Tools for High-dimensional Bell Basis Distinguishability with LELM Devices

Thomas Schneider

Theresa Lynn, Advisor

Second Reader, Reader

Department of Physics

May, 2019

Abstract

Your abstract should be a *brief* summary of the contents of your report. Don't go into excruciating detail here—there's plenty of room for that later.

Contents

List of Figures

List of Tables

Acknowledgments

thx

Chapter 1

Introduction

Chapter 2

Background

2.1 Quantum Information and Entanglement

This section will focus on the basics of quantum information that are relevant to understanding the Bell basis distinguishability question for LELM devices.

2.1.1 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 specific 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.

When one wishes to collect a value from a qubit, they *measure* it. 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 $|1\rangle$.

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 values, and *qudits* are refer to the generalizations of qubits that represent systems with an arbitrary (but finite) number of states. We write an arbitrary qutrit as

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

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.

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 $|00\rangle$.

2.1.2 Entanglement

Entanglement refers to any multi-particle quantum state that cannot be represented as

Two examples of non-entangled quantum states are $|11\rangle$ and $\frac{1}{\sqrt{2}}|11\rangle$

A state is maximally entangled if knowing information about one

2.1.3 The Basics of Bell Bases

The canonical Bell basis consists of the four states:

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

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.

2.2 Linear Evolution Local Measurement Apparatuses

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 can linearly evolve either particle separately, but cannot

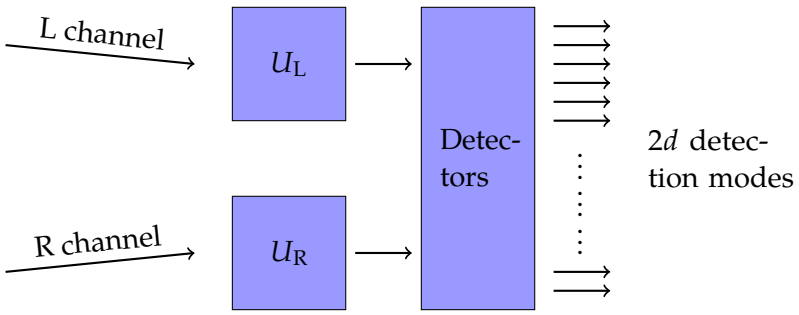


Figure 2.1 A LELM apparatus.

manipulate a particle based on the value of the other. So, for example, LELM devices cannot perform a controlled bit-shift. The Local Measurement part of the LELM apparatus refers to how measurements are restricted to acting on a single particle at a time. Thus, a LELM apparatus takes in two particles, and outputs two detection events or 'clicks'.

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 detector 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 resulting the state.

2.3 The Distinguishability Problem

2.3.1 Motivation

2.3.2 Formalization

Chapter 3

Previous Work

Chapter 4

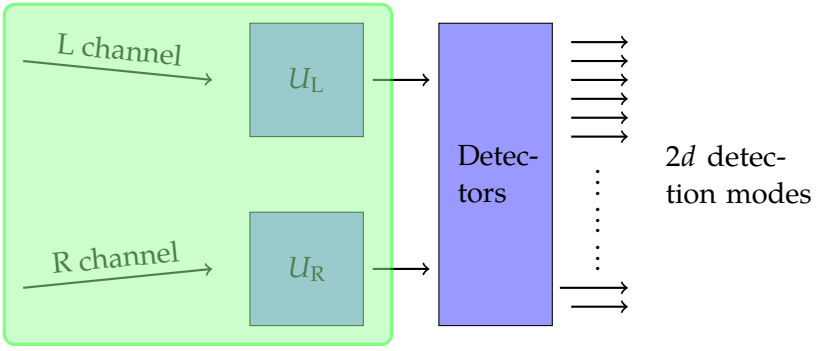
Equivalent Inputs

In this chapter, we are completely concerned with inputs into our LELM device and determining which inputs are equivalent.

4.1 A Group of Transformations

One question it's useful to ask is: What subsets of the Bell bases can be transformed into each other? If we know that we can transform the basis $\mathcal{B}$ into $\mathcal{B}'$, then this transformation can be represented by a unitary matrix, and hence is invertible. Then since we can go back-and-forth between $\mathcal{B}$ and $\mathcal{B}'$, then we know either $\mathcal{B}$ and $\mathcal{B}'$ are both distinguishable, or that $\mathcal{B}$ and $\mathcal{B}'$ are both indistinguishable.

In his senior thesis, Nathaniel Leslie looked at four transformations in the $d = 3$ case, each of which has a corresponding interpretation with reference to visualizations like in Figure **??**. The four rotations that Nataniel looked at were:



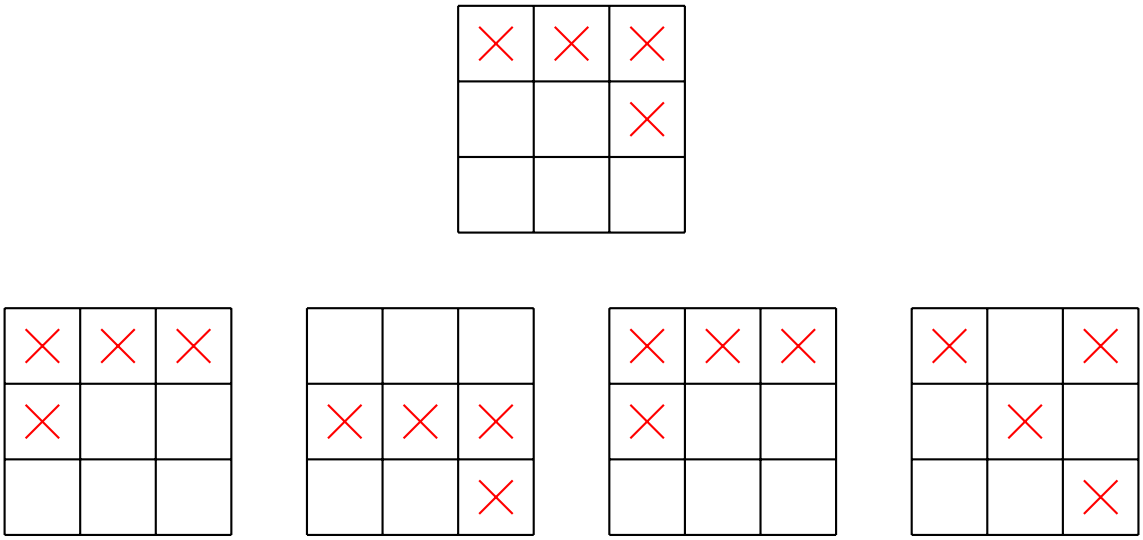


Figure 4.1 Some basic actions on $S = \{|\Psi_0^0\rangle, |\Psi_0^1\rangle, |\Psi_0^2\rangle, |\Psi_1^2\rangle\}$

$\hat{i}_p$: 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 on 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 $S = \{|\Psi_0^0\rangle, |\Psi_0^1\rangle, |\Psi_0^2\rangle, |\Psi_1^2\rangle\}$, the subset from Figure **??**. Figure 4.1 shows $\hat{i}_p S$, $\hat{i}_c S$, $\hat{s}_p S$, and $\hat{s}_c S$.

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

$\hat{i}_p$: $|\Psi_c^p\rangle \to |\Psi_c^{p+1}\rangle$

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

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

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

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. First, consider a generic transformation on the left channel particle:

$$\begin{aligned} \hat{s}_p|0\rangle_L &\to x_0|0\rangle_L \\ \hat{s}_p|1\rangle_L &\to x_1|1\rangle_L \\ &\vdots \\ \hat{s}_p|d-1\rangle_L &\to x_{d-1}|d-1\rangle_L \end{aligned} \tag{4.1}$$

Since $\hat{s}_p|\Psi_0^p\rangle = |\Psi_0^{p+0}\rangle = |\Psi_0^p\rangle$, then we must have that $\hat{s}_p|d-1\rangle_R \to -x_{d-1}|d-1\rangle_R$. Now, setting $c = 1$ gives us a system of equations. We want $\hat{s}_p$ to increment by 1, up to an overall phase, 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:

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

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 $x_0, x_1, \ldots, x_{d-1}$:

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

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:

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

4.1.2 Orbit-Stabilizer on G_d

We've constructed G_d in a completely general way. The goal of creating this group is to determine which subsets of Bell states are equivalent.

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 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 in the table in Figure 4.2. 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 area to 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. 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, $|\mathcal{S}_7| = \binom{16}{7} = 11440$.

For the $d = 4$ case, we can actually just find the orbits explicitly. Calculating the stabilizer for each element of $\mathcal{S}_k$, we find get the data in the table in Figure 4.3

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 4.2 A table of the first 25 values for the size of the stabilizer of $\{|\Psi_0^0\rangle\}$ 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 4.3 A table giving the number of elements for each stabilizer size.

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