therefore, we can make a natural choice for the initial state of the distributed qubit: $\rho = (1/2)\sum_\psi |\psi\rangle\langle\psi| = \mathbb{1}/2$, where $\{|\psi\rangle\}$ is some complete basis of the distributed qubit's Hilbert space. Now, if Alice is in the lab in which the state ρ is created and where ω resides, there are two places eavesdroppers, who we call Eve and Yves, can be located. This setup is shown in Fig. 5.4. Note that we are requiring Eve and Yves to adhere to the causal structure chosen by Alice and Bob. This is an assumption we make throughout. In addition to the state ρ being sent between Alice and Bob, Eve and Yves also have access to independent ancilliary quantum systems E, Y (respectively) initially in the states $\varepsilon := |\varepsilon\rangle\langle\varepsilon|$ and $\eta := |\eta\rangle\langle\eta|$ respectively. Eve and Yves perform the respective unitaries $U_E^{(SE)} =: U_E$, $U_Y^{(SY)} =: U_Y$ on the joint space of the distributed state ρ, living in the space labelled by S, and their respective ancillae ε, η living in the spaces labelled by E, Y respectfully. Following this, the eavesdroppers perform some joint measurement on the ancillae to try and gain some information about Alice and Bob's shared key. Note that Eve and Yves do, therefore, cooperate in this scenario, although not in the most general way possible.

For $k \in \{0, 1, +, -\}$, the eavesdroppers' unitaries are performed most generally as follows [129]:

$$U_E^{(SE)}|k\rangle^{(S)}|\varepsilon\rangle^{(E)} = |k\rangle|\varepsilon_{kk}\rangle + |\bar{k}\rangle|\varepsilon_{k\bar{k}}\rangle, \tag{5.16a}$$

$$U_Y^{(SY)}|k\rangle^{(S)}|\eta\rangle^{(Y)} = |k\rangle|\eta_{kk}\rangle + |\bar{k}\rangle|\eta_{k\bar{k}}\rangle, \tag{5.16b}$$

where $|\varepsilon_{mn}\rangle$ and $|\eta_{mn}\rangle$ are, in general, unnormalised and non-orthogonal, and $\bar{k}$ is taken to mean "not k". Note that we, from now on, will drop the superscripts unless it is unclear which space is which. Note also,

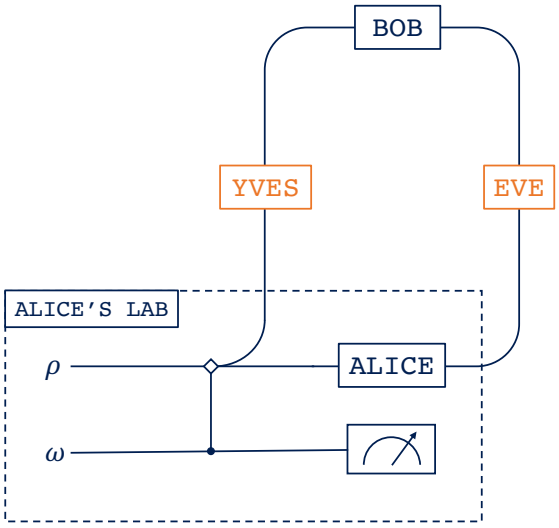

Figure 5.4: Indefinite causal quantum key distribution with two eavesdroppers Eve and Yves.

that[6]

$$|\varepsilon_{\pm\pm}\rangle = \frac{1}{2}(|\varepsilon_{00}\rangle \pm |\varepsilon_{01}\rangle \pm |\varepsilon_{10}\rangle + |\varepsilon_{11}\rangle), \tag{5.17a}$$

$$|\varepsilon_{\pm\mp}\rangle = \frac{1}{2}(|\varepsilon_{00}\rangle \mp |\varepsilon_{01}\rangle \pm |\varepsilon_{10}\rangle - |\varepsilon_{11}\rangle), \tag{5.17b}$$

and

$$|\eta_{\pm\pm}\rangle = \frac{1}{2}(|\eta_{00}\rangle \pm |\eta_{01}\rangle \pm |\eta_{10}\rangle + |\eta_{11}\rangle), \tag{5.18a}$$

$$|\eta_{\pm\mp}\rangle = \frac{1}{2}(|\eta_{00}\rangle \mp |\eta_{01}\rangle \pm |\eta_{10}\rangle - |\eta_{11}\rangle). \tag{5.18b}$$

When $k \in \{0,1\}$, we define $\langle\varepsilon_{kk}|\varepsilon_{kk}\rangle = F$, $\langle\varepsilon_{k\bar{k}}|\varepsilon_{k\bar{k}}\rangle = D$ and $\langle\eta_{kk}|\eta_{kk}\rangle = F'$, $\langle\eta_{k\bar{k}}|\eta_{k\bar{k}}\rangle = D'$, which can all be taken to be positive real numbers. These values relate to the probability that Eve and Yves leave the distributed state unaffected or not. In order to ensure unitarity,

$$F + D = 1 = F' + D', \tag{5.19a}$$

$$\langle\varepsilon_{00}|\varepsilon_{10}\rangle + \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0 = \langle\eta_{00}|\eta_{10}\rangle + \langle\eta_{01}|\eta_{11}\rangle. \tag{5.19b}$$

This allows us, without loss of generality [129], to set $\langle\varepsilon_{kk}|\varepsilon_{k\bar{k}}\rangle = \langle\varepsilon_{kk}|\varepsilon_{\bar{k}k}\rangle = 0 = \langle\eta_{kk}|\eta_{k\bar{k}}\rangle = \langle\eta_{kk}|\eta_{\bar{k}k}\rangle, \forall k \in \{0,1\}$. Also, $|\varepsilon_{kl}\rangle, |\varepsilon_{\bar{k}\bar{l}}\rangle$ are generally non-orthogonal (likewise for $|\eta_{kl}\rangle$). So, we take

$$\langle\varepsilon_{00}|\varepsilon_{11}\rangle = F\cos x, \tag{5.20a}$$

$$\langle\varepsilon_{01}|\varepsilon_{10}\rangle = D\cos y, \tag{5.20b}$$

$$\langle\eta_{00}|\eta_{11}\rangle = F'\cos x', \tag{5.20c}$$

$$\langle\eta_{01}|\eta_{10}\rangle = D'\cos y', \tag{5.20d}$$

where $x, y, x', y' \in [0, \pi/2]$. We can think of x, y (x', y') as dictating the distinguishability between Eve's (Yves's) possible ancilla states.

[6] To see this explicitly, we perform $U_E|\pm\rangle|\varepsilon\rangle = U_E(|0\rangle|\varepsilon\rangle \pm |1\rangle|\varepsilon\rangle)/\sqrt{2}$ using Eq. (5.16a). This results in $(|0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle \pm |1\rangle|\varepsilon_{11}\rangle \pm |0\rangle|\varepsilon_{10}\rangle)/\sqrt{2} = \big[|0\rangle(|\varepsilon_{00}\rangle \pm |\varepsilon_{10}\rangle) + |1\rangle(|\varepsilon_{01}\rangle \pm |\varepsilon_{11}\rangle)\big]/\sqrt{2}$, which can be rewritten (ignoring the global phase ± 1) as $\big[|\pm\rangle(|\varepsilon_{00}\rangle \pm |\varepsilon_{01}\rangle \pm |\varepsilon_{10}\rangle + |\varepsilon_{11}\rangle) + |\mp\rangle(|\varepsilon_{00}\rangle \mp |\varepsilon_{01}\rangle \pm |\varepsilon_{10}\rangle + |\varepsilon_{11}\rangle)\big]/2$. The form of $|\varepsilon_{\pm\pm}\rangle$ and $|\varepsilon_{\pm\mp}\rangle$ follow from this.

Similarly to in the previous section, following the basis comparison step, the state of the entire system is updated as follows:

$$\begin{aligned}\rho\otimes\varepsilon\otimes\eta\otimes\omega\to\rho_{\text{keep}}=\frac{1}{2}\sum_{S\in B}\sum_{j,k\in S}\Big(&\{U_Y,A_j,U_E,A_k\}\rho\otimes\varepsilon\otimes\eta\{U_Y,A_j,U_E,A_k\}^\dagger\otimes\omega\\&+[U_Y,A_j,U_E,A_k]\rho\otimes\varepsilon\otimes\eta[U_Y,A_j,U_E,A_k]^\dagger\otimes\sigma_z\omega\sigma_z\\&+\{U_Y,A_j,U_E,A_k\}\rho\otimes\varepsilon\otimes\eta[U_Y,A_j,U_E,A_k]^\dagger\otimes\omega\sigma_z\\&+[U_Y,A_j,U_E,A_k]\rho\otimes\varepsilon\otimes\eta\{U_Y,A_j,U_E,A_k\}^\dagger\otimes\sigma_z\omega\Big),\end{aligned}\tag{5.21}$$

where

$$\{U_Y,A_j,U_E,A_k\}:=U_YA_jU_EA_k+A_kU_EA_jU_Y,\tag{5.22a}$$
$$[U_Y,A_j,U_E,A_k]:=U_YA_jU_EA_k-A_kU_EA_jU_Y.\tag{5.22b}$$

Denoting Eve and Yves's joint strategy using $\mathcal{Z}$, we are now equipped to calculate the following:

1. Minimum probability of detection: d.
2. Eavesdroppers and Alice's [Bob's] mutual information: $H(\mathcal{Z}:\mathcal{A})$ $[H(\mathcal{Z}:\mathcal{B})]$.
3. Alice and Bob's mutual information: $H(\mathcal{A}:\mathcal{B})$.

5.4.2 Minimum probability of detection

Let us first calculate the eavesdropper detection probability. Recall that, in this protocol, this corresponds to measuring the control qubit to be in the state $|-\rangle\langle-|$ given that it was initially prepared in the state $|+\rangle\langle+|$. Therefore, using $\rho=\mathbb{1}/2=(1/2)\sum_\psi|\psi\rangle\langle\psi|$, the probability of detection is given by

$$P_{\text{detect}}=\frac{1}{4}\sum_\psi\sum_{S\in B}\sum_{j,k\in S}\langle\psi\varepsilon\eta|[U_Y,A_j,U_E,A_k]^\dagger[U_Y,A_j,U_E,A_k]|\psi\varepsilon\eta\rangle,\tag{5.23}$$

where $|\psi\varepsilon\eta\rangle:=|\psi\rangle^{(S)}\otimes|\varepsilon\rangle^{(E)}\otimes|\eta\rangle^{(Y)}$. Now, noting that,

$$U_YA_jU_EA_k|\psi\varepsilon\eta\rangle=\frac{1}{2}\delta_{\psi k}\big(\delta_{jk}|\varepsilon_{kk}\rangle+\delta_{j\bar{k}}|\varepsilon_{k\bar{k}}\rangle\big)\big(|j\rangle|\eta_{jj}\rangle+|\bar{j}\rangle|\eta_{j\bar{j}}\rangle\big),\tag{5.24a}$$
$$A_kU_EA_jU_Y|\psi\varepsilon\eta\rangle=\frac{1}{2}|k\rangle\big(\delta_{kj}|\varepsilon_{jj}\rangle+\delta_{k\bar{j}}|\varepsilon_{j\bar{j}}\rangle\big)\big(\delta_{j\psi}|\eta_{\psi\psi}\rangle+\delta_{j\bar{\psi}}|\eta_{\psi\bar{\psi}}\rangle\big),\tag{5.24b}$$

where, in the first equation, the order of the qubits was changed for convenience, we can calculate P_{detect} to be

$$\begin{aligned}P_{\text{detect}}=\frac{1}{2}-\frac{1}{8}\big[&FF'(3+\cos x\cos x')\\&+DD'(1+3\cos y\cos y')\\&+FD'(\cos x+\cos y')\\&+DF'(\cos y+\cos x')\big].\end{aligned}\tag{5.25}$$

Recalling that $D=1-F$ and $D'=1-F'$, and minimising P_{detect} over F,F', we find there are two[7] possibilities when minimising the probability of detection $d:=P_{\text{detect}}^{\min}$. Note that we can take this approach since D,F,D',F' can be chosen *independently* of x,x',y,y'.

Option 1: $F=0=F'$. Here,

$$d=\frac{3}{8}(1-\cos y\cos y').\tag{5.26}$$

[7]There are actually 4 possibilities, but the two options not written explicitly: $F=0=D'$ and $F=1=D'$, result in larger detection probabilities than the $F=1=F'$ case.

Option 2: $F = 1 = F'$. Here,

$$d = \frac{1}{8}(1 - \cos x \cos x'). \tag{5.27}$$

Since there are values of x, y, x', y' such that each option is smaller, we must consider both options when calculating the various mutual information values.

5.4.3 Eavesdroppers - Alice/Bob mutual information

It turns out that $H(\mathcal{Z} : \mathcal{A}) = H(\mathcal{Z} : \mathcal{B})$. So, in what follows, we only look at $H(\mathcal{Z} : \mathcal{A})$ explicitly. With the setup we're considering, after Eve and Yves have both carried out their unitaries, they perform some joint measurement on both of their ancillae that best distinguishes between a 0 and a 1 in Alice's key. In order to do this, they should utilise all public information, which means waiting for Alice to reveal her basis choice before choosing which joint measurement to perform on their ancillae. Therefore, in order to find the maximum mutual information (subject to a minimal probability of detection), two optimal measurements must be constructed: one to distinguish $\{\Psi_0^{AZ}, \Psi_1^{AZ}\}$, and one to distinguish $\{\Psi_+^{AZ}, \Psi_-^{AZ}\}$ which are the possible states of the eavesdroppers' ancillae when the z and x-bases were chosen by Alice and Bob, respectively.

For both cases, the states to be distinguished are found using

$$\Psi_l^{AZ} = \frac{1}{\mathcal{N}} \operatorname{Tr}_{S,C} \left(\rho_{\text{keep}}\big|_{k=l}\right), \tag{5.28}$$

where $\mathcal{N}$ is a normalisation constant, and S, C indicate that the trace is being carried out over the distributed and control qubit respectively. Further, $\rho_{\text{keep}}|_{k=l}$ denotes the terms in ρ_{keep} [Eq. (5.21)] in which Alice's measurement outcome is l. Let's consider the two options we found in the previous subsection.

Option 1: $F = 0 = F'$.

In this case, when $l \in \{0, 1\}$,

$$\Psi_l^{AZ} = \frac{1}{2}(\varepsilon_{01} \otimes \eta_{10} + \varepsilon_{10} \otimes \eta_{01}), \tag{5.29}$$

and when $l \in \{+, -\}$,

$$\Psi_l^{AZ} = \frac{1}{4}(\varepsilon_{10} + \varepsilon_{01}) \otimes (\eta_{10} + \eta_{01}). \tag{5.30}$$

Note that $\Psi_0^{AZ} = \Psi_1^{AZ}$ and $\Psi_+^{AZ} = \Psi_-^{AZ}$ which implies Eve and Yves's best strategy is to just guess. Therefore, the mutual information between the eavesdroppers and Alice is $H(\mathcal{Z} : \mathcal{A}) = 0$ when $F = 0 = F'$.

Option 2: $F = 1 = F'$.

In this case, when $l \in \{0, 1\}$,

$$\Psi_l^{AZ} = \varepsilon_{ll} \otimes \eta_{ll}, \tag{5.31}$$

and, when $l \in \{+, -\}$,

$$\Psi_l^{AZ} = \frac{1}{4}\big(\varepsilon_{00} + \varepsilon_{11}\big) \otimes \big(\eta_{00} + \eta_{11}\big). \tag{5.32}$$

This means that, although $\Psi_+^{AZ} = \Psi_-^{AZ}$ as in the previous case (and therefore no information can be gained here), unlike in Option 1, $\Psi_0^{AZ} \neq \Psi_1^{AZ}$ in general, and information about Alice's key can thus be accessed.

Now, like mentioned earlier, in order to maximise the mutual information between Alice and the eavesdroppers, we must find the optimal measurement that distinguishes $\{\Psi_0^{AZ}, \Psi_1^{AZ}\}$. As we saw in Sec. 2.2.6, we can do this by noticing that these states can be written as $\Psi_l^{AZ} = |\Psi_l^{AZ}\rangle\langle\Psi_l^{AZ}|$, such that

$$|\Psi_l^{AZ}\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{1 + |\langle\Psi_0^{AZ}|\Psi_1^{AZ}\rangle|}|a\rangle + (-1)^l\sqrt{1 - |\langle\Psi_0^{AZ}|\Psi_1^{AZ}\rangle|}|b\rangle\right), \tag{5.33}$$

where $|a\rangle, |b\rangle$ are some orthonormal vectors in Eve and Yves's shared ancilla space. In our case, $|\langle\Psi_0^{AZ}|\Psi_1^{AZ}\rangle|$ $= \cos x \cos x'$. The optimal measurement to distinguish these states is known to be made up of the following operators [37]:

$$\pi_l = \frac{1}{2}(|a\rangle + (-1)^l|b\rangle)(\langle a| + (-1)^l\langle b|). \tag{5.34}$$

To calculate the mutual information in the z-basis case, we use

$$\begin{aligned} H_{0/1}(\mathcal{Z}:\mathcal{A}) = &- \sum_{i\in\{0,1\}} P(z_i)\log P(z_i) \\ &- \sum_{j\in\{0,1\}} P(a_j)\log P(a_j) \\ &+ \sum_{i,j\in\{0,1\}} P(z_i,a_j)\log P(z_i,a_j), \end{aligned} \tag{5.35}$$

where the subscript 0/1 is used to highlight that this is the mutual information *only* in the z-basis case. Here, the outcome z_i corresponds to Eve and Yves performing their joint optimal measurement $\{\pi_k\}$, with outcome $k=i$, and a_j corresponds to Alice measuring j, or equivalently (and perhaps more usefully for the calculation), a_j can be thought of as the preparation of the state Ψ_j^{AZ}. After some algebra, it turns out that

$$H_{0/1}(\mathcal{Z}:\mathcal{A}) = 1 - h\Big[\big(1+\sqrt{1-\cos^2 x\cos^2 x'}\big)/2\Big], \tag{5.36}$$

where $h(q) = -q\log(q) - (1-q)\log(1-q)$ is the binary entropy function [17]. Using Eq. (5.27), this can be rewritten in terms of the minimum detection probability as

$$H_{0/1}(\mathcal{Z}:\mathcal{A}) = 1 - h\Big[\big(1+4\sqrt{d[1-4d]}\big)/2\Big], \tag{5.37}$$

such that $0 \le d \le 1/8$.

5.4.4 Alice - Bob mutual information

The calculation of the mutual information between Alice and Bob, $H(\mathcal{A}:\mathcal{B})$, is less involved than that of $H(\mathcal{Z}:\mathcal{A})$ since Alice and Bob's measurements are fixed. The key thing to note is that the probabilities required for the calculations are found using

$$P(a_l,b_m) = \mathrm{Tr}\left(\rho_{\mathrm{keep}}\big|_{k=l,j=m}\right), \tag{5.38}$$

where, similarly to before, $\rho_{\mathrm{keep}}\big|_{k=l,j=m}$ is made up from the $k=l, j=m$ terms in Eq. (5.21).

Carrying out all the algebra, we find that, when Alice and Bob measure in the z-basis, the mutual information between them is

$$H_{0/1}(\mathcal{A}:\mathcal{B}) = 1, \tag{5.39}$$

which makes sense since the unitaries being performed by Eve and Yves cause no disturbance in the distributed qubit when Alice and Bob are measuring it in the z-basis. When Alice and Bob measure in the x-basis however,

$$H_{\pm}(\mathcal{A}:\mathcal{B}) = 1 - h\big[(1+\cos x)/2\big]. \tag{5.40}$$

Intuitively, this can be understood when we realise that any errors between Alice and Bob's keys are induced purely by Eve's intervention and not Yves's (this is discussed slightly more in the following subsection). We may therefore expect to see a $\cos x$ dependence but not a $\cos x'$ one.

This second point does, however, mean we cannot directly determine $H_{\pm}(\mathcal{A}:\mathcal{B})$ [and therefore $H(\mathcal{A}:\mathcal{B})$] using the probability of detection d. However, we can use d to put some bounds on $H_{\pm}(\mathcal{A}:\mathcal{B})$. To do this, we look at how Eve and Yves maximise $H_{0/1}(\mathcal{Z}:\mathcal{A})$ [and therefore $H(\mathcal{Z}:\mathcal{A})$] for any given value of d. Plotting $H_{0/1}(\mathcal{Z}:\mathcal{A})$ with respect to x, x', it can be seen that this maximisation occurs along either the $x=0$ or $x'=0$ axis. This results in

$$H_{\pm}(\mathcal{A}:\mathcal{B})|_{x=0} = 1, \tag{5.41a}$$

$$H_{\pm}(\mathcal{A}:\mathcal{B})|_{x'=0} = 1 - h(4d), \tag{5.41b}$$

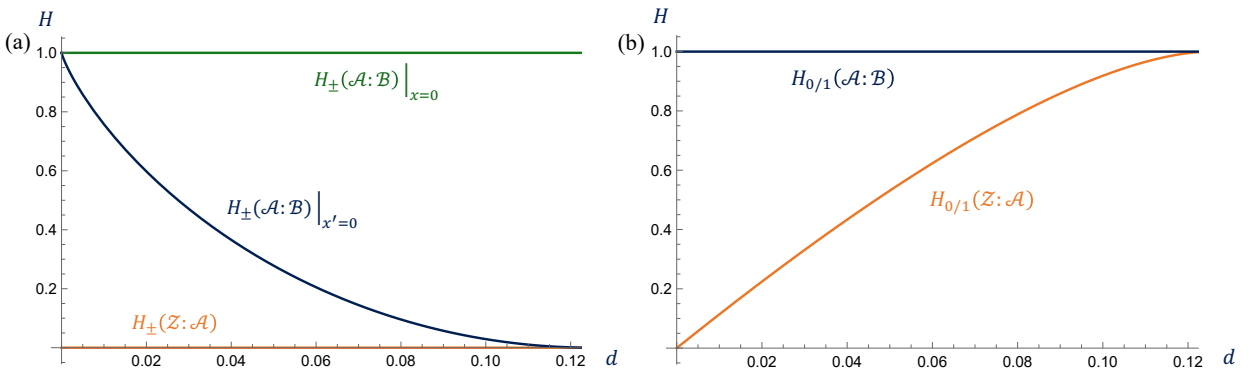

Figure 5.5: When eavesdroppers Eve and Yves carry out individual (not fully correlated) attacks, the mutual information, $H(\mathcal{Z}:\mathcal{A})$, they share with Alice (or Bob) compares to the mutual information between Alice and Bob $H(\mathcal{A}:\mathcal{B})$ as plotted. In (a), this is shown for the case in which Alice and Bob measure in the x-basis, and in (b), Alice and Bob measure in the z-basis.

where, as before, $0 \leq d \leq 1/8$. Thus, if Eve and Yves are aiming to minimise the probability of being detected,

$$H_{0/1}(\mathcal{A}:\mathcal{B}) = 1, \tag{5.42a}$$
$$H_{\pm}(\mathcal{A}:\mathcal{B}) \in [1 - h(4d), 1]. \tag{5.42b}$$

It is interesting to note that, since $H(\mathcal{Z}:\mathcal{A})|_{x=0}$ and $H(\mathcal{Z}:\mathcal{A})|_{x'=0}$ take the same range of values, the eavesdroppers can choose whether or not they want to induce errors in Alice and Bob's shared key whilst extracting information about it[8]. This effectively corresponds to how much impact they allow Eve to have.

In Fig. 5.5, we plot these various different mutual information functions with respect to the minimum detection probability d. Notice the difference between the x and z-basis cases in these plots. This is purely an artifact of how the eavesdroppers' measurements were set up in a basis dependent way. By an appropriate redefinition of these measurements, we could flip these results and have the eavesdroppers learn something about the x cases but not the z ones, or some combination of both. These plots make it clear that in both cases of Alice and Bob's basis choice, the mutual information between the eavesdroppers and Alice (or Bob) is less than or equal to the mutual information shared by Alice and Bob. Therefore, the normal post processing protocols can be undertaken to obtain a secure key between Alice and Bob, at least in the class of attacks considered here [131].

5.4.5 Example

Let us consider a simple example to gain some intuition as to how this protocol differs from its definite causal counterpart. Before we do so, let us write down the probability of error P_{error} between Alice and Bob's keys in the case of $F, F' = 1$. Using $P_{\text{error}} = \text{Tr}\left(\rho_{\text{keep}}\big|_{j=\bar{k}}\right)$, it can be shown that

$$P_{\text{error}} = \frac{1}{4}(1 - \cos x). \tag{5.43}$$

Note once again that the errors are caused purely by Eve and not Yves. Similarly to in the previous subsection, we can use the maximisation of $H(\mathcal{Z}:\mathcal{A})$ to put bounds on P_{error}. Recall that to do this, we let either $x = 0$ or $x' = 0$, from which it follows that

$$P_{\text{error}} \in [0, 2d]. \tag{5.44}$$

So, let's consider the case in which Eve performs the measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. This corresponds to $x = \pi/2$. Using Eq. (5.27) and Eq. (5.43), we can see that $P_{\text{error}} = 1/4$, but $d = 1/8$. This differs from the

[8]Note that here, we have ignored the subscripts in the mutual entropy notation since $H(\mathcal{Z}:\mathcal{A}) = H_{0/1}(\mathcal{Z}:\mathcal{A})$.

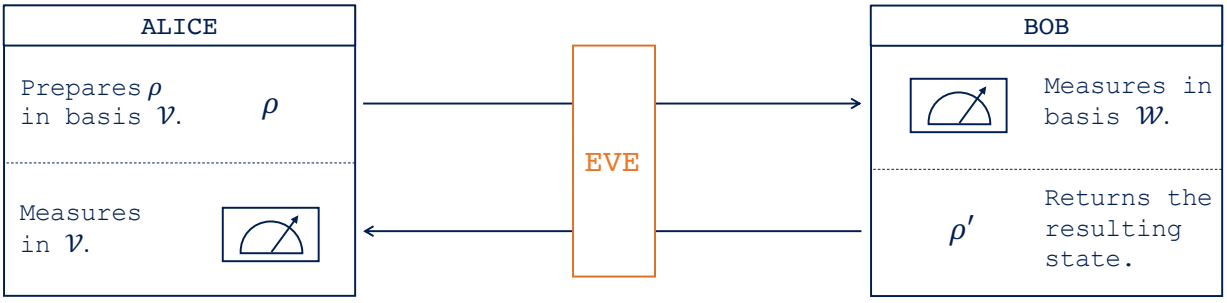

Figure 5.6: Two way QKD protocol in a definite causal order that realises private detection. The bases $\mathcal{V}, \mathcal{W}$ are independently and randomly chosen between the x and z-bases.

analogous case in BB84 where the error rate of 1/4 is used as the detection probability. This is because the effects of the eavesdroppers are not solely contained in the terms used to calculate P_{detect} (that is, the $\sigma_z\omega\sigma_z$ terms). Some of them lie in the $\omega, \omega\sigma_z$ and $\sigma_z\omega$ terms. It is possible that a different measurement on the control qubit could result in better odds. However, we do not attempt to optimise this measurement here.

It is interesting to note that the location of the eavesdroppers dictates the errors induced between Alice and Bob's key. For example, if only Yves is present, there will be no errors found (despite being detected using our methods). If, however, Eve is present, regardless of whether Yves is there or not, the probability of error between Alice and Bob's key is 1/4, similarly to what is observed in BB84. This phenomenon is true beyond this example: if only Eve is present, every detection event implies an error between Alice and Bob's corresponding key bit, since $[A_k, U_E, A_k] = 0\ \forall k$. If, however, only Yves is present, there are never any errors induced, since $[U_Y, A_k, A_{\bar{k}}] = 0\ \forall k$. This means that, if the location of the eavesdropper(s) is (are) unknown, whether or not errors occur is unknown. These ideas were hinted at in the previous subsection where we saw that the eavesdroppers had the ability to affect how much mutual information Alice and Bob shared.

5.4.6 Correlated individual attacks and beyond

As noted before, the strategies considered until now have not allowed Eve and Yves's operations to be correlated prior to the measurement of their ancillae. It turns out that the presence of eavesdroppers, performing individual attacks, can be privately detected regardless of the correlations shared between them. More precisely, for eavesdroppers working in the indefinite causal structure we have been considering, it can be shown that if the probability of detection[9] is zero for any (individual) eavesdropping strategy, then the eavesdroppers gain no useful information about the distributed key. This result is proved in Appendix 5.A. To clarify: when undetected, Eve and Yves can learn something about the key, but nothing useful. In Appendix 5.A, we show that they can learn something about which basis was chosen (which is already publicly known) as well as whether errors have occurred between Alice and Bob's keys. It follows from this that, similarly to in the previous subsection, Eve and Yves can choose to induce errors in Alice and Bob's key without being detected. But the fact remains that the information the eavesdroppers have access to has no use when it comes to learning about Alice and Bob's key.

5.5 Private detection in a definite causal order

In this section, we consider whether this same phenomena of private detection could be achieved *without* the help of indefinite causal order. Indeed, we provide here evidence that it *is* possible, albeit with the help of an extra measurement on Alice's part. We outline two possibilities.

[9] Again, taken to be the probability of measuring the control system to be in the state $|-\rangle\langle -|$.

5.5.1 Definite causal ordered protocol: option one

Suppose, as depicted in Fig. 5.6, Alice prepares a state ρ in a basis $\mathcal{V}$ that is either the x or z-basis (with corresponding key bits as before), then sends ρ to Bob, who measures in the basis $\mathcal{W}$ which, again, is chosen randomly between the x and z-bases. Following this, Bob returns the updated state back to Alice who measures it in the *same* basis that she prepared the state in: $\mathcal{V}$. As they did in the other sections of this chapter, Alice and Bob then compare which bases they chose, and only use the cases in which they agree for their shared key. Now, by counting how often she measures a different state from the one she prepared, a scenario that we call an error, Alice can monitor for eavesdroppers. This is possible since she knows *two things* when there are no eavesdroppers:

1. When $\mathcal{V} = \mathcal{W}$, the probability of error $P_{\text{error}}^{\text{same}}$ is zero.[10]
2. When $\mathcal{V} \neq \mathcal{W}$, the probability of error $P_{\text{error}}^{\text{diff}}$ is $1/2$.[11]

Let's consider an example showing how an eavesdropper's intervention affects at least one of these probabilities.

Suppose an eavesdropper, Eve, attempts to keep $P_{\text{error}}^{\text{same}}$ at its expected value of zero. As depicted in Fig. 5.7, she can do this by sending out a probe state σ to Bob, whilst returning Alice's qubit state ρ back to her, unaffected[12]. In this scheme, Eve can access as much information as she wants about Bob's key without affecting $P_{\text{error}}^{\text{same}}$. However, this strategy would also result in $P_{\text{error}}^{\text{diff}} = 0 \neq 1/2$, thereby allowing Alice to detect Eve. This is, of course, an extreme case: Eve could attempt to find out which measurement Bob performed and induce errors using some operation $\mathcal{E}$ on ρ to increase $P_{\text{error}}^{\text{diff}}$. For instance, Eve could prepare and measure her probe state σ in the same basis, say $\{|\pm\rangle\langle\pm|\}$. If Eve does this, and measures something different to what she prepared when she receives it back from Bob, she can conclude with certainty that Bob measured in the z-basis. When this happens, she could act on Alice's state ρ with σ_z (i.e. taking $\mathcal{E}$ in Fig. 5.7 to be the Pauli-z unitary channel), inducing an error if $\rho \in \{|\pm\rangle\langle\pm|\}$, whilst leaving ρ unaltered if $\rho \in \{|0/1\rangle\langle 0/1|\}$. Although this leaves $P_{\text{error}}^{\text{same}}$ at its expected value, the probability $P_{\text{error}}^{\text{diff}}$ is only $1/4$ in this case, and not the required $1/2$. Of course, more general correlations between Eve's probe state σ, and how she acts on Alice's state ρ are possible. That being said, we found no strategy that allowed for Eve to extract information whilst leaving both $P_{\text{error}}^{\text{same}}$ and $P_{\text{error}}^{\text{diff}}$ unaltered. We leave the full analysis of this scenario for future work.

So, are there any differences between the definite and indefinite causal cases? Perhaps a slight difference lies in how often we can use a key bit, whilst simultaneously monitoring for eavesdroppers. Until now in the ICO case, we have not been utilising the fact that the target qubit (initially in the state ρ) ends up back in Alice's lab and can therefore be remeasured. To describe this situation, as shown in Fig. 5.8, let Alice's lab be made up of three quantum cryptographers: Alice 1, Alice 2 and Alice 3. Now, suppose Alice 1 prepares a state ρ in one basis (either x or z as always) $\mathcal{V} = \{|i\rangle\}$, Alice 2 performs an intermediate measurement (when in an indefinite causal order) in the corresponding mutually unbiased basis $\mathcal{V}' := \{H|i\rangle \mid |i\rangle \in \mathcal{V}\}$, and Alice 3 measures the returned state in the original basis $\mathcal{V}$. Once finished, the Alices compare bases with Bob who measures independently and randomly in the basis $\mathcal{W}$, which is, once again, either the x or z basis. Focusing on how Alice 2 and Bob's bases relate to one another, there are three possibilities to note:

1. Bob and Alice 2 *agree* on their bases: $\mathcal{W} = \mathcal{V}'$. This happens with probability $p_1 = 1/2$.
2. Bob and Alice 2 *disagree* on their bases: $\mathcal{W} \neq \mathcal{V}'$, *and* Alice 3's outcome *agrees* with the state Alice 1 prepared. This happens with probability $p_2 = 1/4$.
3. Bob and Alice 2 *disagree* on their bases: $\mathcal{W} \neq \mathcal{V}'$, *and* Alice 3's outcome *disagrees* with the state Alice 1 prepared. This happens with probability $p_3 = 1/4$.

The probabilities stated follow from Eq. (5.8).

[10] For example, suppose Alice prepares the state $|-\rangle\langle-|$ and Bob measures it in the basis $\{|\pm\rangle\langle\pm|\}$. Since $\langle+|-\rangle = 0$, Bob is guaranteed to obtain an outcome of $-$, and therefore send the state $|-\rangle\langle-|$ back to Alice. So, when Alice goes to measure this state in the basis she prepared it in: $\{|\pm\rangle\langle\pm|\}$, she will always obtain a result of $-$. In other words, she will never register an error.

[11] For example, suppose Alice prepares the state $|0\rangle\langle 0|$ and Bob measures in the basis: $\{|\pm\rangle\langle\pm|\}$. Then the state Alice receives

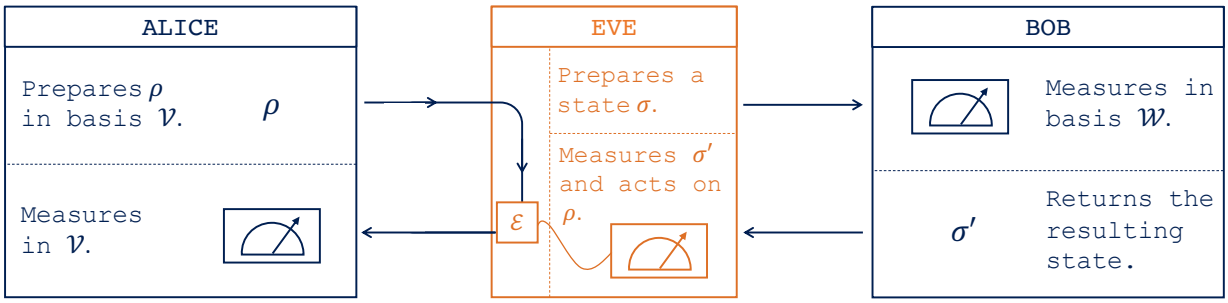

Figure 5.7: Eavesdropping strategy allowing for Alice's state to be returned to her unaffected whilst letting Eve learn something about Bob's key. If the probability $P_{\text{error}}^{\text{same}}$ is left unaltered at its expected value of zero, we found no strategy that allowed the probability $P_{\text{error}}^{\text{diff}}$ to remain at its expected value of 1/2.

Suppose there are no eavesdroppers. In the first of these possibilities, when $\mathcal{W} = \mathcal{V}'$, it can be shown, again via Eq. (5.8), that Bob's measurement result must agree with that of Alice 2, *and* the control qubit is guaranteed to be in the state $|+\rangle\langle+|$. Considering the second possibility, when $\mathcal{W} \neq \mathcal{V}'$, since Alice 3's measurement outcome agrees with the state Alice 1 prepared, it follows that Bob must agree with Alice 1 and 3. To understand this, suppose, for example, Alice 1 prepares the state $\rho = |k\rangle\langle k|$ and Alice 3 measures k for some $|k\rangle \in \mathcal{V}$. The fact that $\mathcal{W} \neq \mathcal{V}'$ means Bob also measured in $\mathcal{V}$. When we restrict Eq. (5.8) to this scenario, and apply Alice 3's measurement operator $|k\rangle\langle k|$, we find that the only option is for Bob to have also obtained an outcome of k. Similar analysis applied to the third possibility above tells us that we *cannot* deduce anything about Bob's measurement outcome when Alice 1 and Alice 3 disagree. Having said this, in both the second and third cases, eavesdroppers can still be monitored for by taking note of how often we measure the control qubit to be $+$ or $-$: when there are no eavesdroppers, we'd expect the probability of measuring a $+$ to be 3/4, whereas the probability of a $-$ should be 1/4. Any deviation from these indicates the presence of an eavesdropper (again, asssuming noiseless and lossless transmission). The probabilities quoted for the $\pm$ outcomes can, once again, be found using Eq. (5.8). So overall, whilst simultaneously watching for eavesdroppers, $p_1 + p_2 = 3/4$ of the qubits that Alice's lab sends can be used in the key, in the ideal case.

Comparing this with the aforementioned definite causal case, Alice can only monitor for eavesdroppers when she prepares and measures in the same basis. Therefore, whenever her and Bob's basis choice does not coincide, they must discard that case. So overall, whilst simultaneously watching for eavesdroppers, 1/2 of the qubits that Alice sends can be used, in the ideal case, which is less than the indefinite causal case. This argument is perhaps not surprising: in comparison to the definite causal case, the indefinite one uses an extra qubit and an extra measurement, along with the coherence required for causal orders to be in the controlled superposition. An alternate avenue to explore in terms of differences arising by using ICO, is to consider, in more depth, the security of such a protocol. Intuitively, one might expect there to be some difference due to the coherence that eavesdroppers must preserve in order to go undetected. This, however, is beyond the scope of this thesis.

5.5.2 Definite causal ordered protocol: option two

Another direction to consider what happens when we use the circuit depicted in Fig. 5.9 (once again relaxing the earlier requirement that Alice acts once on the system), where Alice and Bob's operations ($\mathcal{A}, \mathcal{B}$ respectively) are the same choice of x and z measurements as always. In this scenario, the target qubit T would be sent to Bob and then back to Alice, while the control qubit C stays in Alice's lab. The Kraus operators describing the evolution through this circuit are given by

$$S_{jj'k} = B_k A_j \otimes |0\rangle\langle 0| + A_{j'} B_k \otimes |1\rangle\langle 1|, \tag{5.45}$$

from Bob is $\mathbb{1}/2$, meaning that when Alice measures this in her original basis $\{|0/1\rangle\langle 0/1|\}$, the probability she measures the state to be different to the one she prepared is $\langle 1|\mathbb{1}|1\rangle/2 = 1/2$.

[12] In Fig. 5.7 this would correspond to setting the operation $\mathcal{E}$ equal to the identity $\mathcal{I}$.

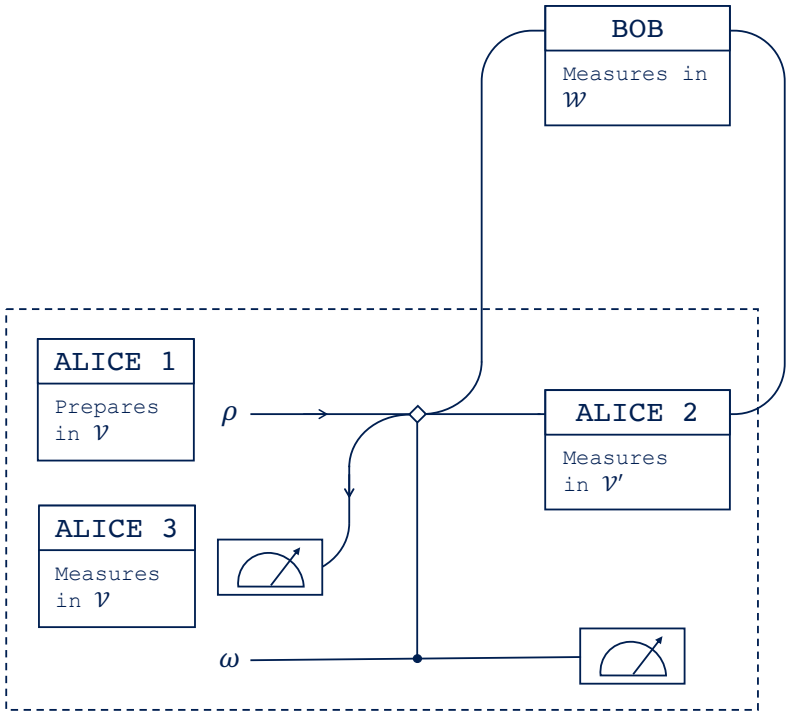

Figure 5.8: Adapted indefinite causal key distribution protocol that takes into account Alice's ability to remeasure ρ when it is returned to her lab. To simplify discussions, we split Alice's lab into three parts, run by three people: Alice 1, Alice 2 and Alice 3. The bases $\mathcal{V}, \mathcal{V}', \mathcal{W}$ can each be either the x or z-basis, such that $\mathcal{V}, \mathcal{W}$ are randomly and independently chosen, but $\mathcal{V}, \mathcal{V}'$ are mutually unbiased.

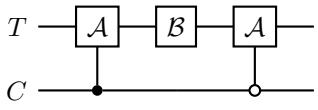

Figure 5.9: Possible implementation of ICKD in a definite causal order. Here, T labels the target qubit, sent to Bob and then back to Alice, and C the control, that lives in Alice's lab throughout.

where $\{A_j\}$ ($\{B_k\}$) are the Kraus operators of Alice's (Bob's) measurement operation $\mathcal{A}, (\mathcal{B})$. Since we only keep the cases in which Alice and Bob work in the same basis, the only terms that ultimately survive are those in which $j = k = j'$. Therefore, when there are no eavesdroppers, this situation is just as we found in the ICO case in that the control qubit C (if initially prepared in the state $|+\rangle$) would never be measured to be $|-\rangle$ at the end of the protocol.

Without going into full detail here, there is a difference (with respect to the ICO case) when an eavesdropper is introduced. For example, consider the situation, depicted in Fig. 5.10, of a single eavesdropper being introduced. The Kraus operators describing this situation are given by

$$S_{ii'jk} = A_i E_j B_k \otimes |0\rangle\langle 0| + E_j B_k A_{i'} \otimes |1\rangle\langle 1|, \tag{5.46}$$

where Eve's operation $\mathcal{E}$ is described by the Kraus operators $\{E_j\}$. This cannot be written in a similar way to Eq. (5.13):

$$\begin{aligned} S_{ii'jk} &= \frac{1}{2}(A_i E_j B_k + E_j B_k A_{i'}) \otimes \mathbb{1} + \frac{1}{2}(A_i E_j B_k - E_j B_k A_{i'}) \otimes \sigma_z \\ &\neq \frac{1}{2}(A_i E_j B_k + B_k E_j A_{i'}) \otimes \mathbb{1} + \frac{1}{2}(A_i E_j B_k - B_k E_j A_{i'}) \otimes \sigma_z, \end{aligned} \tag{5.47}$$

perhaps indicating the possibility of different eavesdropping scenarios and security analyses. We leave this for future work.

5.6 Conclusion and discussion

In this chapter we explored the idea of performing the QKD protocol BB84 in an indefinite causal regime. We defined a protocol that achieves this by performing projective measurements in an indefinite causal order. In doing so, we found that, with the use of indefinite causal order, it is possible to detect eavesdroppers during a QKD task *without* publicly comparing any subset of a shared private key between the two parties involved, Alice and Bob. We found that this could be achieved using a second system that acts as the control in inducing the indefinite causal ordering. In contrast to one-way QKD protocols, but similarly to two-way protocols, there are two locations eavesdroppers can reside, allowing for cooperative attacks. These have both been considered and the security against a class of individual attacks by the eavesdroppers was proved. Further, it was shown (in Appendix 5.A) that, when working in the indefinite causal structure chosen by the sharing parties, correlated eavesdroppers cannot extract any useful information about the key without inducing a non-zero detection probability, at least when they act on each distributed state individually. Having said this, and contrary to the past literature we are aware of, we tow possible ways of privately detecting eavesdroppers using a two-way protocol in a definite causal order. To do this, an extra instance of Alice's operation was required, a property consistent with other discussions of indefinite versus definite causal orderings [11]. We noted a possible difference between the definite and indefinite cases which may merit further study, but did not, in this work, find a benefit to applying ICO to QKD, at least in they way considered here.

Finally, we note that the ICO protocol would be challenging to realise experimentally due to the requirement to preserve coherence between the two causal orderings over the distance of communication. This could however have benefits in that eavesdroppers have to be very careful not to deduce the causal order of how the key bit is distributed in order to maintain the coherence of causal orderings. We conclude with a brief discussion of the practical limitations on this protocol. One difficulty lies in that ρ must go through (projective) measurement apparatuses and carry on around the loop while simultaneously doing the same

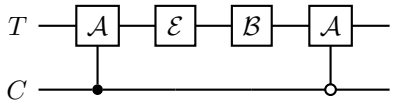

Figure 5.10: Possible implementation of ICKD in a definite causal order with a single eavesdropper.

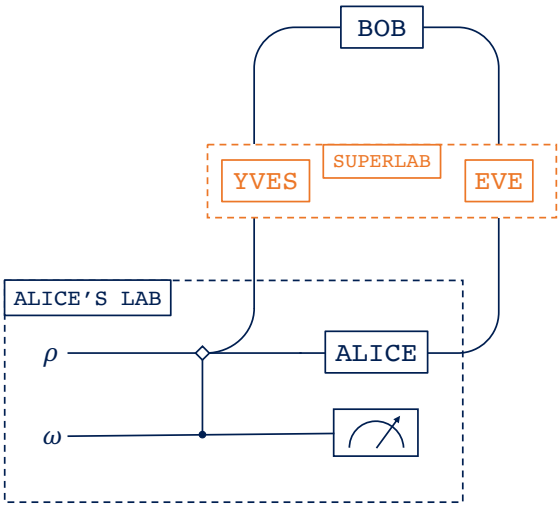

Figure 5.11: Indefinite causal quantum key distribution with fully correlated eavesdroppers Eve and Yves.

in the opposite direction along the same loop. However, the results of this protocol could be simulated using linearly polarised light, a Sagnac interferometer and some polarising filters. The Sagnac interferometer creates the indefinite causal order[13] and the polarising filters can be orientated in various different ways to correspond to each of Alice and Bob's measurement outcomes. More details are included in Appendix 5.B.

When it comes to practicality, consider using a Sagnac interferometer or something similar to create an indefinite causal ordering of operations. In order for the ICO to be legitimate, the coherence length of the light used must be considerably larger than the path length of the interferometer [13], perhaps indicating a limit to how practical such a protocol would be. Another limitation becomes apparent when we notice that two qubits are required to distribute one key bit securely, compared to BB84's one qubit. Perhaps this second, control state could find a secondary use beyond determining the presence of eavesdroppers, but we leave this consideration for future work. Finally, we note that the effects of noise and loss on this protocol have not been considered here. Indeed, being similar in nature to two-way protocols, they are likely to have a substantial impact (in comparison to one-way protocols). Having said this, there is evidence that noise behaves counter-intuitively in the indefinite causal regime, with noise being reduced in certain scenarios [122]. Analysing the affects of noise and loss is vital for understanding the practicality of this protocol, but is beyond the scope of this work.

Appendix 5.A Fully correlated eavesdroppers

Let us consider the situation in which our eavesdroppers Eve and Yves can work together with the help of both classical and quantum correlations to perform individual attacks. In order to do this, it is convenient to use the process matrix formalism [134]. To utilise this technique, we reinterpret the Hilbert space $\mathcal{H}^X$ (where $X \in \{A, B, E, Y\}$) of the system passing through the labs of Alice, Bob, Eve and Yves as two spaces $\mathcal{H}^{X_I}, \mathcal{H}^{X_O}$ which correspond to the Hilbert spaces of the system incoming to and outgoing from the lab X respectively. We can then employ the Choi-Jamiołkowski (CJ) isomorphism which details a correspondence between completely positive (CP) maps $\mathcal{X} : \mathcal{L}(\mathcal{H}^{X_I}) \to \mathcal{L}(\mathcal{H}^{X_O})$ and positive semi-definite operators $M^X \in \mathcal{L}(\mathcal{H}^{X_I}) \otimes \mathcal{L}(\mathcal{H}^{X_O})$, where $\mathcal{L}(\mathcal{H}^X)$ denotes the space of linear operators on $\mathcal{H}^X$. Explicitly,

$$M^X = (\mathcal{I} \otimes \mathcal{X})(|\mathbb{1}\rangle\!\rangle^{X_I X_I'} \langle\!\langle \mathbb{1}|^{X_I X_I'}) \tag{5.48}$$

where $|\mathbb{1}\rangle\!\rangle^{AB} = \sum_j |jj\rangle^{AB}$ with $j \in \{0, 1\}$ for our purposes, and the primed superscript X_I' indicates that the space $\mathcal{H}^{X_I'}$ is a copy of $\mathcal{H}^{X_I}$. The channel $\mathcal{X}$ can be recovered using

$$\mathcal{X}(\rho) = \mathrm{Tr}_{X_I}\left[(\rho^T \otimes \mathbb{1})M^X\right] \tag{5.49}$$

[13] Provided the coherence length of the light used is large enough.

for some state ρ, where the superscript T denotes the transpose with respect to the $\{|0\rangle, |1\rangle\}$ basis. Since we require each lab to obey quantum mechanics locally, to keep things as general as possible, one might expect that the CP maps we consider make up *quantum instruments*.

As discussed in Sec. 2.2.5, a quantum instrument is the most general description of a quantum measurement. Following [12], they are a sets of CP trace-non-increasing maps $\{\mathcal{M}_i^X\}$ such that each i corresponds to some measurement outcome. Writing $\mathcal{M}_i^X$ in the Kraus representation, with Kraus operators $\{E_j^{(i)}\}_j$, if we were to measure some state σ and obtain the outcome i, the state would update to $\mathcal{M}_i^X(\sigma) = \sum_j E_j^{(i)} \sigma E_j^{(i)\dagger}$, such that $\sum_j E_j^{(i)\dagger} E_j^{(i)} \leq \mathbb{1}$ and $\sum_{i,j} E_j^{(i)\dagger} E_j^{(i)} = \mathbb{1}$. In what follows, however, it turns out that we only require quantum instruments such that each measurement outcome corresponds to a channel described by a *single* Kraus operator. In other words, in the above notation, for each i, there is a single j.

For our situation, (depicted in Fig. 5.11) we have the labs of Alice, Bob, Eve and Yves. Further to this, and following [134, 136], we think of there being another lab C that takes in the target and control states at the end of the process. That is, we think of this space as being composed from a target component and control component respectively: $\mathcal{H}^{C_t} \otimes \mathcal{H}^{C_c}$. Analogously to [134, 136], we use the process matrix to encode the causal structure of the setup shown in Fig. 5.11. If we input a pure state $\rho = |\psi\rangle\langle\psi|$ with control state $\omega = |+\rangle\langle+|$, the process matrix we use is $W = |w\rangle\langle w|$ where

$$|w\rangle = \frac{1}{\sqrt{2}}\big(|\psi\rangle^{Y_I}|\mathbb{1}\rangle\!\rangle^{Y_O B_I}|\mathbb{1}\rangle\!\rangle^{B_O E_I}|\mathbb{1}\rangle\!\rangle^{E_O A_I}|\mathbb{1}\rangle\!\rangle^{A_O C_t}|0\rangle^{C_c} + |\psi\rangle^{A_I}|\mathbb{1}\rangle\!\rangle^{A_O E_I}|\mathbb{1}\rangle\!\rangle^{E_O B_I}|\mathbb{1}\rangle\!\rangle^{B_O Y_I}|\mathbb{1}\rangle\!\rangle^{Y_O C_t}|1\rangle^{C_c}\big). \tag{5.50}$$

Intuitively, the CJ isomorphism says that one can think of the temporal evolution of a state through a channel from $\mathcal{L}(\mathcal{H}^{X_I})$ to $\mathcal{L}(\mathcal{H}^{X_O})$ as a spatial teleportation of the state between the same two spaces. Therefore, we can intuitively think of the process matrix as providing the route by which $|\psi\rangle$ is teleported to $\mathcal{H}^{C_t}$.

Let us now write down the positive semidefinite operators that describe each lab's channel. For Alice and Bob, being independent, these are given by

$$\begin{aligned} M^X &= (\mathcal{I} \otimes \mathcal{X})(|\mathbb{1}\rangle\!\rangle^{X_I X_I'}\langle\!\langle\mathbb{1}|^{X_I X_I'}) \\ &= \sum_{i,j,k} (|i\rangle\langle j|)^{X_I} \otimes (X_k|i\rangle\langle j|X_k^\dagger)^{X_O}, \end{aligned} \tag{5.51}$$

where $X \in \{A, B\}$ and $X_k \in \{A_k, B_k\}$ are the Kraus operators defining the channel $\mathcal{X} \in \{\mathcal{A}, \mathcal{B}\}$. Remember that Alice and Bob's channels are the same, we just give them different labels here to make the setup clearer. Contrarily to Alice and Bob, Eve and Yves don't necessarily act independently from one another. As shown in Fig. 5.11, we can think of Eve and Yves as belonging to some "superlab" (with CJ operator, channel and Kraus operators denoted using $M^Z, \mathcal{Z}, Z_k$ respectively) which acts on the space $\mathcal{L}(\mathcal{H}^{Y_I}) \otimes \mathcal{L}(\mathcal{H}^{Y_O}) \otimes \mathcal{L}(\mathcal{H}^{E_I}) \otimes \mathcal{L}(\mathcal{H}^{E_O})$ using

$$M^Z = (\mathcal{I}^{Y_I E_I} \otimes \mathcal{Z}^{Y_I' E_I'})(|\mathbb{1}\rangle\!\rangle^{Y_I Y_I'}\langle\!\langle\mathbb{1}|^{Y_I Y_I'} \otimes |\mathbb{1}\rangle\!\rangle^{E_I E_I'}\langle\!\langle\mathbb{1}|^{E_I E_I'}) \tag{5.52}$$

$$= \sum_{i,j,k,l,m} (|ik\rangle\langle jl|)^{Y_I E_I} \otimes (Z_m|ik\rangle\langle jl|Z_m^\dagger)^{Y_O E_O}. \tag{5.53}$$

It turns out that this quantum instrument is of a more general form that what is physically possible. To see this, consider the most general physical scenario in which Yves and Eve share a, possibly entangled, ancilliary quantum state $\tau^{P_Y P_E} \in \mathcal{L}(\mathcal{H}^{P_Y} \otimes \mathcal{H}^{P_E})$ that encodes the correlations between their locally carried out quantum instruments. Here P_Y (P_E) labels the part of the ancilliary space contained in Yves's (Eve's) lab. Then each eavesdropper is allowed to carry out a quantum instrument $\{\mathcal{M}_i^X\}$ on the space $\mathcal{L}(\mathcal{H}^{X_I}) \otimes \mathcal{L}(\mathcal{H}^{P_X})$. Now, by the Stinespring dilation theorem, any quantum instrument on some system $\mathcal{S}$ can be represented as a joint unitary on $\mathcal{S}$ together with some ancilliary system $\mathcal{P}$ followed by a projective measurement on $\mathcal{P}$. Therefore, instead of considering $\{\mathcal{M}_i^X\}$, we can consider some unitary map $\mathcal{U}^{X_I P_X} : \mathcal{L}(\mathcal{H}^{X_I}) \otimes \mathcal{L}(\mathcal{H}^{P_X}) \to \mathcal{L}(\mathcal{H}^{X_O}) \otimes \mathcal{L}(\mathcal{H}^{P_X})$, where, since $\mathcal{H}^{P_X}$ is arbitrary, we have absorbed the extra degrees of freedom required for the Stinespring dilation into it.

We can now see how this scenario relates to the "superlab" formulation by observing how some quantum

state σ, passing through Eve and Yves's labs, evolves:

$$\begin{aligned}\tilde{\mathcal{Z}}(\sigma^{Y_I E_I}) &= \mathrm{Tr}_{P_Y P_E}\left[\mathcal{U}^{Y_I P_Y} \circ \mathcal{V}^{E_I P_E}(\sigma^{Y_I E_I} \otimes \tau^{P_Y P_E})\right] \\ &= \mathrm{Tr}_{P_Y P_E}\left[U^{Y_I P_Y} V^{E_I P_E}(\sigma^{Y_I E_I} \otimes \tau^{P_Y P_E}) U^{Y_I P_Y\,\dagger} V^{E_I P_E\,\dagger}\right].\end{aligned} \tag{5.54}$$

Here, Yves's effects are described by the map and corresponding (unitary) Kraus operator $\mathcal{U}^{Y_I P_Y}, U^{Y_I P_Y}$ respectively and Eve's by $\mathcal{V}^{E_I P_E}, V^{E_I P_E}$. Also, note that we have written $\tilde{\mathcal{Z}}$ to distinguish this physical scenario from the "superlab" scenario described by $\mathcal{Z}$. Now, using the operator-Schmidt decomposition [137, 138], we can write

$$U^{Y_I P_Y} = \sum_i \alpha_i G_i^{Y_I} \otimes H_i^{P_Y}, \tag{5.55a}$$

$$V^{E_I P_E} = \sum_j \beta_i Q_j^{E_I} \otimes R_j^{P_E}, \tag{5.55b}$$

where $\alpha_i, \beta_j \geq 0$ and $G_i^{Y_I}, H_i^{P_Y}, Q_j^{E_I}, R_j^{P_E}$ are operators whose specific properties aren't required for this argument. Finally, noting that, given a large enough ancilliary space, $\tau^{P_Y P_E} = |\tau\rangle\langle\tau|$, Eq. (5.54) can be rewritten as

$$\begin{aligned}\tilde{\mathcal{Z}}(\sigma^{Y_I E_I}) &= \sum_n \left(\sum_{i,j} \alpha_i \beta_j \langle n| \left[H_i^{P_Y} \otimes R_j^{P_E}\right] |\tau\rangle \left[G_i^{Y_I} \otimes Q_j^{E_I}\right] \right) \sigma^{Y_I E_I} \\ &\qquad \times \left(\sum_{i',j'} \alpha_{i'} \beta_{j'} \langle n| \left[H_{i'}^{P_Y} \otimes R_{j'}^{P_E}\right] |\tau\rangle \left[G_{i'}^{Y_I} \otimes Q_{j'}^{E_I}\right] \right)^\dagger \\ &= \sum_n Z_n \sigma^{Y_I E_I} Z_n^\dagger\end{aligned} \tag{5.56}$$

where $\{|n\rangle\} \subset \mathcal{H}^{P_Y} \otimes \mathcal{H}^{P_E}$ is some complete basis used for the partial trace. It follows that any physical situation described by correlated instruments, can described by this "superlab" formulation.

Let us now return to using the more general, less physical eavesdropping channel $\mathcal{Z}$. At this point, using similar logic to Eq. (5.49) and [134], we can find out what $\rho \otimes \omega$ becomes when put through the setup illustrated in Fig. 5.11:

$$\begin{aligned}\rho \otimes \omega &\to \mathrm{Tr}_{Y_I Y_O B_I B_O E_I E_O A_I A_O}\left[(M^Z \otimes M^A \otimes M^B \otimes \mathbb{I}^{C_t C_c})^T W\right] \\ &\xrightarrow[\text{comparison}]{\text{basis}} 2 \sum_{S \in B} \sum_i \sum_{j,k \in S} \langle\!\langle Z_i^* | \langle\!\langle A_j^* | \langle\!\langle B_k^* | (|w\rangle\langle w|) | Z_i^* \rangle\!\rangle | A_j^* \rangle\!\rangle | B_k^* \rangle\!\rangle,\end{aligned} \tag{5.57}$$

where,

$$\begin{aligned}|X_l^*\rangle\!\rangle &= (\mathbb{1} \otimes X_l^*)|\mathbb{1}\rangle\!\rangle^{X_I X_O} = \sum_{m \in \{0,1\}} |m\rangle^{X_I} X_l^* |m\rangle^{X_O}, \\ |Z_i^*\rangle\!\rangle &= (\mathbb{I} \otimes Z_i^*)|\mathbb{1}\rangle\!\rangle^{Y_I Y_O} |\mathbb{1}\rangle\!\rangle^{E_I E_O} = \sum_{m,n \in \{0,1\}} |mn\rangle^{Y_I E_I} Z_i^* |mn\rangle^{Y_O E_O},\end{aligned} \tag{5.58}$$

for $X \in \{A, B\}$, X^* indicates the complex conjugate of X, and the factor of 2 comes from requiring normalisation. Using these, $\omega = |+\rangle\langle+|$, and Eq. (5.50) for W, we can see, explicitly, that

$$\rho \otimes \omega \to \sum_{S \in B} \sum_i \sum_{j,k \in S} |f_{ijk}\rangle\langle f_{ijk}|^{C_t C_c}, \tag{5.59}$$

where,

$$|f_{ijk}\rangle^{C_t C_c} = \sum_{n \in \{0,1\}} \left[(\langle n| \otimes \mathbb{1})(B_k \otimes A_j) Z_i |\psi\rangle |n\rangle^{C_t} |0\rangle^{C_c} + (\mathbb{1} \otimes \langle n|) Z_i (B_k \otimes A_j) |n\rangle^{C_t} |\psi\rangle |1\rangle^{C_c}\right]. \tag{5.60}$$

We can quickly check our sanity by considering the case when Eve and Yves are not present. That is, when $Z_i \propto \mathbb{1} \otimes \mathbb{1},\ \forall i$. Here, it turns out that

$$|f_{ijk}\rangle^{C_tC_c} \propto \frac{1}{\sqrt{2}}\left(A_jB_k|\psi\rangle^{C_t}|0\rangle^{C_c} + B_kA_j|\psi\rangle^{C_t}|1\rangle^{C_c}\right) \tag{5.61}$$

which is what we'd expect from a quantum switch with two operations [13].

Recall that earlier, we found that when no eavesdroppers are present, measuring the state of the control qubit C_c at the end in the $\{|\pm\rangle\}$ basis would always result in $+$. In other words, the probability of measuring $-$, denoted $P(-^{C_c})$ is zero. The question now is, if a correlated Eve and Yves are present, what form must Z_i have if $P(-^{C_c}) = 0$? And further, with this form of Z_i, can Eve and Yves extract information about the key being shared between Alice and Bob?

Theorem 5.A.1. *For any input state $|\psi\rangle$, $P(-^{C_c}) = 0$ if and only if*

$$Z_i = \sum_{\mu=0}^{3} r_i^{\mu}\sigma_\mu \otimes \sigma_\mu, \tag{5.62}$$

where $r_i^{\mu} \in \mathbb{C}\ \forall \mu, i$ and $(\sigma_0, \sigma_1, \sigma_2, \sigma_3) = (\mathbb{1}, \sigma_x, \sigma_y, \sigma_z)$.

Proof. First, assume that $P(-^{C_c}) = 0$, this means that

$$\sum_{S\in B}\sum_{i}\sum_{j,k\in S}\sum_{m\in\{0,1\}} \left|(\langle m|^{C_t}\langle -|^{C_c})|f_{ijk}\rangle^{C_tC_c}\right|^2 = 0 \tag{5.63}$$

which implies that $(\langle m|^{C_t}\langle -|^{C_c})|f_{ijk}\rangle^{C_tC_c} = 0\ \forall j,k \in S, S \in B, m \in \{0,1\}$ and $\forall i$. Using Eq. (5.60), it follows that

$$\sum_{n\in\{0,1\}} (\langle n|\langle m|(B_k \otimes A_j)Z_i|\psi\rangle|n\rangle - \langle m|\langle n|Z_i(B_k \otimes A_j)|n\rangle|\psi\rangle) = 0, \tag{5.64}$$

$\forall j,k \in S, S \in B, m \in \{0,1\}$ and $\forall i$. Suppose we have an arbitrary, pure input state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ subject to $|\alpha|^2 + |\beta|^2 = 1$. If we show the theorem to be true for this case, it follows that it is true for any mixed state $\rho = \sum_\psi p_\psi|\psi\rangle\langle\psi|$ by the linearity of the theory. In order to achieve this, we first of all take $|\psi\rangle \neq |0\rangle, |1\rangle$, that is, $\alpha, \beta \neq 0$.

Note that Eq. (5.64) must hold for both $j,k \in \{0,1\}$ *and* $j,k \in \{+,-\}$. Let us first see what we can find out about Z_i when we take $j \in \{0,1\}$. In this case, Eq. (5.64) has the following form:

$$\delta_{jm}\left(\alpha\langle km|Z_i|0k\rangle + \beta\langle km|Z_i|1k\rangle\right) = (\alpha\delta_{j0} + \beta\delta_{j1})\langle mk|Z_i|kj\rangle. \tag{5.65}$$

When $j \neq m$, we can quickly see that $\langle 00|Z_i|01\rangle, \langle 01|Z_i|11\rangle, \langle 10|Z_i|00\rangle, \langle 11|Z_i|10\rangle = 0$. Next, when $m = j$, Z_i is constrained by

$$\alpha\langle km|Z_i|0k\rangle + \beta\langle km|Z_i|1k\rangle = (\alpha\delta_{m0} + \beta\delta_{m1})\langle mk|Z_i|km\rangle. \tag{5.66}$$

When $(k,m) = (0,0), (1,1)$ we find that $\langle 00|Z_i|10\rangle, \langle 11|Z_i|01\rangle = 0$ respectively. And, defining $e_i = \langle 10|Z_i|01\rangle$, $d_i = \langle 01|Z_i|10\rangle$, when $(k,m) = (0,1)$, it turns out that $\langle 01|Z_i|00\rangle = \frac{\beta}{\alpha}(e_i - d_i)$, and when $(k,m) = (1,0)$, $\langle 10|Z_i|11\rangle = \frac{\alpha}{\beta}(e_i - d_i)$. Here we can see why we have not allowed $\alpha = 0$ or $\beta = 0$.

Taking stock so far, Z_i has the form

$$Z_i = \begin{pmatrix} a_i & 0 & 0 & b_i \\ \frac{\beta}{\alpha}(e_i - d_i) & c_i & d_i & 0 \\ 0 & e_i & f_i & \frac{\alpha}{\beta}(e_i - d_i) \\ g_i & 0 & 0 & h_i \end{pmatrix}, \tag{5.67}$$

where all entries can be complex numbers. This can be simplified further by summing Eq. (5.64) over j and k. This results in

$$\sum_{n\in\{0,1\}} \langle nm|Z_i|\psi n\rangle = \sum_{n\in\{0,1\}} \langle mn|Z_i|n\psi\rangle, \tag{5.68}$$

which implies

$$\sum_{n\in\{0,1\}} \alpha\left(\langle nm|Z_i|0n\rangle - \langle mn|Z_i|n0\rangle\right) = \sum_{n\in\{0,1\}} \beta\left(\langle mn|Z_i|n1\rangle - \langle nm|Z_i|1n\rangle\right), \tag{5.69}$$

which must be true for all $m \in \{0,1\}$. Choosing $m = 0$ and using Eq. (5.67), we find that $d_i = e_i$. So, we therefore have

$$Z_i = \begin{pmatrix} a_i & 0 & 0 & b_i \\ 0 & c_i & d_i & 0 \\ 0 & d_i & f_i & 0 \\ g_i & 0 & 0 & h_i \end{pmatrix}. \tag{5.70}$$

To finish the derivation, we use the fact that Eq. (5.64) must also hold for $j,k \in \{+,-\}$. Using the Hadamard matrix $H = (\sigma_x + \sigma_z)/\sqrt{2} = H^\dagger$ to relate the x and z-bases, we replace $B_k \otimes A_j$ in Eq. (5.64) with $(H\otimes H)(B_k \otimes A_j)(H \otimes H)$, and after some rearranging, we find that

$$\begin{aligned}\sum_{n\in\{0,1\}} &[\delta_{k0} + (-1)^n\delta_{k1}]\langle kj|(H\otimes H)Z_i|\psi n\rangle \\ &= \frac{1}{2}\frac{(\alpha+\beta)\delta_{j0} + (\alpha-\beta)\delta_{j1}}{\delta_{j0} + (-1)^m\delta_{j1}} \sum_{n\in\{0,1\}} [\delta_{k0} + (-1)^n\delta_{k1}]\langle mn|Z_i(H\otimes H)|kj\rangle. \end{aligned}\tag{5.71}$$

Straight away, we can see that the RHS has a dependence on m but the LHS does not. So we can equate the $m = 0$ and $m = 1$ cases of the RHS. Doing this, the four cases that come from $k, j \in \{0,1\}$ result in

$$\begin{aligned} a_i &= h_i, \\ g_i &= b_i + c_i - f_i. \end{aligned}\tag{5.72}$$

Updating Z_i and looking at Eq. (5.71) when $(j,k,m) = (0,0,0)$ results in $c_i = f_i$ and $b_i = g_i$. Therefore we have

$$Z_i = \begin{pmatrix} a_i & 0 & 0 & b_i \\ 0 & c_i & d_i & 0 \\ 0 & d_i & c_i & 0 \\ b_i & 0 & 0 & a_i \end{pmatrix} \tag{5.73}$$

which can be rewritten as

$$Z_i = \frac{1}{2}\big[(a_i + c_i)\mathbb{1}\otimes\mathbb{1} + (d_i + b_i)\sigma_x\otimes\sigma_x + (d_i - b_i)\sigma_y\otimes\sigma_y + (a_i - c_i)\sigma_z\otimes\sigma_z\big]. \tag{5.74}$$

Further, since the mapping

$$\begin{cases} r_i^0 = a_i + c_i, \\ r_i^1 = d_i + b_i, \\ r_i^2 = d_i - b_i, \\ r_i^3 = a_i - c_i \end{cases}\tag{5.75}$$

is invertible and linear, $a_i, b_i, c_i, d_i \in \mathbb{C}$ being independent from one another implies that $r_i^\mu \in \mathbb{C}$ are independent from one another. Therefore,

$$Z_i = \sum_{\mu=0}^{3} r_i^\mu \sigma_\mu \otimes \sigma_\mu. \tag{5.76}$$

At this stage, one might notice that we didn't consider all the combinations of j,k in Eq. (5.71). It turns out that these give us no further constraints on Z_i. To confirm this, we just need to prove the reverse implication of the if and only if statement. If it turns out that we missed some constraints on Z_i, $P(-^{C_c})$ would be nonzero in general when using Eq. (5.76) for Z_i.

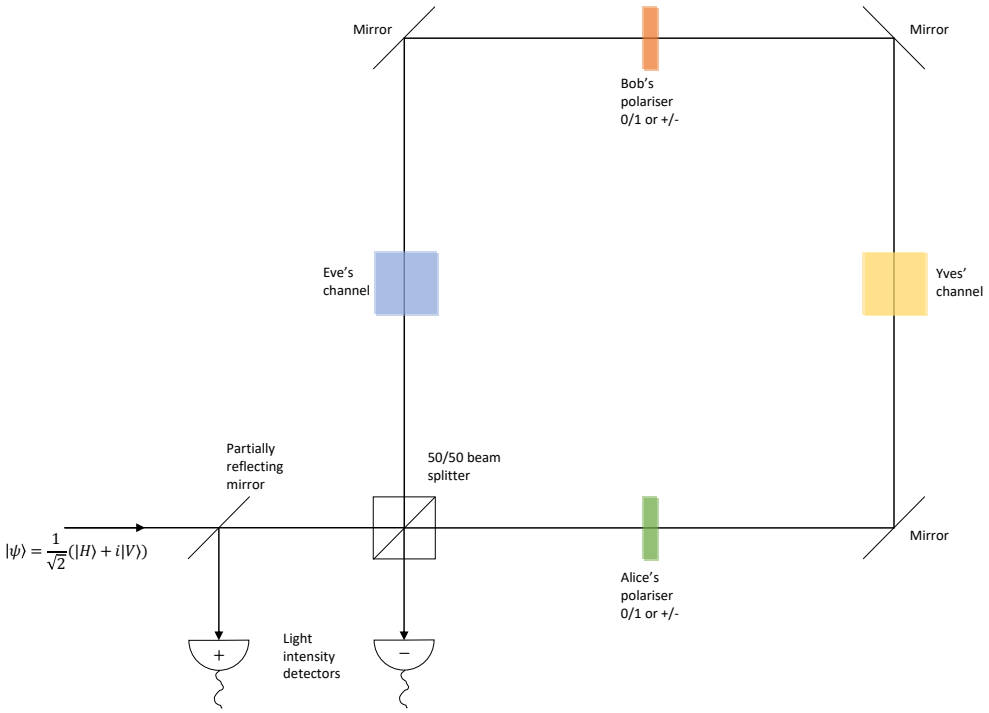

Figure 5.12: The results derived in this work can be simulated using polarised light to share a key between Alice and Bob, and a Sagnac interferometer to induce the indefinite causal order. Within the interferometer, polarising filters are orientated to correspond to all the valid measurement outcomes Alice and Bob obtain during the protocol.

So, suppose that Z_i is given by Eq. (5.76). Substituting this into $(\langle m|^{C_t}\langle -|^{C_c})|f_{ijk}\rangle^{C_tC_c}$ and carrying out the sum over n results in

$$(\langle m|^{C_t}\langle -|^{C_c})|f_{ijk}\rangle^{C_tC_c} = \sum_{\mu=0}^{3} r_i^{\mu}\langle m|[A_j, \sigma_\mu B_k \sigma_\mu]|\psi\rangle = 0 \tag{5.77}$$

for all $j, k \in S, S \in B, m \in \{0, 1\}$ and $\forall i$ since $[A_j, \sigma_\mu B_k \sigma_\mu] = 0\ \forall j, k, \mu$.

Finally, for the cases in which $|\psi\rangle \in \{|0\rangle, |1\rangle\}$, notice that what we have shown so far holds for $|\psi\rangle \in \{|+\rangle, |-\rangle\}$. Now, the process matrix defined using Eq. (5.50) can equivalently be be formulated in the x-basis, and Alice and Bob's measurements are invariant under this basis change. So, after converting everything to the x-basis, what was the situation in which $|\psi\rangle = |+/-\rangle$ becomes that of when $|\psi\rangle = |0/1\rangle$. Thus, since Z_i has the same form when it is changed from the z-basis to the x-basis, the result also holds for this case. □

It is difficult to have any intuition about what Eve and Yves's measurement would look like physically. A little can be gained, however, by considering what happens when only one of the coefficients is nonzero for each i. In this scenario, if one of Eve or Yves performs σ_i, then the other eavesdropper must do the same.

As discussed earlier, an ancilliary quantum state shared between Eve and Yves is likely necessary to understand what is happening here physically with regards to the correlations between the eavesdroppers' measurements. Either way, and to reiterate, since the approach taken here considers no physical constraints on the correlations between Eve and Yves, operations with physical correlations should exist as a subset of the ones we have derived here.

So, can Eve and Yves gain any information about Alice and Bob's shared key using Eq. (5.76)? To answer this, we calculate $P(Z_i, A_j, B_k) = \langle f_{ijk}|f_{ijk}\rangle$ for $j, k \in \{0, 1\}$ and $j, k \in \{+, -\}$. These are given by:

$$P(Z_i, A_j, B_k) = \begin{cases} \frac{|\langle j|\psi\rangle|^2}{2}\left(|r_i^0 + r_i^3|^2\delta_{jk} + |r_i^1 + r_i^2|^2\delta_{j\bar{k}}\right), & j, k \in \{0, 1\} \\ \frac{|\langle j|\psi\rangle|^2}{2}\left(|r_i^0 + r_i^1|^2\delta_{jk} + |r_i^2 + r_i^3|^2\delta_{j\bar{k}}\right), & j, k \in \{+, -\}, \end{cases} \tag{5.78}$$

where $\bar{k}$ denotes "not k". At first glance, it appears that Eve and Yves have access to some information about Alice and Bob's key. However, note first that distinguishing between the two cases of $j,k \in \{0,1\}$ and $j,k \in \{+,-\}$ is of no use as Alice and Bob publicly discuss which basis they measured in after they have done so. Secondly, although Eve and Yves could alter r_i^μ however they like, the only information they could gain is about whether each bit of Alice and Bob's key agree or not. Therefore, they can still do no better than a guess to determine the key. This intuitive argument is backed up by a calculation of the mutual information between the eavesdroppers and either Alice or Bob. In both cases, this turns out to be zero.

Finally, it should be noted this protocol has a weakness if we allow the eavesdroppers to act outwith the causal structure chose by Alice and Bob. Namely, Eve and Yves could perform an attack described in Sec. 5.5. That is, if the eavesdroppers return Alice's qubit unaffected, and in an indefinite causal order, whilst, independently sending out a probe state to Bob, they can learn about Bob's key bit, without inducing any "$-$" measurement results in the control mode. Having said this, it seems as though this eavesdropping strategy can be detected by monitoring ω in the cases when Alice and Bob disagree on their basis choice. The analysis of this idea is beyond the scope of this thesis.

Appendix 5.B Experimental simulation

Figure 5.12 shows a possible experimental setup to simulate some of the results derived. The idea is to use photon polarisation (in the horizontal, vertical basis, with $|H\rangle =: |0\rangle, |V\rangle =: |1\rangle$) as the target state ρ, initially in the state $|\psi\rangle\langle\psi|$, that is acted on by Alice, Bob, Eve and Yves. As is mentioned in the main text, if we wanted Alice and Bob to have approximately equal numbers of 0s and 1s, we can take our input state to be $\mathbb{1}/2$. This can be achieved by taking it to be $|i\rangle$ half of the time and $|-i\rangle$ the remainder of the time. These correspond to left and right circularly polarised light respectively: $|\psi\rangle = |\pm i\rangle = (|H\rangle \pm i|V\rangle)/\sqrt{2}$. The control state ω is taken to be the path degree of freedom induced by a beamsplitter. Using a 50/50 beamsplitter corresponds to taking $\omega = |+\rangle\langle+|$ with $|0\rangle$ corresponding to reflection and $|1\rangle$ to transmission.

Recall that Alice and Bob perform projective measurements in either the x or z-basis. This is difficult to do non-destructively and even more difficult to do while keeping the photon continuing around the Sagnac interferometer in its original superposition of paths. Having said this, it is possible to simulate projective measurements using polarisers. This means we can obtain the statistics that the measurements of Alice, Bob, Eve and Yves would have produced.

Explicitly, when Alice and Bob measure in the z-basis, we use polarisers orientated at 0 and $\pi/2$ which correspond to measurement outcomes of 0 and 1 respectively. Likewise, when measuring in the x-basis, polarisers being orientated at $\pm\pi/4$ correspond to measurement outcomes of $\pm$ respectively. The probability of Alice and Bob measuring i,j can be taken to be the ratio of the total intensity $I_{\text{exit}}(i,j)$ of light exiting the interferometer to that of it entering I_{enter}:

$$P(A_i, B_j) = \frac{I_{\text{exit}}(i,j)}{I_{\text{enter}}}. \tag{5.79}$$

Here, the dependence of $I_{\text{exit}}(i,j)$ on i,j highlights that the interferometer is setup with Alice and Bob's polarisers being orientated correspondingly to the measurement outcomes i,j respectively. Since Alice and Bob only keep measurement results when they have publicly confirmed that they measured in the same basis, there are eight permutations when ignoring Eve and Yves. These are given in the Table 5.1.

The key feature of this protocol involves the measurement of the control state in the $\pm$ basis. Noticing that, after going through the main part of the Sagnac interferometer, the path that the light exits the 50/50 beamsplitter along, is controlled by the path qubit in the x-basis. That is, the $|+\rangle$ component is transmitted through the beamsplitter, whereas the $|-\rangle$ component is reflected. Therefore, placing a detector in the reflected arm corresponds to the $-$ outcome and, after a partially reflecting mirror, a detector in the transmitted arm corresponds to the $+$ outcome. The probability of measuring the eavesdroppers comes from the probability of measuring the control qubit state to be $-$. Therefore, for each run of the experiment (each permutation of polariser angles), the ratio of the intensity in the $-$ arm to the total intensity exiting the interferometer is what is required. As a sanity check, this should always be zero when Eve and Yves are not present. As mentioned before, in order to exploit the features of indefinite causal order, the coherence length of the light used should be significantly longer than the path length of the interferometer. A laser can be used to achieve this.

Table 5.1: Table detailing the eight polariser orientations that correspond to the possible measurement outcomes that Alice and Bob can obtain when they measure in the same basis.

Alice polariser orientation	Bob polariser orientation
0	0
0	$\frac{\pi}{2}$
$\frac{\pi}{2}$	0
$\frac{\pi}{2}$	$\frac{\pi}{2}$
$\frac{\pi}{4}$	$\frac{\pi}{4}$
$\frac{\pi}{4}$	$-\frac{\pi}{4}$
$-\frac{\pi}{4}$	$\frac{\pi}{4}$
$-\frac{\pi}{4}$	$-\frac{\pi}{4}$

Chapter 6

Conclusion and outlook

There are hints that the field of machine learning may benefit from a collaboration with the quantum world. Many predict (or at least hope) that once we have a fully functioning quantum computer, we will be swimming in computational speedups and new found ways to probe and manipulate the quantum world directly. Whether true or not, there is another, equally interesting, side to the story: that of what the quantum world allows us to do with its data. In this thesis, we have been concerned with this latter point, and have explored limitations imposed by uniquely quantum phenomena. More specifically, we focused on the impact measurement disturbance has on the unsupervised learning of quantum data. Indeed, restricting our attention to the task of binary classification, the main question we asked in this work was: how does the classification of a subset of quantum data affect our ability to subsequently classify the whole dataset? We saw that, since a quantum classification could be thought of as a quantum measurement, the phenomenon of measurement disturbance makes this question less than trivial.

After reviewing the background theory relevant to this thesis in Chapter 2, in Chapter 3 we took our first steps towards understanding this sequential classification scenario by considering the base case of a three-qubit dataset. Here, our dataset consisted of three qubits that could each be in one of two unknown states. Our task was to, first, perform a binary classification on the first two qubits of the dataset and, second, classify the entire three-qubit dataset optimally. As mentioned, this protocol is closely related to sequential measurement [107–110] due to how these classifications can be thought of as quantum measurements. We found that this first classification on two-qubits impacted the ability of the second classification on three qubits in a non-trivial fashion. The relationship between their success rates was derived analytically [Eq. (3.51)] and plotted in Fig. 3.1. An interesting feature of this result was that, although the first classification did ultimately negatively impact the success rate of the second one, for a remarkably large range of strengths, the first classification did not force the second to deviate from its optimal probability of success. This realisation motivated the work carried out in Chapter 4. We concluded Chapter 3 by describing this sequential classification as a quantum circuit. Implementing this circuit using Qiskit's AerSimulater, we demonstrated the tradeoff of Eq. (3.51), plotting our results in Fig. 3.10.

Motivated by the realisation that an intermediate classification on a two-qubit subset need not affect the success rate of a classification on the entire three-qubit dataset, in Chapter 4, we set out to investigate whether the same could be said about a more general scenario. In particular, we set our sights on an n-qubit dataset that, once again, was made up of qubits that could each be in one of two unknown states. After reviewing the work of Sentís et al. [71] to understand how to perform an optimal classification on such a quantum dataset, we asked the question: what, and how much, can be learnt in a classification on the first $n-1$ qubits of the dataset *without* affecting the optimality of a subsequent classification on the entire n-qubit dataset? Before doing so, we noted some numerical results, found using semidefinite programming techniques, that seemed to suggest that nothing about the order of the first $n-1$ qubits could be found without affecting the n-qubit classification. It appeared that all could be learned was something about how many of each type of qubit there was. Equipped with the hint of this surprising feature, we made steps to prove that this is true for an $n-1 \to n$ qubit sequential binary classification. We fell short in two places: first, in proving Conjecture 4.A.1, and second, in that we did not attempt to prove the uniqueness of the optimal measurement we used for the undisturbed n-qubit classification. This second point just means that

our hypothesis is constrained to a fixed n-qubit measurement that shares the symmetries of the possible states of the dataset. Having said this, it would be more interesting to know if this measurement is unique or not. Aside from proving these two missing points, another intriguing future line of research would be to see how this hypothesised property generalises: given a fixed measurement Π which shares its symmetries with a set of quantum states R, does an intermediate measurement on R with a different goal have to be ignorant with regards to these symmetries if we don't want to affect the success rate of Π? Also in this chapter, we proved an interesting consequence of the hypothesis that nothing about the order of the first $n-1$ qubits can be learnt. Namely, that for $m > 1$, a measurement on the first $n-m$ qubits can't even tell us anything about the number of each type of qubit without affecting the subsequent classification. This hints that the disruption induced when learning about a subset of a quantum dataset is, in general, considerable. This realisation is surprising when compared to the $2 \to 3$-qubit case considered in Chapter 3 which allowed for a remarkable amount to be learnt during the two-qubit classification. Aside from the general discussions about which properties of the dataset could be learnt during an intermediate $(n-1)$-qubit classification, we derived a closed form, analytical lower bound [Eq. (4.133)] for the optimal success rate one could achieve in such an $(n-1)$-qubit classification without affecting the subsequent n-qubit one. Further, we hypothesised an algorithm to construct the measurement that realises this optimal value. We leave the determination of whether this is indeed the optimal method to future work.

In Chapter 5 we changed tack and turned our attention to the indefinite causal regime. Motivated by the connections between ICO and non-commutativity, we investigated how the original formulation of quantum key distribution, BB84 [4] (whose security is based on non-commuting observables), could be carried out in an indefinite causal order. We recalled that in BB84, two parties, Alice and Bob, share a key using quantum states belonging to two mutually unbiased bases. They can ensure they have securely shared a cryptographic key by monitoring for errors that, if listening in, an eavesdropping third party would necessarily induce. We highlighted that in order for these errors to be detected, Alice and Bob would have to publicly compare, and subsequently discard, a subset of their private key. Indeed, we noted that this public comparison is usually a feature of QKD, but we saw that if Alice and Bob shared their key in an indefinite causal order, which we showed to be possible using projective measurements, then they can detect eavesdroppers *without* performing this public comparison. We proved this protocol to be secure against the class of individual attacks considered in Ref. [129], and showed that, regardless of whether these eavesdroppers were correlated or not, if they extracted any useful information about the shared key, a non-zero probability of being detected would be induced. In deriving these results, we did, however, implicitly assume that the eavesdroppers had to adhere to the causal structure chosen by Alice and Bob. Further, we found a two-way QKD protocol that seemed to allow for a similar form of private detection. Despite noting that some more subtle differences between definite and indefinite causal QKD protocols may exist, we ultimately concluded that carrying out QKD in an ICO is unlikely to offer any advantage, at least in the way we considered.

As mentioned, the work we have explored on sequential quantum classifications offers many avenues to future work. Other than the points mentioned, there are many other ways our investigations could be generalised: for example, to d-dimensional qudits, to situations in which we have access to multiple copies of the quantum dataset, or perhaps by extending the learning task beyond binary classification, to allow for three or more possible states. Of particular interest to me would be to look more generally into how the symmetry of the states and measurements puts limitations on intermediate measurements. On the indefinite causal key distribution (ICKD) side of things, despite our null result, it would still be interesting to see more generally how the security of such a protocol compares to its definite causal counterpart. Looking into this ICKD idea allowed us to consider quantum measurement in an indefinite causal order, which is a line of research that is largely unexplored. It would be interesting to see whether this can find application somewhere else in quantum information science.

Bibliography

[1] G. A. D. Briggs, J. N. Butterfield, and A. Zeilinger. "The Oxford Questions on the foundations of quantum physics". *Proc. Math. Phys. Eng. Sci.* 469.2157 (2013).

[2] D. Dieks. "Communication by EPR devices". *Phys. Lett. A* 92.6 (1982).

[3] W. K. Wootters and W. H. Zurek. "A single quantum cannot be cloned". *Nature* 299.5886 (1982).

[4] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*. IEEE, New York, 1984.

[5] C. H. Bennett and S. J. Wiesner. "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states". *Phys. Rev. Lett.* 69.20 (1992).

[6] D. Deutsch and R. Jozsa. "Rapid solution of problems by quantum computation". *Proc. Math. Phys. Eng. Sci.* 439.1907 (1992).

[7] C. H. Bennett et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". *Phys. Rev. Lett.* 70.13 (1993).

[8] P. W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". *Proceedings 35th annual symposium on foundations of computer science*. IEEE. 1994.

[9] J. P. Dowling and G. J. Milburn. "Quantum technology: the second quantum revolution". *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 361.1809 (2003).

[10] C. A. Fuchs and A. Peres. "Quantum-state disturbance versus information gain: Uncertainty relations for quantum information". *Phys. Rev. A* 53 (1996).

[11] G. Chiribella et al. "Quantum computations without definite causal structure". *Phys. Rev. A* 88 (2013).

[12] O. Oreshkov, F. Costa, and Č. Brukner. "Quantum correlations with no causal order". *Nat. Commun.* 3.1092 (2012).

[13] K. Goswami et al. "Indefinite causal order in a quantum switch". *Phys. Rev. Lett.* 121.9 (2018).

[14] S. Roman. *Advanced linear algebra*. Vol. 3. Springer, 2005.

[15] K. Hoffmann and R. A. Kunze. *Linear algebra*. Prentice-Hall New Jersey, 1971.

[16] P. R. Halmos. *Finite-dimensional vector spaces*. Courier Dover Publications, 2017.

[17] M. A. Nielsen and I. Chuang. *Quantum computation and quantum information*. American Association of Physics Teachers, 2002.

[18] K. Landsman. *Foundations of quantum theory: From classical concepts to operator algebras*. Springer Nature, 2017.

[19] P. A. M. Dirac. *The Principles of Quantum Mechanics*. Oxford, Clarendon Press, 1930.

[20] J. von Neumann. *Mathematical foundations of quantum mechanics: New edition*. Vol. 53. Princeton university press, 2018.

[21] N. David Mermin. "What's wrong with this pillow?" *Physics Today* 42.4 (1989).

[22] S. Barnett. *Quantum information*. Vol. 16. Oxford University Press, 2009.

[23] M. M. Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[24] J. J. Sakurai. *Modern quantum mechanics revide edition*. Addison-Wesley Publishing Co., Inc., 1994.

[25] A. S. Holevo. *Probabilistic and statistical aspects of quantum theory*. Vol. 1. Springer Science & Business Media, 2011.

[26] J. C. Solem and L. C. Biedenharn. "Understanding geometrical phases in quantum mechanics: An elementary example". *Found. Phys.* 23.2 (1993).

[27] Benjamin Schumacher. "Quantum coding". *Phys. Rev. A* 51.4 (1995).

[28] G. Carcassi, L. Maccone, and C. A. Aidala. "Four postulates of quantum mechanics are three". *Phys. Rev. Lett.* 126.11 (2021).

[29] K. Kraus. *States, effects, and operations: fundamental notions of quantum theory*. Springer Verlag, 1983.

[30] S. Croke, S. M. Barnett, and S. Stenholm. "Linear transformations of quantum states". *Ann. Phys.* 323.4 (2008).

[31] A. Fujiwara and H. Imai. "Quantum parameter estimation of a generalized Pauli channel". *J. Phys. A* 36.29 (2003).

[32] E. B. Davies and J. T. Lewis. "An operational approach to quantum probability". *Commun. Math. Phys.* 17.3 (1970).

[33] G. Lüders. "Über die Zustandsänderung durch den Meßprozeß". *Ann. Phys. (Leipzig)* 443.5-8 (1950).

[34] H. Barnum. *arXiv preprint quant-ph/0205155* (2002).

[35] M. A. Naimark. "Spectral functions of a symmetric operator". *Izv. Akad. Nauk SSSR Ser. Mat.* 4 (1940).

[36] M. G. A. Paris. "The modern tools of quantum mechanics: A tutorial on quantum states, measurements, and operations". *Eur. Phys. J. Spec. Top.* 203.1 (2012).

[37] S. M. Barnett and S. Croke. "Quantum state discrimination". *Adv. Opt. Photonics* 1.2 (2009).

[38] J. Bae and L-C. Kwek. "Quantum state discrimination and its applications". *J. Phys. A* 48.8 (2015).

[39] J. A. Bergou. "Discrimination of quantum states". *J. Mod. Opt.* 57.3 (2010).

[40] C. H. Bennett, G. Brassard, and N. D. Mermin. "Quantum cryptography without Bell's theorem". *Phys. Rev. Lett.* 68.5 (1992).

[41] H. Barnum and E. Knill. "Reversing quantum dynamics with near-optimal quantum and classical fidelity". *J. Math. Phys.* 43.5 (2002).

[42] I. D. Ivanovic. "How to differentiate between non-orthogonal states". *Phys. Lett. A* 123.6 (1987).

[43] D. Dieks. "Overlap and distinguishability of quantum states". *Phys. Lett. A* 126.5-6 (1988).

[44] A. Peres. "How to differentiate between non-orthogonal states". *Phys. Lett. A* 128.1-2 (1988).

[45] S. Croke et al. "Maximum Confidence Quantum Measurements". *Phys. Rev. Lett.* 96 (2006).

[46] H. Lee et al. "Maximum-confidence measurement for qubit states". *Phys. Rev. A* 106 (2022).

[47] C. W. Helstrom. "Quantum detection and estimation theory". *J. Stat. Phys.* 1 (1969).

[48] J. Bae. "Structure of minimum-error quantum state discrimination". *New J. Phys.* 15.7 (2013).

[49] H. Wolkowicz, R. Saigal, and L. Vandenberghe. *Handbook of semidefinite programming: theory, algorithms, and applications*. Vol. 27. Springer Science & Business Media, 2012.

[50] P. Skrzypczyk and D. Cavalcanti. *Semidefinite programming in quantum information science*. IOP Publishing, 2023.

[51] A. S. Holevo. "Statistical decision theory for quantum systems". *J. Multivariate Anal.* 3.4 (1973).

[52] H. Yuen, R. Kennedy, and M. Lax. "Optimum testing of multiple hypotheses in quantum detection theory". *IEEE Trans. Inf. Theory* 21.2 (1975).

[53] G. Weir. "Optimal discrimination of quantum states". PhD thesis. University of Glasgow, 2018.

[54] S. M. Barnett and S. Croke. "On the conditions for discrimination between quantum states with minimum error". *J. Phys. A* 42.6 (2009).

[55] C. Mochon. "Family of generalized "pretty good" measurements and the minimal-error pure-state discrimination problems for which they are optimal". *Phys. Rev. A* 73.3 (2006).

[56] K. Hunter. "Optimal measurement strategies for mirror-symmetric states". *6th International Conference on Quantum Communication, Measurement and Computing*. Rinton Press. 2003.

[57] G. Weir, S. M. Barnett, and S. Croke. "Optimal discrimination of single-qubit mixed states". *Phys. Rev. A* 96 (2017).

[58] M. Ban et al. "Optimum measurements for discrimination among symmetric quantum states and parameter estimation". *Int. J. Theor. Phys.* 36 (1997).

[59] S. M. Barnett. "Minimum-error discrimination between multiply symmetric states". *Phys. Rev. A* 64.3 (2001).

[60] K. Hunter. "Measurement does not always aid state discrimination". *Phys. Rev. A* 68 (2003).

[61] Y. C. Eldar and G. D. Forney. "On quantum detection and the square-root measurement". *IEEE Trans. Inf. Theory* 47.3 (2001).

[62] G. Weir et al. "Optimal measurement strategies for the trine states with arbitrary prior probabilities". *Quantum Sci. Technol.* 3.3 (2018).

[63] E. Andersson et al. "Minimum-error discrimination between three mirror-symmetric states". *Phys. Rev. A* 65 (2002).

[64] D. S. Dummit and R. M. Foote. *Abstract algebra*. Vol. 3. Wiley, 2004.

[65] J-Q. Chen, J. Ping, and F. Wang. *Group representation theory for physicists*. World Scientific Publishing Co., 2002.

[66] R. Goodman and N. R. Nolan. *Symmetry, representations and invariants*. Springer, 2009.

[67] H. F. Jones. *Groups, representations and physics*. IOP Publishing Ltd., 1990.

[68] E. P. Wigner. *Group theory and its application to quantum mechanics of atomic spectra*. Academic Press, 1959.

[69] G. James and A. Kerber. *The representation theory of the symmetric group*. Cambridge University Press, 2009.

[70] A. W. Harrow. *arXiv preprint quant-ph/0512255* (2005).

[71] G. Sentís et al. "Unsupervised Classification of Quantum Data". *Phys. Rev. X* 9 (2019).

[72] D. Bacon, I. L. Chuang, and A. W. Harrow. "Efficient Quantum Circuits for Schur and Clebsch-Gordan Transforms". *Phys. Rev. Lett.* 97 (2006).

[73] R. Blume-Kohout, S. Croke, and D. Gottesman. "Streaming universal distortion-free entanglement concentration". *IEEE transactions on information theory* 60.1 (2013).

[74] D. H. Fremlin. *Measure theory*. Torres Fremlin, 2004.

[75] D. Williams. *Probability with martingales*. Cambridge University Press, 1991.

[76] A. A. Mele. "Introduction to Haar Measure Tools in Quantum Information: A Beginner's Tutorial". *arXiv preprint arXiv:2307.08956* (2023).

[77] H. Spencer-Wood, J. Jeffers, and S. Croke. "Measurement disturbance tradeoffs in three-qubit unsupervised quantum classification". *Phys. Rev. A* 105 (2022).

[78] V. Dunjko and H. J Briegel. "Machine learning & artificial intelligence in the quantum domain: a review of recent progress". *Rep. Prog. Phys.* 81.7 (2018).

[79] A. Hentschel and B. C. Sanders. "Machine learning for precise quantum measurement". *Phys. Rev. Lett.* 104.6 (2010).

[80] M. August and X. Ni. "Using recurrent neural networks to optimize dynamical decoupling for quantum memory". *Phys. Rev. A* 95.1 (2017).

[81] R. P. Feynman. "Simulating physics with computers". *Int. J. Theor. Phys.* 21.467 (1982).

[82] L. K. Grover. "A fast quantum mechanical algorithm for database search". *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996.

[83] S. Aaronson. "Read the fine print". *Nat. Phys.* 11.4 (2015).

[84] R. LaRose and B. Coyle. "Robust data encodings for quantum classifiers". *Phys. Rev. A* 102.3 (2020).

[85] H. Neven et al. "Training a binary classifier with the quantum adiabatic algorithm". *arXiv preprint arXiv:0811.0416* (2008).

[86] R. Babbush et al. "Construction of non-convex polynomial loss functions for training a binary classifier with quantum annealing". *arXiv preprint arXiv:1406.4203* (2014).

[87] K. L. Pudenz and D. A. Lidar. "Quantum adiabatic machine learning". *Quantum Inf. Process.* 12 (2013).

[88] A. W. Harrow, A. Hassidim, and S. Lloyd. "Quantum algorithm for linear systems of equations". *Phys. Rev. Lett.* 103.15 (2009).

[89] E. Aïmeur, G. Brassard, and S. Gambs. "Quantum speed-up for unsupervised learning". *Mach. Learn.* 90 (2013).

[90] N. Wiebe, D. Braun, and S. Lloyd. "Quantum Algorithm for Data Fitting". *Phys. Rev. Lett.* 109 (2012).

[91] S. Lloyd, M. Mohseni, and P. Rebentrost. "Quantum principal component analysis". *Nat. Phys.* 10.9 (2014).

[92] S. M. Barnett, A. Chefles, and I. Jex. "Comparison of two unknown pure quantum states". *Phys. Lett. A* 307.4 (2003).

[93] J. A. Bergou and M. Hillery. "Universal Programmable Quantum State Discriminator that is Optimal for Unambiguously Distinguishing between Unknown States". *Phys. Rev. Lett.* 94 (2005).

[94] M. Guţă and W. Kotłowski. "Quantum learning: asymptotically optimal classification of qubit states". *New J. Phys.* 12 (2010).

[95] M. Sasaki, A. Carlini, and R. Jozsa. "Quantum template matching". *Phys. Rev. A* 64 (2001).

[96] D. Akimoto and M. Hayashi. "Discrimination of the change point in a quantum setting". *Phys. Rev. A* 83 (2011).

[97] G. Sentís et al. "Quantum Change Point". *Phys. Rev. Lett.* 117 (2016).

[98] M. Fanizza et al. "Universal algorithms for quantum data learning". *EPL* 140.2 (2022).

[99] H-Y. Huang et al. "Quantum advantage in learning from experiments". *Science* 376.6598 (2022).

[100] A. Monras, G. Sentís, and P. Wittek. "Inductive supervised quantum learning". *Phys. Rev. Lett.* 118.19 (2017).

[101] A. Peres and W. K. Wootters. "Optimal detection of quantum information". *Phys. Rev. Lett.* 66 (1991).

[102] S. Massar and S. Popescu. "Optimal Extraction of Information from Finite Quantum Ensembles". *Phys. Rev. Lett.* 74 (1995).

[103] J. Calsamiglia et al. "Local Discrimination of Mixed States". *Phys. Rev. Lett.* 105 (2010).

[104] E. Chitambar and M-H. Hsieh. "Revisiting the optimal detection of quantum information". *Phys. Rev. A* 88 (2013).

[105] B. L. Higgins et al. "Multiple-copy state discrimination: Thinking globally, acting locally". *Phys. Rev. A* 83 (2011).

[106] S. Croke and S. M. Barnett. "Difficulty of distinguishing product states locally". *Phys. Rev. A* 95 (2017).

[107] J. Bergou, E. Feldman, and M. Hillery. "Extracting Information from a Qubit by Multiple Observers: Toward a Theory of Sequential State Discrimination". *Phys. Rev. Lett.* 111 (2013).

[108] M. Hillery and J. Mimih. "Sequential discrimination of qudits by multiple observers". *J. Phys. A Math* 50 (2017).

[109] D. Fields et al. "Extracting unambiguous information from a single qubit by sequential observers". *Phys. Rev. A* 101 (2020).

[110] L. Leppäjärvi and M. Sedlák. "Postprocessing of quantum instruments". *Phys. Rev. A* 103 (2021).

[111] E. Andersson and D. K. L. Oi. "Binary search trees for generalized measurements". *Phys. Rev. A* 77 (2008).

[112] J. Dressel, T. A. Brun, and A. N. Korotkov. "Implementing generalized measurements with superconducting qubits". *Phys. Rev. A* 90 (2014).

[113] L. A. Rozema et al. "Quantum Data Compression of a Qubit Ensemble". *Phys. Rev. Lett.* 113 (2014).

[114] A. Ambainis and J. Emerson. "Quantum t-designs: t-wise independence in the quantum world". *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*. IEEE. 2007.

[115] D. Bacon, I. L. Chuang, and A. W. Harrow. "The quantum Schur transform: I. efficient qudit circuits". *arXiv preprint quant-ph/0601001* (2005).

[116] H. Spencer-Wood. "Indefinite causal key distribution". *arXiv preprint arXiv:2303.03893* (2023).

[117] M. Araújo, F. Costa, and Č. Brukner. "Computational Advantage from Quantum Controlled Ordering of Gates". *Phys. Rev. Lett.* 113 (2014).

[118] P. A. Guérin et al. "Exponential Communication Complexity Advantage from Quantum Superposition of the Direction of Communication". *Phys. Rev. Lett.* 117 (2016).

[119] X. Zhao, Y. Yang, and G. Chiribella. "Quantum Metrology with Indefinite Causal Order". *Phys. Rev. Lett.* 124 (2020).

[120] D. Ebler, S. Salek, and G. Chiribella. "Enhanced Communication with the Assistance of Indefinite Causal Order". *Phys. Rev. Lett.* 120 (2018).

[121] N. Loizeau and A. Grinbaum. "Channel capacity enhancement with indefinite causal order". *Phys. Rev. A* 101 (2020).

[122] G. Chiribella et al. "Indefinite causal order enables perfect quantum communication with zero capacity channels". *New J. Phys.* 23.3 (2021).

[123] D. Felce and V. Vedral. "Quantum Refrigeration with Indefinite Causal Order". *Phys. Rev. Lett.* 125 (2020).

[124] A. Z. Goldberg, K. Heshami, and L. L. Sánchez-Soto. "Evading noise in multiparameter quantum metrology with indefinite causal order". *Phys. Rev. Res.* 5 (2023).

[125] A. K. Ekert. "Quantum cryptography based on Bell's theorem". *Phys. Rev. Lett.* 67 (1991).

[126] W-Y. Hwang. "Quantum key distribution with high loss: toward global secure communication". *Phys. Rev. Lett.* 91.5 (2003).

[127] V. Scarani et al. "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations". *Phys. Rev. Lett.* 92.5 (2004).

[128] M. Koashi and N. Imoto. "Quantum cryptography based on split transmission of one-bit information in two steps". *Phys. Rev. Lett.* 79.12 (1997).

[129] M. Lucamarini and S. Mancini. "Secure deterministic communication without entanglement". *Phys. Rev. Lett.* 94.14 (2005).

[130] K. Boström and T. Felbinger. "Deterministic secure direct communication using entanglement". *Phys. Rev. Lett.* 89.18 (2002).

[131] V. Scarani et al. "The security of practical quantum key distribution". *Rev. Mod. Phys.* 81.3 (2009).

[132] S. Pirandola et al. "Advances in quantum cryptography". *Adv. Opt. Photonics* 12.4 (2020).

[133] C-H. F. Fung, X. Ma, and H. F. Chau. "Practical issues in quantum-key-distribution postprocessing". *Phys. Rev. A* 81.1 (2010).

[134] M. Araújo et al. "Witnessing causal nonseparability". *New J. Phys.* 17.10 (2015).

[135] H-K. Lo, H. F. Chau, and M. Ardehali. "Efficient quantum key distribution scheme and a proof of its unconditional security". *J. Cryptology* 18 (2005).

[136] E. Castro-Ruiz, F. Giacomini, and Č. Brukner. "Dynamics of quantum causal structures". *Phys. Rev. X* 8.1 (2018).

[137] M. A. Nielsen. "Quantum information theory". *arXiv preprint quant-ph/0011036* (2000).

[138] M. A. Nielsen et al. "Quantum dynamics as a physical resource". *Phys. Rev. A* 67.5 (2003).