Tools for High-dimensional Bell Basis Distinguishability with LELM Devices

Thomas Schneider

Theresa Lynn, Advisor

, Reader

HARVEY MUDD COLLEGE

Department of Physics

May, 2019

Abstract

For many quantum information protocols, it is useful to be able to reliably differentiate between several maximally entangled states. Moreover, practical restrictions on building quantum devices have pushed theorists towards studying the power of quantum devices limited to locally manipulating their particles. In this thesis, we are concerned with determining the power of linear evolution, local measurement (LELM) devices for distinguishing sets of Bell states. The qubit case has already been fully studied: projective LELM devices cannot distinguish all four qubit Bell states, they can only reliably distinguish three. However, the question of how many qudit Bell states a projective LELM device can reliably distinguish is still open; the problem also becomes exponentially more difficult as the dimension of the particle increases. Many of the computational and algebraic techniques used to solve the $d = 2$ and $d = 3$ cases become infeasible for higher dimensional particles. In this thesis, we explore various computational and algebraic tools for investigating the LELM Bell basis distinguishability question.

Contents

List of Figures

Acknowledgments

I would like to thank Professor Theresa Lynn for doing all of the things I could have possibly wanted an advisor to do, and doing those things very well. I would also like to thank Anna Barth, with whom I developed almost as many ideas as we shot down. And more generally, I would like to thank the people at Harvey Mudd College—it is them that have made this experience worth it.

Chapter 1

Introduction

The central question of this thesis—How many qudit Bell states can a projective LELM device reliably distinguish?—is of both practical and theoretical importance.

Measurements in the Bell basis are necessary for many quantum information protocols, such as quantum teleportation and dense coding. In fact, each protocol for being able to reliably distinguish sets of maximally entangled vectors (of which Bell bases are canonical examples) has a one-to-one correspondence with both a quantum teleportation scheme as well as a dense coding scheme (1). It is, however, difficult in practice to reliably make measurements in the Bell basis. This is because it is difficult to evolve one particle conditionally based on the first.

For example, if the particles in question are photons that store information in their polarization, performing a measurement in the Bell basis would require the ability to alter the polarization of one photon based on the polarization of the other photon. While possible to do, it cannot be done reliably (i.e. with high probability of success).[1]

The structure of this thesis is as such. Chapter 2 provides background for understanding the problem of LELM distinguishability. This includes information about the basics of quantum information, entanglement, and a formal definition of the LELM distinguishability problem. Chapter 3 outlines relevant progress made towards answering the LELM distinguishability problem. In particular, it focuses on: 1) a group distinguishability-preserving transformations for inputs in the $d = 3$ case and 2) the LELM distinguisha-

[1] Since dense coding schemes are meant to maximize the amount of information transferable by as few particles as possible, needing many copies of a particle to reliably produce an intended result is counterproductive.

bility problem for particles 'hyperentangled' in two variables.

Chapter 4 presents the major results, providing a generalization of the group of transformations discussed in Chapter 3.[2] In Chapter 5, we discuss attempts to utilize information about the hyperentangled Bell basis to provide insight into the Bell basis LELM distinguish question when $d = 4$.

[2] In particular, we generalize the group to higher dimensional particles.

Chapter 2

Background

This chapter will focus on the basics of quantum information that are relevant to understanding the Bell basis distinguishability question for LELM devices. In the first section, we will cover the basics of qubits, quidits, entanglement, Bell bases. In the next two sections, we will formally define LELM devices and the LELM distinguishability question.

2.1 Bits, Qubits, Qutrits, Qudits

The basic unit of classical information is the bit, which can take on either the value 0 or 1. A bit is exactly enough information necessary to describe the state of a two-state system. A common example is that of a light-switch, for which 0 could represent "off" and 1 could represent "on."

The quantum analog of the bit is the *qubit*. Qubits also describe two-state systems; however, they allow for linear combinations of possibilities. Qubits can take on either the value $|0\rangle$, $|1\rangle$, or any value of the form

$$|b\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are complex numbers normalized such that $|\alpha|^2 + |\beta|^2 = 1$. The notation $|\rangle$ is called a *ket*. Another way to represent the same qubit is as a column vector

$$b = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

but the ket notation is often more efficient. [1]

[1] An aditional reason to prefer to ket notation to column vector notation is because the

When one wishes to collect a value from a qubit, they *measure* it. If one were to measure the qubit in the $\{|0\rangle, |1\rangle\}$ basis (more on this later), then the qubit 'collapses' and unambiguously become either $|0\rangle$ or $|1\rangle$. The probability of the qubit collapsing to each state are determined by α and β, with probability $|\alpha|^2$ of collapsing to $|0\rangle$ and probability $|\beta|^2$ of collapsing to $|1\rangle$.

One canonical example of a physical qubit is the polarization of a photon. A photon can be found to be either horizontally polarized (written as the single ket $|H\rangle$) or vertically polarized (written as $|H\rangle$). But in general, a the state of the polarization of a photon can be anything of the form

$$|\text{photon}\rangle = \alpha|H\rangle + \beta|V\rangle$$

so long as α and β obey the normalization condition.

The set of all possible values for a qubit is a vector space of dimension two. One basis for this space is $\{|0\rangle, |1\rangle\}$. Measurements can be performed in any orthogonal basis. Other common orthogonal bases include

$$\left\{\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right\}$$

and

$$\left\{\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle,\ \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle\right\}.$$

If a qubit $|b\rangle$ is measured in the orthogonal basis $\{|x\rangle, |y\rangle\}$, then there is a $|\langle b|x\rangle|^2$ probability of measuring $|x\rangle$ and a $|\langle b|y\rangle|^2$ probability of measuring $|y\rangle$. Here, we've used the notation $\langle b|x\rangle$ to represent the inner product of $|b\rangle$ and $|x\rangle$. Moreover, the symbol $\langle|$ is called a *bra*, and it is used to represent the conjugate transpose of a ket. Hence, the conjugate transpose of the 'column' vector $\frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle$ would be the 'row' vector $\frac{1}{\sqrt{2}}\langle 0| + \frac{i}{\sqrt{2}}\langle 1|$.

Sometimes—such as in this thesis—we have the desire to represent systems that can take on more than two states. *Qutrits* represent systems that can take on three mutually-orthogonal states, and *qudits* are refer to the generalizations of qubits that represent systems with an arbitrary (but finite) number of mutually-orthogonal states. We write an arbitrary qutrit as

$$|t\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$$

column vector is a coordinate vector we must specify an entire basis for the column vector to make sense. And while the individual kets present in a vector expressed via ket notation from a basis, the full basis does not need to be specified. For example, we can write $|\psi\rangle = |0\rangle$ instead of $|\psi\rangle = 1 \cdot |0\rangle + 0 \cdot |1\rangle$.

and an arbitrary qudit as

$$|q\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{d-1}|d-1\rangle.$$

The numerical labels inside the kets can of course be changed without affecting any of the physics or the math.

A common physical example of a qutrit is the spin of any spin-1 particle, such as a photon. When the spin angular momentum of a photon is measured, it can either be $-\hbar$, 0, or $\hbar$—there are three mutually-orthogonal options. Qudits can be created for any dimension d by storing information as the potential energy of a particle (with some fixed total energy) that trapped in a harmonic oscillator.

2.2 Multi-particle Systems and Entanglement

Another useful generalization to consider is that of multi-particle systems. In classical computing, two-bit systems can take on four values: 00, 01, 10, and 11. In the notation of quantum information, we write these four values as:

$$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, \text{ and } |1\rangle \otimes |1\rangle.$$

The $\otimes$ symbol is used because our $|0\rangle$ and $|1\rangle$ kets are vectors, and their product in an element of a tensor product space. Similarly to how a qubit can be an arbitrary normalized linear combination of $|0\rangle$ and $|1\rangle$, states in a multi-particle system can be any normalized linear combination of the vectors $|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle,$ and $|1\rangle \otimes |1\rangle$. Often we will omit the $\otimes$ and write $|0\rangle \otimes |0\rangle$ as either $|0\rangle|0\rangle$ or as $|00\rangle$.

Tensor products obey the distributive property, so we have that

$$(|0\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle).$$

Entanglement refers to any multi-particle quantum state that cannot be represented as a tensor-product of two single-particle systems. Two examples of non-entangled quantum states are $|10\rangle$ and $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ because they can be written as

$$|1\rangle \otimes |0\rangle \quad \text{and} \quad \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

One example of an entangled state is

$$|\text{some entangled state}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + i|11\rangle\right).$$

A state is *maximally entangled* if knowing information about one particle reveals information about the other particle. For example, while the state

$$|\text{a state that's not maximally entangled}\rangle = \frac{1}{\sqrt{3}}\left(|00\rangle + |10\rangle + |11\rangle\right)$$

is entangled, if we were to measure the first particle and see that it is in the $|0\rangle$ state, then we know with certainty that second particle is also in its $|0\rangle$ state.

2.3 The Basics of Bell Bases

The canonical Bell basis (alternatively: the $d = 2$ Bell basis) consists of the four states:

$$\begin{aligned}
|\Phi^{+}\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)\\
|\Phi^{-}\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle - |1\rangle|1\rangle\right)\\
|\Psi^{+}\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right)\\
|\Psi^{-}\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)
\end{aligned}$$

Together, these states span the same space as the set $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

For many tasks, it is useful to be able to distinguish the Bell states. As an example, we'll look at a simple superdense coding scheme. The reason we'll focus on superdense coding is because even being able to distinguish three of the four $d = 2$ Bell states is an improvement over what can be done classically.

2.3.1 A Superdense Coding Scheme

What is the most amount of information can be sent via one-bit? Classically, the answer is simple: one bit of information. This is true even if the information is sent between two parties—call them A and B and associate with them whatever A and B names you find appropriate—who are able to share information with each other and devise strategies ahead of time.

But this answer changes if the parties are able to share and transmit quantum information. The scheme for doing so is as follows.

A and B share the Bell state $|\Phi^+\rangle$. The person named A holds on to the left particle and the person named B holds onto the right particle. Then, B travels far, far away. So far that the cost of sending information from A to B becomes expensive enough to justify humanity's investments in developing quantum information as a technology. Now, suppose A has four messages to send. She associates each message with a Bell state:

$|\Phi^+\rangle$: "All is lost."

$|\Phi^-\rangle$: "Did you leave the refrigerator running?"

$|\Psi^+\rangle$: "There is no hope left. Well, almost none. There is you."

$|\Psi^-\rangle$: "New phone, who 'dis?"

Depending on the message she wants to send, she performs one of four operations on her particle, the left one:

$|\Phi^+\rangle$: Leave the particle alone ($|x\rangle \mapsto |x\rangle$).

$|\Phi^-\rangle$: Flip the phase ($|x\rangle \mapsto -|x\rangle$).

$|\Psi^+\rangle$: Flip the bit ($|x\rangle \mapsto |1-x\rangle$).

$|\Psi^-\rangle$: Flip the phase and the bit ($|x\rangle \mapsto -|1-x\rangle$).

For example, if A performs the last operation, the state of the overall system transforms like

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \mapsto \frac{1}{\sqrt{2}}(|1\rangle|0\rangle - |0\rangle|1\rangle) = |\Psi^-\rangle.$$

A is able operate on just her particle and yet produce four separate Bell states. She can then send her particle to B and, assuming B is able to distinguish between the four Bell states, will be able to decode A's message.

But what happens if B is restricted to linear evolution, local measurement devices? (Perhaps B doesn't want to risk scrambling A's bit by sending it into a crystal that has a very low probability of performing a general Bell basis measurement and has a very high chance of outputting noise.) It's been shown that under this restriction, B would only be able to reliably distinguish three of the four Bell states. Then A would only be able to send three messages.

Three may not be as big as four, but it's considerably bigger than two. LELM devices are unable to perform as well as unrestricted quantum devices in this scenario, but perform strictly better than classical devices. The latter clause is why LELM devices are interesting for practical study; the former clauses is why they're interesting for theory.

2.3.2 The Generalized Bell Basis

The Bell basis is a basis of entangled states for a two-particle system. If each particle has dimension d, then the Bell basis is:

$$\left\{ |\Psi_c^p\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{pj} |j\rangle |j + c \pmod{d}\rangle \text{ such that } c, p \in \mathbb{Z} \text{ and } 0 \leq c, p < d \right\}$$

where $\omega = e^{i2\pi/d}$ is a primitive dth root of unity. Thus, for two d-dimensional particles, there are d^2 states in the Bell basis. We usually refer to a particle in the generalized Bell basis by specifying its correlation class c and its phase p. Motivation for why we care about the generalized Bell basis can be found in Chapter 3.

2.4 Linear Evolution Local Measurement Devices

A Linear Evolution Local Measurement (LELM) apparatus (Figure 2.1) has two main parts to it. The Linear Evolution part of the LELM apparatus refers to how the device cannot manipulate either of the input particles based on the value of the other. (The device cannot, for example, perform a controlled bit-shift.) It evolves either particle separately, with the exception that it is allowed to mix channels—i.e., to put itself in a state where it knowns information about a particle, but not whether the particle entered through the right or left input channel.

The Local Measurement part of LELM refers to how measurements are restricted to acting on a single particle at a time. A LELM apparatus takes in two particles, and outputs two detection events or 'clicks', each corresponding to one of the $2d$ *detection modes*.

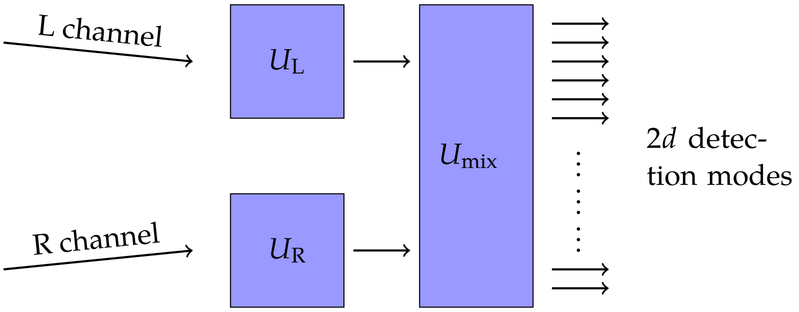

Figure 2.1 A LELM apparatus.

The basis of single-particle states is:

$$\mathcal{B}_{\text{single-particle}} = \{|0,L\rangle, |0,R\rangle, |1,L\rangle, |1,R\rangle, \ldots, |d-1,L\rangle, |d-1,R\rangle\}$$

The basis is of size $2d$, since each particle can either be from the left channel or the right channel. A pair of two detection modes is called a *detection signature*. Each detection mode is an element in the span of $\mathcal{B}_{\text{single-particle}}$. However, if $|i\rangle$ and $|j\rangle$ are detection modes then when determining their combined detection signature, we cannot simply take $|i\rangle \otimes |j\rangle$, since that may include inputs where two particles are coming from the same channel. Thus, we introduce the P_{LR} projection operator, which removes all elements of $\mathcal{B}_{\text{single-particle}} \times \mathcal{B}_{\text{single-particle}}$ of the form $|*,L\rangle|*',L\rangle$ or $|*,R\rangle|*',R\rangle$ and renormalizes the resulting state.

As an example for how to calculate a detection signature, take $|i\rangle$ and $|j\rangle$ to be

$$|i\rangle = \frac{1}{\sqrt{2}}\left(|1,L\rangle + |2,R\rangle\right) \quad \text{and} \quad |j\rangle = \frac{1}{\sqrt{3}}\left(|0,L\rangle + i|1,L\rangle - |2,R\rangle\right).$$

Their tensor product is:

$$|i\rangle\otimes|j\rangle = \frac{1}{\sqrt{6}}\left(|1,L\rangle|0,L\rangle + i|1,L\rangle|1,L\rangle - |1,L\rangle|2,R\rangle + |2,R\rangle|0,L\rangle + i|2,R\rangle|1,L\rangle - |2,R\rangle|2,R\rangle\right)$$

and their detection signature is $|i\rangle|j\rangle = P_{LR}\left(|i\rangle \otimes |j\rangle\right)$, i.e.,

$$\begin{aligned} &P_{LR}\left(|i\rangle \otimes |j\rangle\right) = \\ &\frac{1}{\sqrt{6}}\left(\cancel{|1,L\rangle|0,L\rangle} + \cancel{i|1,L\rangle|1,L\rangle} - |1,L\rangle|2,R\rangle + |2,R\rangle|0,L\rangle + i|2,R\rangle|1,L\rangle - \cancel{|2,R\rangle|2,R\rangle}\right) = \\ &\frac{1}{\sqrt{3}}\left(-|1,L\rangle|2,R\rangle + |2,R\rangle|0,L\rangle + i|2,R\rangle|1,L\rangle\right). \end{aligned} \tag{2.1}$$

An LELM device is specified by defining the $d \times d$ matrices U_{R} and U_{L}, the $2d \times 2d$ matrix U_{mix}, and the $2d$ detection signatures $|1\rangle, \ldots, |2d\rangle$, which are vectors in the vector space $\textsc{span}\left(\mathcal{B}_{\text{single-particle}}\right)$.

A small technicality. We've introduced here three transformations: U_{R}, U_{L}, and U_{mix}. The purpose of U_{mix} is to allow mixing of channels that the particles may take in addition to possible operations the particles may go through individually. We can, however, incorporate the operation U_{mix} into the detection modes. The LELM device with $U_{\mathrm{mix}} = U$ and detection modes $|1\rangle, \ldots, |2d\rangle$ as detection modes is equivalent to the device with $U_{\mathrm{mix}} = I$, the identity matrix, and detection modes $U^{\dagger}|1\rangle, \ldots, U^{\dagger}|2d\rangle$.

2.5 The Distinguishability Problem

Here, we formally define the LELM Bell basis distinguishability problem. First, we fix d, the dimension of our particles. Let $\mathcal{B}_d$ refer to the d-dimensional Bell basis. The distinguishability problem is the following.

What's the largest k such that there exists a subset of the Bell basis $S = \{|\Psi_1\rangle, \ldots, |\Psi_1\rangle\} \subseteq \mathcal{B}_d$ and an LELM device such that each state has a nonzero probability of causing some detection signature to fire and whenever a state $|\Psi_a\rangle \in S$ has a nonzero probability of causing detector pair i, j to fire then no other state $|\Psi_a\rangle \in S$ has a nonzero probability of causing detector pair i, j to fire.

Chapter 3

Previous Work

In this section, we'll examine previous work towards answering the LELM Bell basis distinguishability question. We'll first overview the current state of the $d = 3$ case, which has been solved for bosons but not for fermions. Then, we'll examine some general bounds. After that, we'll shift focus to the LELM distinguishability question for two hyperentangled particles, which we'll use in Chapter 5.

3.1 Work on Equivalent Inputs

Any answer to the distinguishability question comes in two parts. If one wants to show that k answers the distinguishability question for some particular d, they must show both that there exists an LELM device that distinguishes k bell States and that there does not exist a device that distinguishes $k + 1$ Bell states. The first part is often much easier, involving the specification of a device and some simple linear algebra to verify the device works.

In "Methods for Reliable Teleportation," there are two pages of algebra used to explain why an LELM device cannot distinguish all four $d = 2$ Bell states. In contrast, the proof that there exists an LELM device that does distinguish three Bell states is five sentences (2). For the $d = 3$ case, explored in Nathaniel Leslie's senior thesis, the discrepancy in work between the existence and non-existence parts of the proof is even more extreme. There are 14 pages (the majority of Chapter 2) devoted to proving that, for bosons, an LELM device cannot distinguish four of the nine $d = 3$ Bell states. The proof that an LELM device can distinguish three $d = 3$ Bell states is trivial—so trivial, that it's relegated to a footnote in my thesis.[1]

3.1.1 Nathaniel Leslie's Thesis Work

3.1.2 Other Work

3.2 Work on Hyperentanglement

[1] An LELM device can always distinguish d Bell states. Let the inputs be from different correlation classes, such as $|\Psi_0^0\rangle, \dots, |\Psi_0^{d-1}\rangle$. Let the detection modes be $|0, L\rangle, \dots, |d-1, L\rangle, |0, R\rangle, \dots, |d-1, R\rangle$. The detector clicks will reveal the correlation class of the input state, and there is only one input for each correlation class, so our device can reliably distinguish the d inputs!

Chapter 4

Characterizing Equivalent Inputs

When considering an LELM device, it's convenient to break the device into two components: the linear evolution section, which is comprised of the L and R channels as well as the transformations U_L and U_R, and the local measurement section, which is comprised of the $2d$ detection modes. In this chapter, we are completely concerned with inputs into our LELM device and what can be done on them by local operations. We focus on the question of which subsets of a Bell basis can be transformed into one another using only local operations (if so, we call these sets *equivalent*).

This question of determining equivalence classes of input sets is interesting in its own right, but is also useful for proving indistinguishably results. Once we prove that some subset of Bell states cannot be distinguished by and LELM device, we've shown that no equivalent subset can be distinguished by an LELM device. Generally, we hope to find that the equivalence classes are as large as possible since then results about particular sets of Bell states carry the most weight.

4.1 A Group of Transformations

One approach to answering the question "What subsets of the Bell bases can be transformed into each other by local operations?" is to look at transformations of the form $U_L \otimes U_R$ that permute the Bell basis. In his senior thesis, Nathaniel Leslie presents a set of four transformations for the $d = 3$ case that permute the Bell basis. Each transformation has a

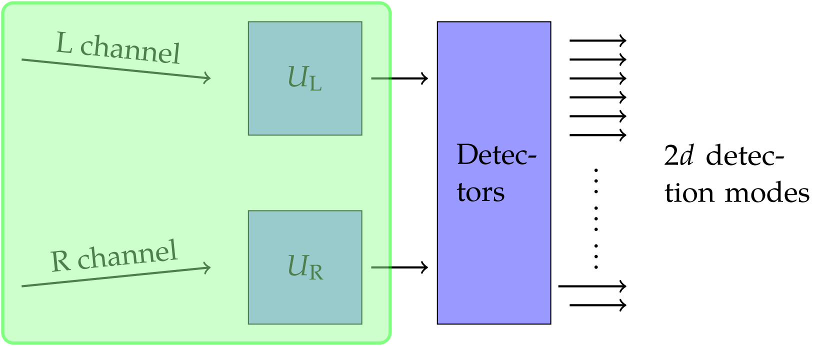

Figure 4.1 An LELM device, with the focus of this chapter highlighted in green.

simple corresponding description in terms of tic-tac-toe diagrams. The four rotations that Nathaniel looked at were:

$\hat{i}_p$: Cycle all the columns right.

$\hat{i}_c$: Cycle all the rows down.

$\hat{s}_p$: Shift the rows in a staggered manner. Leave the first ($c = 0$) row unchanged. Move the second ($c = 1$) row one to the right. Move the third ($c = 2$) row two to the right. [Note: moving a row two the right is the same as moving it one to the left.]

$\hat{s}_c$: Move the columns in a staggered manner. Leave the first ($p = 0$) column unchanged. Move the second ($p = 1$) column one down. Move the third ($p = 2$) column two down.

We've chosen to name these four translations $\hat{i}_p$, $\hat{i}_c$, $\hat{s}_p$, $\hat{s}_c$ for increment phase, increment correlation class, stagger phase, stagger correlation class. The way we have defined these transformations is in terms of our diagram, so we need to describe them in terms of separate operations on left and right channel particles, which we will do shortly. But first, it's useful to see how the group generated by these simple transformations acts on subsets of the Bell basis. Let $G_d = \langle i_p, i_c, s_p, s_c \rangle$ and let $S = \{|\Psi^0_0\rangle, |\Psi^1_0\rangle, |\Psi^2_0\rangle, |\Psi^2_1\rangle\}$, the subset from Figure 4.2, which also depicts the same set S after the operations $\hat{i}_p$, $\hat{i}_c$, $\hat{s}_p$, and $\hat{s}_c$.

Another way we can describe these transformations is by what they send a generic state to:

$\hat{i}_p$: $|\Psi^p_c\rangle \rightarrow |\Psi^{p+1}_c\rangle$

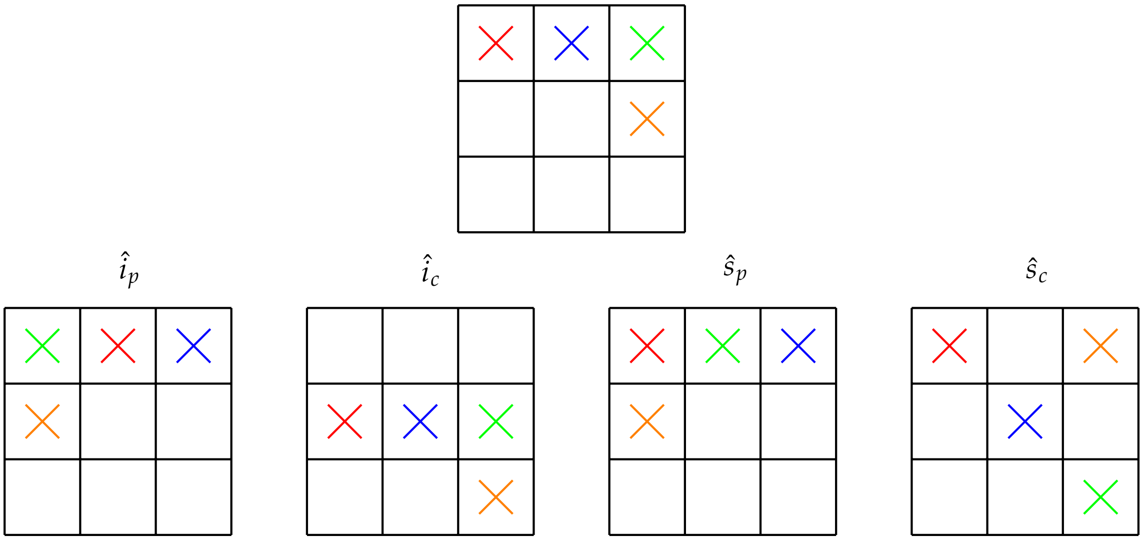

Figure 4.2 Some basic actions on $S = \{|\Psi_0^0\rangle, |\Psi_0^1\rangle, |\Psi_0^2\rangle, |\Psi_1^2\rangle\}$

$\hat{i}_c\colon\ |\Psi_c^p\rangle \to |\Psi_{c+1}^p\rangle$

$\hat{s}_p\colon\ |\Psi_c^p\rangle \to |\Psi_c^{p+c}\rangle$

$\hat{s}_c\colon\ |\Psi_c^p\rangle \to |\Psi_{c+p}^p\rangle$

4.1.1 Defining the Transformations

Now it's time for us to define the transformations $\hat{i}_p$, $\hat{i}_c$, $\hat{s}_p$, and $\hat{s}_c$ in terms of operations on single-particles. Here, we'll switch to a more condensed notation for denoting which channel a particle came from, using a subscript. As usual, arithmetic is done mod d.

$\hat{i}_p$: To do this transformation, we cycle the phase in the left channel:

$$\hat{i}_c|k\rangle_L \to \omega^k|k\rangle_L \quad \text{and} \quad \hat{i}_c|k\rangle_R \to |k\rangle_R$$

where $\omega = e^{i2\pi/d}$. This increments the phase.

$\hat{i}_c$: To do this transformation, we cycle the variable in the right channel:

$$\hat{i}_p|k\rangle_L \to |k\rangle_L \quad \text{and} \quad \hat{i}_p|k\rangle_R \to |k+1\rangle_R.$$

This increments the correlation class.

$\hat{s}_p$: This transformation is trickier, so we'll show how to derive it. Instead of simply guessing the solution like for the incrementing transformations, we'll begin by describing symbolically a semi-generic transformation on the left channel particle looks like.[1] The free variables in this our description (i.e. $x_0, x_1, \ldots, x_{d-1}$) represent information about how the phase of each left-particle ket changes. They're defined as such:

$$\begin{aligned} \hat{s}_p|0\rangle_L &\to \omega_0^x|0\rangle_L \\ \hat{s}_p|1\rangle_L &\to \omega_1^x|1\rangle_L \\ &\vdots \\ \hat{s}_p|d-1\rangle_L &\to \omega_{d-1}^x|d-1\rangle_L \end{aligned} \tag{4.1}$$

Next, we'll derive from our desired behavior of $\hat{s}_p$ what the values we need for our x_i's. Since $\hat{s}_p|\Psi_0^p\rangle = |\Psi_0^{p+0}\rangle = |\Psi_0^p\rangle$, then we must have that $\hat{s}_p|d-1\rangle_R \to \omega^{-x_{d-1}}|d-1\rangle_R$. This guarantees that $\hat{s}_p|(d-1)(d-1)\rangle \to \omega^{-x_{d-1}}\omega^{x_{d-1}}|(d-1)(d-1)\rangle = |(d-1)(d-1)\rangle$.

Now, setting $c = 1$ gives us a system of equations. We want $\hat{s}_p$ to increment by 1, up to an overall phase of $\frac{dy}{2\pi}$, meaning:

$$\begin{aligned} \hat{s}_p|\Psi_1^p\rangle &= \hat{s}_p\left(\frac{1}{\sqrt{d}}\left(|0\rangle_L|1\rangle_R + \omega^p|1\rangle_L|2\rangle_R + \omega^{2p}|2\rangle_L|3\rangle_R + \cdots + \omega^{(d-1)p}|d-1\rangle_L|0\rangle_R\right)\right) \\ &= \frac{\omega^y}{\sqrt{d}}\left(|0\rangle_L|1\rangle_R + \omega^{p+1}|1\rangle_L|2\rangle_R + \omega^{2p+2}|2\rangle_L|3\rangle_R + \cdots + \omega^{(d-1)p+d-1}|d-1\rangle_L|0\rangle_R\right). \end{aligned} \tag{4.2}$$

We have from our definition of $\hat{s}_p$ that:

$$\begin{aligned} \hat{s}_p|\Psi_1^p\rangle &= \hat{s}_p\left(\frac{1}{\sqrt{d}}\left(|0\rangle_L|1\rangle_R + \omega^p|1\rangle_L|2\rangle_R + \cdots + \omega^{(d-1)p}|d-1\rangle_L|0\rangle_R\right)\right) \\ &= \frac{1}{\sqrt{d}}\left(\omega^{x_0-x_1}|0\rangle_L|1\rangle_R + \omega^{x_1-x_2+p}|1\rangle_L|2\rangle_R + \cdots + \omega^{x_{d-1}-x_0+(d-1)p}|d-1\rangle_L|0\rangle_R\right). \end{aligned} \tag{4.3}$$

[1] By semi-generic, we mean that we will restrict ourselves to looking at the subset transformations where the correlation class is fixed but the resulting phases are completely generic.

Matching the exponents of the ω's, we get the system of equations:

$$\begin{aligned} x_0 - x_1 &= y \\ p + x_1 - x_2 &= y + p + 1 \\ 2p + x_2 - x_3 &= y + 2p + 2 \\ &\vdots \\ (d-1)p + x_{d-1} - x_0 &= y + (d-1)p + d - 1, \end{aligned} \tag{4.4}$$

which we can re-write such that we can solve it by recursively plugging an equation for x_{k+1} into the equation for x_k. We have,

$$\begin{aligned} x_0 &= x_1 + y \\ x_1 &= x_2 + y + 1 \\ x_2 &= x_3 + y + 2 \\ &\vdots \\ x_{d-1} &= x_0 + y + d - 1. \end{aligned} \tag{4.5}$$

This tells us that

$$x_0 = x_0 + dy + \sum_{k=0}^{d-1} k = x_0 + dy + \frac{d(d-1)}{2},$$

which we can solve to get that $y = \frac{1-d}{2} \pmod{d}$. Let's take $y = (d+1)/2$. We can also arbitrarily choose $x_0 = 0$ to get values for $x_0, x_1, \ldots, x_{d-1}$:

$$\begin{aligned} x_1 &= x_0 - y - 0 \Rightarrow x_1 = -y \\ x_2 &= x_1 - y - 1 \Rightarrow x_2 = -2y - 1 \\ x_3 &= x_2 - y - 2 \Rightarrow x_3 = -3y - 3 \\ &\vdots \\ x_{d-1} &= x_0 + y + d - 1 \Rightarrow x_{d-1} = \cancelto{y}{-(d-1)y} - \sum_{k=0}^{d-1} k = (d+1)/2 - d/2 = 1/2. \end{aligned} \tag{4.6}$$

Now we must check that this transformation sends $|\Psi_c^p\rangle$ to $|\Psi_c^{p+c}\rangle$ in general. We have that:

$$\begin{aligned}
\hat{s}_p|\Psi_c^p\rangle &= \hat{s}_p\left(\frac{1}{\sqrt{d}}\left(|0\rangle_L|0+c\rangle_R + \omega^p|1\rangle_L|1+c\rangle_R + \cdots + \omega^{(d-1)p}|d-1\rangle_L|d-1+c\rangle_R\right)\right) \\
&= \frac{\omega^{y_c}}{\sqrt{d}}\left(|0\rangle_L|0+c\rangle_R + \omega^{p+c}|1\rangle_L|1+c\rangle_R + \cdots + \omega^{(d-1)p+(d-1)c}|d-1\rangle_L|d-1+c\rangle_R\right) \\
&= \frac{1}{\sqrt{d}}(\omega^{x_0-x_c}|0\rangle_L|0+c\rangle_R + \omega^{x_1-x_{c+1}+p}|1\rangle_L|1+c\rangle_R + \cdots \\
&\quad + \omega^{x_{d-1}-x_{d-1+c}+(d-1)p}|d-1\rangle_L|d-1+c\rangle_R).
\end{aligned} \tag{4.7}$$

From this, we get the system of equations:

$$\begin{aligned}
0 + x_0 - x_c &= y_c + 0 + 0 \\
p + x_1 - x_{c+1} &= y_c + c + p \\
2p + x_2 - x_{c+2} &= y_c + 2c + 2p \\
&\vdots \\
(d-1)p + x_{d-1} - x_{c+d-1} &= y_c + (d-1)c + (d-1)p
\end{aligned} \tag{4.8}$$

which can be re-arranged to get:

$$\begin{aligned}
x_0 &= x_c + y_c + 0 \\
x_1 &= x_{c+1} + y_c + c \\
x_2 &= x_{c+2} + y_c + 2c \\
&\vdots \\
x_{d-1} &= x_{c+d-1} + y_c + (d-1)c
\end{aligned} \tag{4.9}$$

Now we wish to look back to the $c = 1$ case in the system of equations Equation 4.5. Notice that if we plug in the second equation ($x_1 = x_2 + y + 1$) into the first equation, then plug the third equation into ($x_2 = x_3 + y + 2$), and we repeat this process c times, then we get:

$$x_0 = x_c + cy + 1 + 2 + \cdots + (c-1) = x_c + cy + c(c-1)/2. \tag{4.10}$$

Moreover, we can perform a similar process of cascading plugging-in of equations to get:

$$x_k = x_{k+c} + cy + k + (k+1) + \cdots (k+c-1) = x_{k+c} + cy + c(c-1)/2 + ck. \tag{4.11}$$

Thus, the system equations Equation 4.5 implies that:

$$\begin{aligned}
x_0 &= x_c + cy + c(c-1)/2 \\
x_1 &= x_{c+1} + cy + c(c-1)/2 + c \\
x_2 &= x_{c+2} + cy + c(c-1)/2 + 2c \\
&\vdots \\
x_{d-1} &= x_{d-1+c} + cy + c(c-1)/2 + (d-1)c.
\end{aligned} \tag{4.12}$$

Comparing this to the system of equations Equation 4.9, we find that setting $y_c = cy + c(c-1)/2$, that Equation 4.5 begin solvable implies that Equation 4.9 is solvable. And we're done—$\hat{s}_p$ actually exists!

$\hat{s}_c$: Instead of constructing $\hat{s}_c$ directly, we'll first show that we are able to swap the phase and the correlation class. The way we'll do this is by performing the inverse Quantum Fourier Transform to the particle in the left channel and the Quantum Fourier Transform to the particle in the right channel. That is, if $|\Psi_c^p\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{pj}|j\rangle|j+c\rangle$, then we perform the transformations:

$$|j\rangle \mapsto \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{-kj}|k\rangle \quad \text{and} \quad |j+c\rangle \mapsto \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega^{l(j+c)}|l\rangle. \tag{4.13}$$

Thus,

$$\begin{aligned}
|\Psi_c^p\rangle &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{pj}|j\rangle|j+c\rangle \mapsto \\
&= \left(\frac{1}{\sqrt{d}}\right)^3 \sum_{j=0}^{d-1}\omega^{pj}\left(\sum_{k=0}^{d-1}\omega^{-kj}|k\rangle\right)\left(\sum_{l=0}^{d-1}\omega^{l(j+c)}\right)|l\rangle \\
&= \left(\frac{1}{\sqrt{d}}\right)^3 \sum_{j=0}^{d-1}\sum_{k=0}^{d-1}\sum_{l=0}^{d-1}\left(\omega^{l-k+p}\right)^j\omega^{lc}|k\rangle|l\rangle \\
&= \left(\frac{1}{\sqrt{d}}\right)^3 \sum_{k=0}^{d-1}\sum_{l=0}^{d-1}\left[\left(\omega^{lc}|k\rangle|l\rangle\right)\left(\sum_{j=0}^{d-1}\left(\omega^{l-k+p}\right)^j\right)\right]
\end{aligned} \tag{4.14}$$

The sum $\sum_{j=0}^{d-1}\left(\omega^{l-k+p}\right)^j$ is d if $l-k+p$ is a multiple of d and the sum is 0 otherwise. Since $0 \leq l,k,p \leq d-1$, we know that $-d+1 \leq$

$l - k + p < 2d - 2$. Thus, if $l - k + p$ is a multiple of d then either $l - k + p = 0$ or $l - k + p = d$. Another way to phrase this, is that the $|k\rangle|l\rangle$ pairs of kets that are kept are exactly the ones that differ by p, where $l - k \equiv p \pmod{d}$. Thus, we have:

$$\begin{aligned}
|\Psi_c^p\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{pj} |j\rangle|j + c\rangle \mapsto& \\
&= \left(\frac{1}{\sqrt{d}}\right)^3 \sum_{k=0}^{d-1}\sum_{l=0}^{d-1} \omega^{lc}|k\rangle|k+p\rangle d \\
&= \left(\frac{1}{\sqrt{d}}\right) \sum_{k=0}^{d-1} \omega^{(k+p)c}|k\rangle|k+p\rangle \\
&= \left(\frac{\omega^{kc}}{\sqrt{d}}\right) \sum_{k=0}^{d-1} \omega^{kc}|k\rangle|k+p\rangle = \omega^{kc}|\Psi_p^c\rangle
\end{aligned} \tag{4.15}$$

[Note that $\omega^{(k+p)c} = \omega^{(k+p+d)c}$.]

Thus, we can construct the operation $\hat{s}_c : |\Psi_c^p\rangle \mapsto |\Psi_{c+p}^p\rangle$ by applying the swapping operation, applying $\hat{s}_p$, then applying and the swapping operation again:

$$\hat{s}_c : |\Psi_c^p\rangle \mapsto |\Psi_p^c\rangle \mapsto |\Psi_p^{c+p}\rangle \mapsto |\Psi_{c+p}^p\rangle. \tag{4.16}$$

Phew, that was quite some algebra. A quick recap what we have done in this section:

- We've looked at the transformations defined in Nathaniel Leslie's thesis (which we've renamed). They are valid only for the $d = 3$ case.
- We've extended the definitions of $\hat{i}_c, \hat{i}_p, \hat{s}_c, \hat{s}_p$for the general quditcase.
- We've proved that each of the transformations $\hat{i}_c, \hat{i}_p, \hat{s}_c, \hat{s}_p$ take the form of $U_L \otimes U_R$ and are thus implementable in an LELM device.

4.1.2 Orbit-Stabilizer on our Group of Transformations

Let G_d be the group comprised of arbitrary compositions of the transformations $\hat{i}_c, \hat{i}_p, \hat{s}_c, \hat{s}_p$.

We've constructed G in a for a general d. The goal of creating this group is to determine which subsets of Bell states are equivalent, but it's not necessarily true that the G_d completely characterizes all equivalent inputs. We do, however, have the know the following.

Theorem 1. *If S_1 and S_2 are subsets of the Bell basis, and $gS_1 = S_2$ for some $g \in G$, then S_1 and S_2 are either both distinguishable or both indistinguishable.*

The set of all S such that $gS = S_1$ for some $g \in G$ is called the orbit of S_1. Letting $\mathcal{S} = \mathcal{P}(S)$ be the set of all subsets of the Bell basis, and $\mathcal{S}_k = \{S \in \mathcal{S} \text{ such that } |S| = k\}$. Our goal is to partition $\mathcal{S}$ into distinct orbits, so that we only need to determine the distinguishability of one element from each orbit. To do this, we'll use the Orbit-Stabilizer Theorem, which tells us that $|G_d| = |\text{Orb}(S)||\text{Stab}(S)|$ for any $S \in \mathcal{S}$. In general, once we've described G_d, it's much easier to count the size of the stabilizer of an element than the size of its orbit. In order to find $|G_d|$, we can calculate the size of the orbit and the size of the stabilizer for any element. Choosing $S_0 = \{|\Psi_0^0\rangle\}$ allows us to quickly see which elements of G_d are in $\text{Stab}(S_0)$. They are elements of G that can be written only using the two staggering operations ($\hat{s}_p$ and $\hat{s}_c$). We must now count them. We've done this computationally via an exhaustive search algorithm, the results of which are tabulated in Figure 4.3 (see the appendix for more details). Looking carefully at this table, we can formulate two conjectures:

Conjecture 2. *If $d = p^n$ where p is prime, then the size of G_d is $d^2(p^{3n} - p^{3n-2})$.*

Conjecture 3. *If $d = mn$ where m and n are relatively prime, then $|G_d| = |G_{mn}| = |G_m||G_n|$.*

These conjectures hold true for $d = 1$ through $d = 25$.

4.2 The $d = 4$ Case

One way to make progress would be to prove the conjectures from the last section. However, it's probably good to check right now to make sure what we're doing is worthwhile—that the equivalence classes are large enough to warrant worrying about them. To do this, we'll decompose G_4 into orbits. We know that for the $d = 4$ case, we can distinguish 4 Bell states whereas every set of Bell states of size 8 is indistinguishable. Let's focus on the case where $d = 4$ and we're looking at sets of Bell states of size $k = 7$. Thus, $|\mathcal{S}_7| = \binom{16}{7} = 11440$.

d	$\lvert\mathrm{Stab}(\{\lvert\Psi_0^0\rangle\})\rvert$	$\lvert G_d\rvert$
1	1	1
2	6	24
3	24	216
4	48	768
5	120	3000
6	144	5184
7	336	16464
8	384	24576
9	648	52488
10	720	72000
11	1320	159720
12	1152	165888
13	2184	369096
14	2016	395136
15	2880	648000
16	3072	786432
17	4896	1414944
18	3888	1259712
19	6840	2469240
20	5760	2304000
21	8064	3556224
22	7920	3833280
23	12144	6424176
24	9216	5308416
25	15000	9375000

Figure 4.3 A table of the first 25 values for the size of the stabilizer of $\{\lvert\Psi_0^0\rangle\}$ and the size of G_d

Size of stabilizer	Size of orbit	Number of elements	Number of distinct orbits
1	768	6912	9
2	384	2304	6
3	256	512	2
4	192	1536	8
6	128	128	1
16	48	48	1

Figure 4.4 A table giving the number of elements for each stabilizer size.

For the $d = 4$ case, we can actually just find the orbits explicitly. Calculating the stabilizer for each element of $\mathcal{S}_7$, we find get the data in the table in Figure 4.4

Overall, we find that there are 27 distinct orbits. Working with 27 elements is still a lot of work, but it's quite a bit better than dealing with 11440 elements.

Chapter 5

Comparing the $d = 4$ Bell Basis with the Hyperentangled Basis

5.1 Which Reductions are Possible?

Find the set of systems of equations that describe the restrictions that define reductions from $d = 4$ Bell basis to the hyperentangled basis.

5.2 An Experimental Approach

5.2.1 Gardient Descent into Madness

Bibliography

[1] R. F. Werner. All teleportation and dense coding schemes. 2000.

[2] L. Vaidman and N. Yoran. Methods for reliable teleportation. 1998.

[3] N. Pisenti, C. P. E. Gaebler, and T. W. Lynn. Distinguishability of hyperentangled bell state by linear evolution and local projective measurement. 2011.

[4] Nathaniel Leslie. Maximal lelm distinguishability of qubit and qutrit bell states using projective and non-projective measurements, 2017.

[5] Victor Shang. Computational progress towards maximum distinguishability of bell states by linear evolution and local measurement, 2016.

[6] Neal C. Pisenti. Distinguishability of hyper-entangled bell states with linear devices, 2011.

[7] Eleanor Rieffel and Wolfgang Polak. *Quantum Computing: A Gentle Introduction*. The MIT Press, 2014.

[8] John S. Townsend. *A Modern Approach to Quantum Mechanics*. University Science Books, 2012.

[9] Chistos M. Papadimitriou. *Computational Complexity*. Pearson, 1993.