Quantum Tomography with Pauli Operators

by

Tyler B. Jackson

A Thesis
presented to
The University of Guelph

In partial fulfilment of requirements
for the degree of
Master of Science
in
Mathematics and Statistics

Guelph, Ontario, Canada

© Tyler B. Jackson, November, 2013
In experiments it is often required that we determine an unknown quantum state produced by a source. Quantum Tomography accomplishes this through repeated measurements on the state. This process requires $4^n$ measurements for an $n$-qubit system. However, if it is known that the state is pure, fewer measurements are required. Many such results already exist, but they either use non-local measurements or they have some chance of failing. Our goal is to obtain the smallest set of Pauli operators which can uniquely determine any pure state among all states. This involves ensuring the complement of the span of the measurements must have two positive and two negative eigenvalues. This is nontrivial since there are few relationships between the eigenvalues of a set of operators and the eigenvalues their real linear combinations. We obtain the lower bound of 30 Paulis necessary for 3-qubit tomography which improves on any known result.
Acknowledgements

I would like to thank Dr. Bei Zeng and Dr. David Kribs for the opportunity to do my masters degree with them and for their excellent guidance and encouragement through the processes. I would also especially like to thank Dr. Jianxin Chen for working so closely with me on this project and always listening to my ideas and taking the time to explain (more often than not) why they would not work. Finally I would like to thank my parents for all their support and encouragement through my (continuing) education.
## Contents

Acknowledgements iii

1 Basics 1
   1.1 The Qubit .................................................. 1
   1.2 Pauli Operators ............................................. 4
   1.3 The Clifford Group ......................................... 5

2 Quantum State Tomography 8
   2.1 Tomography Basics ........................................... 8
   2.2 Pure State Tomography ...................................... 10

3 Pauli Tomography of Pure States 14
   3.1 Introduction .................................................. 14
   3.2 2-Qubit Case ................................................ 15
   3.3 3-Qubit Case ................................................ 17
   3.4 Conclusion .................................................. 44

4 Future Directions 45

Bibliography 47
Chapter 1

Basics

1.1 The Qubit

In classical computing the fundamental unit of information is the bit, or binary digit. It can be in one of two states typically known as 0 and 1. There is an analogous quantity in quantum computing which is called a ‘qubit’ or quantum bit. Instead of two distinct values, qubits are represented by unit vectors in a two dimensional complex Hilbert space [24]. The ‘standard basis’ for this Hilbert space is typically represented as |0⟩ and |1⟩.

Here we are using Dirac notation for the states of the qubit/ vectors of the Hilbert space. |a⟩ is ‘ket’ a and is the vector \( \overrightarrow{a} \) in the vector space. The Hermitian conjugate of \( \overrightarrow{a} \), \( (\overrightarrow{a})^\dagger \) is then written in Dirac notation as ‘bra’ a, \( \langle a| \). The inner product between two vectors \( \overrightarrow{a} \) and \( \overrightarrow{b} \) is represented as \( \langle a|b \rangle \).

Physically a qubit is a quantum system with two basis states (or one with more than two states but is constrained to only two). Typical examples include spin half particles such as the electron for which measuring its angular momentum yields either an ‘up’ or
Another common system is a photon with either vertical or horizontal polarization. These distinct states form an orthonormal basis for the Hilbert space. The correspondence of any state to a particular basis vector is arbitrary.

While it is important to understand the physical systems which implement a qubit, for the purposes of quantum information theory we deal with the abstraction of the qubit from the system which implements it. For us a qubit is the vector in the two dimensional complex Hilbert space with some basic assumptions about behaviour, usually quoted as the axioms of quantum information [24] [26]. This is similar to the classical bit which can be representative of any number of systems from magnetized strips to high and low voltage in a wire. The abstraction of the qubit from the physical system that implements it allows for consistency and broadly applicable results. The advantage of qubits over bits is a property called superposition. A classical bit can be 0 or 1, but it cannot be some complex linear combination of 0 and 1. At best it can have some probability of being 0 or 1, which constrains bits to a line segment. The qubit, whose states can be described as $|\psi\rangle = a|0\rangle + b|1\rangle$ where $a$ and $b$ are complex numbers which satisfy $|a|^2 + |b|^2 = 1$ (the unit length constraint). This gives the qubit two complex degrees of freedom with one constraint.

Up until now we have restricted the discussion to states of qubits known as ‘pure’. There is another type of state known as mixed states. These states represent probabilistic mixtures of pure states. In order to represent mixed states we need to introduce a new way to represent quantum states called density matrices. Single qubit density matrices are 2-by-2 Hermitian matrices. The density matrix of a pure state $|\psi\rangle$ can be written as $|\psi\rangle \langle \psi|$
in outer product notation. A mixed state is then any state of the form \( \rho = \sum_{i=1}^{n} p_i |\psi_i\rangle \langle \psi_i| \)
where \( \sum_{i=1}^{n} p_i = 1 \). These are also 2-by-2 Hermitian matrices. The difference between mixed states and pure states is subtle but important. A mixed state represents some missing information about the system, a good example is to imagine a source of quantum states which produces the states \(|0\rangle\) and \(|1\rangle\) with equal probability.

**Example 1.1.** To demonstrate the subtle difference between some pure and mixed states, compare the density matrices of the \(|+\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle] \) state and the maximally mixed state, that is the mixture of states \(|0\rangle\) and \(|1\rangle\) with equal probability. In the first case the state is in an even superposition of the \(|0\rangle\) and \(|1\rangle\) states. Its density matrix is:

\[
\rho = \frac{1}{\sqrt{2}}[|0\rangle \langle 0| + |1\rangle \langle 1| + |0\rangle \langle 1| + |1\rangle \langle 0|] = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.
\]

In the second case we get:

\[
\rho = \frac{1}{2} [|0\rangle \langle 0| + |1\rangle \langle 1|] = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.
\]

These two states are clearly different.

Since these are still states, there is still a Hilbert space associated with them. The norm/inner product in this case is now the Hilbert-Schmidt inner product: \( \langle \rho, \sigma \rangle = \text{Tr}(\rho \sigma^\dagger) \), \( ||\rho|| = \sqrt{\text{Tr}(\rho \rho^\dagger)} \) where \( \rho \) and \( \sigma \) are Hermitian matrices (either an operator or a density matrix). In order for a Hermitian matrix \( \rho \) to be a valid quantum state it must satisfy two properties. First \( \text{Tr}(\rho) = 1 \), this is the normalization constraint of states. In the case of
pure states this is equivalent to the unit length constraint of state vectors.

\[ \text{Tr}(\rho) = \text{Tr}(|\psi\rangle \langle \psi|) = \text{Tr}(\langle \psi | \psi \rangle) = \langle \psi | \psi \rangle = 1 \] (1.3)

The second property \( \rho \) must satisfy is being positive semi-definite. This represents the fact that when projecting onto a state, you cannot have negative probability of getting that result. Mathematically its stated as \( \langle x | \rho | x \rangle \geq 0 \) for all vectors \( |x\rangle \).

For a mixed state \( \rho = \sum_{i=1}^{n} (p_i |\psi_i\rangle \langle \psi_i|) \), since each pure state in the mixture has trace 1 and the trace is linear, it follows that the trace equals one for all mixed states as well.

Larger systems, such as many-qubit systems, can be represented by states in a higher dimensional Hilbert space. For \( n \) qubits this is the \( 2^n \) dimensional complex vector space. All of the same requirements hold from the single qubit case. Combining two systems together, say of two qubits in states \( \rho_1 \) and \( \rho_2 \) respectively is done by taking the tensor product of their states, \( \rho_{12} = \rho_1 \otimes \rho_2 \). This state now exists in the space \( \mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4 \).

### 1.2 Pauli Operators

The single qubit Pauli operators are 2-by-2 Hermitian matrices which form a basis for the space of 2-by-2 Hermitian matrices. In the standard basis they are written as:
\[ \sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_1 = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \]

\[ \sigma_2 = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_3 = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \]

For \( n \)-qubit systems, the \( n \)-qubit Pauli operators still form a basis for the space of \( 2^n \)-by-\( 2^n \) Hermitian matrices. The \( n \)-qubit Pauli operators are defined as:

\[ P = \bigotimes_{j=1}^{n} s_j \]

\[ s_j \in \{I, X, Y, Z\} \]

When there is no confusion in the meaning, the notation \( XYZ \) will be used for the operator \( X \otimes Y \otimes Z \) for ease of reading.

### 1.3 The Clifford Group

The set of Pauli operators are of great interest for many reasons. They are Hermitian, unitary, traceless (orthogonal to the identity), they form a basis for Hermitian matrices, and in many experimental systems they are easy to measure.

The Clifford group is defined as the set of operators which maps the set of Paulis (without the identity) \( \mathcal{P} = \{\pm X, \pm Y, \pm Z\} \) to itself under conjugation [9]. That is to say
that any element $C$ of the Clifford group, a Clifford operator is a bijective map $C : \mathcal{P} \to \mathcal{P}$. The Clifford operators are then the subgroup of the unitaries $U(2^n)$ which normalize the Pauli operators. The Clifford group can be generated by, or written as a product of some combination of, the Hadamard ($H$), controlled-not($CNOT$) and phase ($S$) operators typically written as:

$$
H = \frac{1}{\sqrt{2}} \begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix},
S = \begin{bmatrix}
1 & 0 \\
0 & i
\end{bmatrix},
CNOT = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
$$

(1.4)

When dealing with $n$-qubit systems the Hadamard and the Phase gates are appropriately tensored with identities on the other $n - 1$ qubits. The action of the CNOT in the $n$-qubit case is one qubit is the ‘control’ and the other is the target. If the control qubit is in the state $|1\rangle$ then the target qubit has a ‘Not’ gate applied to it and the control qubit has the identity applied to it. However if the control qubit is in state $|0\rangle$ the identity is applied to both qubits.

Also the Clifford group for an $n$-qubit system, denoted $C_n$ has order given by [3]:

$$
|C_n| = 2^{n^2 + 3n + 3} \prod_{j=1}^{n}(4^j - 1).
$$

(1.5)

In the one, two and three qubit cases the Clifford groups have order 24, 11520, and 92897280 elements respectively. In the one qubit case this is easy to obtain, any $U \in C_1$ will be defined on its action on $X$ and $Z$ and $U$ must preserve the structure of the Paulis under
conjugation, namely $UXU^\dagger$ must anti-commute with $UZU^\dagger$. Therefore a counting argument can be made, $U$ can take $X$ to any other element of $\mathcal{P}$. This allows for six images of $X$, $UZU^\dagger$ can then be any element that is not $\pm UXU^\dagger$. This allows for four options. Therefore $|C_1| = 6 \cdot 4 = 24$ elements. For higher dimensional systems the counting argument holds and gives the result stated above.

Later when we are using a Clifford operator on a set of Paulis it will mean conjugating every Pauli in the set by the same Clifford. We also will ignore signs since we care about subspaces spanned by a certain set of Pauli operators. This will greatly reduce computational work needed to be performed later.
Chapter 2

Quantum State Tomography

2.1 Tomography Basics

Quantum state tomography is the method by which an unknown quantum state produced by a source can be determined or reconstructed from the its measurement values on a set of operators [1] [25] [19] [29]. Since measuring a state destroys it, the source must produce many of the same quantum state with relative reliability for this to work. When the state can be any valid quantum state, pure or mixed, the set of measurements taken must be ‘tomographically’ complete in order to uniquely determine the state.

Tomographically complete means the measured operators form a complete operator basis for the states in the Hilbert space. In the case of single and multi-qubit states, the Pauli operators form one possible tomographically complete set of measurements. In order for a set of measurements of a $d$-dimensional system to be tomographically complete, a minimum of $d^2 - 1$ measurements must be performed. This is due to the fact that all density matrices must be $d$-by-$d$ Hermitian matrices which have $d^2$ degrees of freedom, less
one for the constraint that the trace is 1. However, quite often we are only concerned with states with particular properties, such as being a pure state or one of low rank. Under certain assumptions about the properties of an unknown state $\rho$ it should be possible to require fewer measurements to be made. Intuitively this can be thought of in a simple $\mathbb{R}^n$ vector space. If you want to determine an unknown vector $\vec{u}$ you need to measure its projection onto each of the $n$ basis vectors. However if you know that $\vec{u} = \alpha \vec{v}$, then only one measurement is required.

When an operator is measured for a quantum state, a classical result of the measurement is produced. The probability of a given result being produced is equal to the projection of the quantum state being measured onto the measurement outcome projectors. This is known as Born’s rule [30] which states, when measuring an operator $A$ on a state $|\psi\rangle$, the outcome will be one of the eigenvalues $\lambda$ of $A$ with the probability of obtaining $\lambda_i$ being $\text{Tr}(|\psi\rangle \langle v_i| \langle v_i|) = |\langle \psi|v_i \rangle|^2$. Where $v_i$ is the eigenvector associated with $\lambda_i$.

**Example 2.2.** The Pauli ‘$Z$’ operator has two measurement outcomes, 1 and -1. The resultant states from measuring the $Z$ Pauli are $M_0 = |0\rangle \langle 0|$ and $M_1 = |1\rangle \langle 1|$. In essence this means that when you measure any quantum state, it will give you a number 1 or -1 and be left in the state $|0\rangle \langle 0|$ or $|1\rangle \langle 1|$ respectively. If the quantum state being measured is $\rho$ then the probability of getting outcome $i$ is $\text{Tr}(M_i \rho)$.

When doing state tomography we have a source which repeatedly produces $\rho$, we then measure each of the operators many times to obtain an estimate to the probabilities associated with getting each result. From this we are able to reconstruct the original quantum state, but only if the measurements we made are tomographically complete, since
if they do not form a complete basis, then not all the information for every state will be obtained. Any component of a state which is orthogonal to the measurement operators will not be represented.

### 2.2 Pure State Tomography

Often in experiment we care about pure states or states very close to pure. Our question is then, if we assume the state is pure, how many measurements are required to uniquely determine the state? There can be two distinct goals in this regard which were characterized in [4]. The first is to be able to determine a pure state among all pure states with a set of measurement operators $A = \{A_1, A_2, \ldots, A_n\}$.

**Definition 2.1.** A pure state $|\psi\rangle$ is uniquely determined among all pure states (UDP) by the measuring a set of operators $A = \{A_1, A_2, \ldots, A_n\}$ if there does not exist a $|\phi\rangle$ which has the same measurement results as $|\psi\rangle$.

The second definition is the natural extension of the first.

**Definition 2.2.** A pure state $|\psi\rangle$ is uniquely determined among all states (UDA) by the measuring of a set of operators $A = \{A_1, A_2, \ldots, A_n\}$ if there does not exist a state $\sigma$ (pure or mixed) which has the same measurement results as $|\psi\rangle$.

Note that it is immediately obvious that UDA implies UDP, however the reverse is not necessarily true. It is possible that since UDP has fewer dimensions to distinguish between that fewer measurements are required than UDA.

One solution called compressed sensing [6] [11] [18] put forth in [12] uses matrix completion techniques to reconstruct a state $\rho$ of dimension $d$ and rank $r$ which is low
(pure or nearly pure) from its measurement results. Their method involves choosing order $O(d \log d)$ Pauli operators at random to measure. They show that these will uniquely determine the state in question with some probability of failure which is exponentially small in $c$. This probability of failure results from the fact that these randomly chosen Paulis might be UDA for all but some set of states of non-zero measure for which the method will fail. The benefits of this method are that it does not require a tomographically complete set of measurements to determine the state, and the post processing algorithm is polynomial in time. However it would be ideal to have a set of measurements which is guaranteed to be UDA for every pure state.

In order for any pure state $|\psi\rangle$ to be UDA by a set of operators $A$ there cannot be any operator $H \in (\text{span}(A))^c$ such that $\sigma = |\psi\rangle\langle\psi| + H$ is positive semi-definite. If this were the case, then measuring the operators would return identical measurement results since $H$ is orthogonal to $\text{span}(A)$ and would not contribute to the measurements. It is sufficient to require that any $H \in (\text{span}(A))^c$ must have at least two positive and 2 negative eigenvalues. Sufficiency can be shown as follows. In order to be positive semi-definite, $\langle x | (|\psi\rangle\langle\psi| + H) |x\rangle \geq 0$ for all $|x\rangle$. Furthermore since we wish for any pure state to be UDA we also require that this be true for any $|\psi\rangle$. Assume $H$ has two negative eigenvalues $\alpha, \beta$ and associated eigenvectors $|a\rangle, |b\rangle$ respectively. Choose $|\psi\rangle = |a\rangle$ and choose a $|x\rangle$
perpendicular to $|a\rangle$. It can then be seen that:

$$
\langle x | (|\psi\rangle \langle \psi| + H) | x \rangle \\
= \langle x | a \rangle \langle a | x \rangle + \langle x | H | x \rangle \\
= \langle x | H | x \rangle
$$

Since $|x\rangle$ is orthogonal to $|a\rangle$ ($\langle a | x \rangle = 0$) which means any contribution from it is automatically 0. From the spectral theorem, we know that the eigenvectors of a Hermitian matrix are orthogonal, so we can choose that $|x\rangle = |b\rangle$, this would make the final quantity negative which is sufficient to make $\langle x | (|\psi\rangle \langle \psi| + H) | x \rangle$ non-definite.

An easier way to understand this is, in order to be UDA there must be only one valid quantum state with a particular set of measurement results. Any other matrices which differ by a quantity orthogonal to your measurements must not represent any valid quantum state.

The method presented in [4] aims to find a particular choice of general operators $A$ which is UDA for all pure states. It was shown that $5d - 7$ such operators were required. This is in comparison to a result in a previous paper [15] that only $4d - 5$ operators were required for any pure state to be UDP. The method to construct this set of operators was to first construct a family of Hermitian matrices of dimension $d$ which has a single anti-diagonal with non-zero entries. This family of operators was shown to be linearly independent and to satisfy the requirement that any operator in its span’s complement has two positive and two negative eigenvalues.

It is clear that this method has several strengths, for one this set of operators will
uniquely determine any pure state, with theoretically zero error rate. It also uses a number of observables that is linear in $d$. The largest downside is the set of constructed observables, which are derived to perform nicely in the proof, are not practical to implement experimentally due to the fact that they are entangled operators. They cannot be represented as a set of local operators tensored together. Local operators are always easier to implement since each subsystem can be measured on its own and only the classical correlation between subsystems must be recorded.
Chapter 3

Pauli Tomography of Pure States

3.1 Introduction

As mentioned in the previous section, when conducting quantum state tomography experimentally, measuring the Pauli operators is typically easy since they are not entangled. While the compressed sensing method uses Pauli operators, it has some chance of error, furthermore it uses $O(d \log(d))$ measurements. The method in [4] is of $O(d)$ but the operators they construct are not feasible to measure in experiment. It would be ideal to find a minimal set of Pauli operators which succeed in determining any possible pure state with no theoretical error.

Here we present a set of 30 Pauli operators which will uniquely determine any pure state among all states for a 3-qubit system, the method by which it was found and the proof that it does in fact satisfy the criterion. Note that 30 operators is less than the $5d - 7 = 33$ operators given by [4].

Recall that in order for a set of operators $A = \{A_1, A_2, \ldots, A_n\}$ to be UDA, any
$H \in (\text{span}(A))^c$ must have at least two positive and two negative eigenvalues. We are therefore required to find the largest set of Pauli operators $\mathcal{P} = \{P_i : 1 \leq i \leq k\}$ such that there does not exist real coefficients $\alpha_i$ for which the operator $H = \sum_i \alpha_i P_i$ fails to have two positive and two negative eigenvalues. We will often refer to this as the ‘criteria’ which we are hoping to satisfy. This $\mathcal{P}$ is the set of Paulis which span the complement of the span of the measurement operators, $\text{span}\{\mathcal{P}\} = (\text{span}\{A\})^c$, so maximizing the set $\mathcal{P}$ corresponds to minimizing the number of measurement operators we need to use.

**Definition 3.3.** A ‘failing set’ $F = \{P_i : 1 \leq i \leq l\}$ is a collection of traceless $N$-qubit Pauli operators such that some linear combination of them with real coefficients does not have at least two positive and two negative eigenvalues.

It becomes clear that the set $\mathcal{P}$ cannot have any failing set as a subset, otherwise it will fail the requirements.

### 3.2 2-Qubit Case

The two-qubit version is much simpler to solve, since the two-qubit density matrices are 4-by-4, no eigenvalue can be zero or else there would be less than two positive and two negative eigenvalues. Therefore if two Pauli matrices commute, then they are simultaneously diagonalizable. This means there must exist some real combination of them which can set at least one of the eigenvalues to 0. Therefore in the two-qubit case any pair of commuting Paulis is a failing set. Note this doesn’t exclude the possibility that there is some failing set consisting of only anti-commuting matrices, but this will turn out not to matter.
Theorem 3.1. Any Hermitian operator perpendicular to

\[ \{ IX, IY, IZ, XI, YX, YY, YZ, ZX, ZY, ZZ \} \]  \hspace{1cm} (3.1)

must have at least two positive and two negative eigenvalues.

Proof. The complement of the span of the given operators is itself the span of the operators \( \{ XX, XY, XZ, YI, ZI \} \). It is relatively easy to prove that there are no sets of mutually anti-commuting two-qubit Paulis with more than five elements by exhaustive search. It is also easy to verify that these Paulis mutually anti-commute. They therefore do not contain any of the known failing sets in the two-qubit case nor can there be any larger set which satisfies the criteria. There could however be a failing set which was not accounted for. We must then prove that any operator of the form \( H = \alpha_1 XX + \alpha_2 XY + \alpha_3 XZ + \alpha_4 YI + \alpha_5 ZI \) has two positive and two negative eigenvalues. \( H \) then has the following form:

\[
\begin{pmatrix}
\alpha_5 & 0 & \alpha_3 + \alpha_4 i & \alpha_1 + \alpha_2 i \\
0 & \alpha_5 & \alpha_1 - \alpha_2 i & -\alpha_3 + \alpha_4 i \\
\alpha_3 - \alpha_4 i & \alpha_1 + \alpha_2 i & -\alpha_5 & 0 \\
\alpha_1 - \alpha_2 i & -\alpha_3 - \alpha_4 i & 0 & -\alpha_5 \\
\end{pmatrix}.
\]  \hspace{1cm} (3.2)

The determinant of \( H \) can be calculated and the result is:

\[
\alpha_5^4 + \alpha_5^2 |\alpha_3 + \alpha_2 i|^2 + \alpha_5^2 |\alpha_1 + \alpha_2 i|^2 \\
+ |\alpha_3 - \alpha_4 i|^4 + |\alpha_3 - \alpha_4 i|^2 |\alpha_1 + \alpha_2 i|^2 + |\alpha_3 - \alpha_2 i|^2 \alpha_5^2 \\
+ |\alpha_1 - \alpha_2 i|^4 + |\alpha_1 - \alpha_2 i|^2 |\alpha_3 - \alpha_4 i|^2 + |\alpha_1 - \alpha_2 i|^2 \alpha_5^2. \]  \hspace{1cm} (3.3)
This quantity, being the sum of non-negative terms, is greater than or equal to 0. With equality if and only if all terms in the sum are 0. This only occurs when \( \alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = \alpha_5 = 0 \). Since this is a 4-by-4 traceless Hermitian matrix, it can only have positive determinant if and only if it has exactly two positive and two negative eigenvalues. Thus this is the largest set \( \mathcal{P} \) with this property, so \( 15 - 5 = 10 \) Pauli operators are sufficient to uniquely determine any two-qubit pure state among all states.

3.3 3-Qubit Case

The situation in the 3-qubit case is not as simple as the 2-qubit case. The primary reason for this is that 3-qubit operators are 8-by-8 Hermitian matrices with eight eigenvalues, up to four of which can be 0 without failing the criterion. This means that the property of Paulis being commuting no longer defines the failing sets, and the determinant can no longer characterize when a set fails.

Furthermore, showing that a set of Pauli operators is not a failing set is not easy to do since it requires verifying that no set of coefficients from a continuous range of possibilities causes that set to fail. Finding those coefficients for which the set does fail is difficult since as of yet no analytic test has been found by us to distinguish failing sets from non-failing sets. However there are certain circumstances which can make finding a failing set easier. For instance if we restrict ourselves to Pauli operators which consist of only \( I \) and \( Z \) Paulis tensored together, these operators are diagonal and the diagonal can be treated as a vector. We choose some set of these vectors and make them the columns of a matrix. We then attempt to find some submatrix of 5 of the 8 rows which has a non-empty nullspace. If
this can be found, this implies that there exists some real linear combination of the chosen operators which has only three non-zero eigenvalues which contradicts the criterion.

**Definition 3.4.** An I-Z operator is an 3-qubit Pauli operator of the form $\bigotimes_{i=1}^{3} \sigma_{f(i)}$, $f(i) \in \{0,3\}$. There are 8 of them. An I-Z set is a set of I-Z operators.

Using the described method, a failing set was found. In fact several failing sets were found but they turned out to be equivalent. The set that was found, which we refer to as the I-Z failing set, was \{IIZ,IZI,ZII,ZZZ\}.

The notion of Clifford equivalence comes into play here.

**Definition 3.5.** Two sets of Pauli operators $\mathcal{P}_1 = \{P_i : 1 \leq i \leq k\}$ and $\mathcal{P}_2 = \{P_j : 1 \leq j \leq k\}$ are called Clifford equivalent if for some $C$ of the Clifford group, $CP_iC^\dagger \in \mathcal{P}_2$ for all $i$ (ignoring phases).

It can be easily shown through similar matrices that any set which is Clifford equivalent to a failing set is also a failing set. Using this fact we can construct the collection of all failing sets Clifford equivalent to the I-Z failing set. $\mathcal{F} = \{F : F \simeq \{IIZ,IZI,ZII,ZZZ\}\}$.

Using the python package QuaEC [10] $\mathcal{F}$ was found by successively applying every Clifford operator to the I-Z failing set and removing any duplicates. After eliminating duplicates $\mathcal{F}$ contains 945 failing sets.

As noted earlier we require a set of Pauli operators $\mathcal{P}$ which does not contain any failing set. Since all the failing sets we know of contain four operators, this constraint is equivalent to the requirement that $\mathcal{P} \cap \mathcal{F}$ has no more than 3 elements in it. Another way to think of this is to require that for every failing set, at least one operator in that failing set must be an element of $A$, the measured operators. This effectively converts the problem of
finding the largest set $P$ which does not contain any failing set into the problem of finding the smallest set of operators $A$ such that $A \cap F \neq \emptyset$ for all $F \in \mathcal{F}$. Although it is not immediately obvious, this is a well-known problem called the set cover problem.

The set cover problem is typically stated as follows. A collection $S$ of subsets of a given universe of elements $U = \{x_1, x_2, \ldots, x_n\}$ is called a cover if the union of all subsets in $S$ is $U$. The optimization set cover problem is to find the smallest collection of subsets which cover $U$ [14] [21].

In order to view our problem as a set cover problem, view the failing sets $F_j$ as the elements of the universe $\mathcal{F}$. The subsets are then $S_i = \{F_j : P_i \in F_j, 1 \leq i \leq N\}$ where $N$ is the number of Pauli operators of the system less the identity, in the three qubit case this is 63. In essence the $i$-th subset is the collection of all failing sets which have the $i$-th Pauli as an element. If this Pauli is included in the set of measured operators $A$, then those failing sets are ‘covered’.

The set cover decision problem, where if given some $k$ you determine if there is a covering set with $k$ or less sets, was shown to be NP-complete by Richard Karp in 1972 [17]. The optimization problem, where the smallest cover is found can be shown to be NP-hard, that is, at least as hard as an NP-complete problem (in this case the decision problem) [5] [8]. This is easy to prove since if an oracle exists which solves the optimization problem, the decision problem can be solved in polynomial time with use of the oracle which satisfies the definition of NP-hard. Brute forcing the problem is therefore impractical with 63 operators to choose from and 945 failing sets to cover. However since it is such a well-known problem in computer science there are several algorithms which have been devised for
various equivalent forms of this problem [27]. Two common forms of this problem are binary integer programming where it is formulated as a linear algebra problem with constraints [23], or a method known as Hyper-graph Dualization [2] which is the method we ended up using.

**Definition 3.6.** A hyper-graph $G = (V, F)$ is a set of vertices $V$ along with a collection of hyper-edges $F \subseteq V$. Each hyper edge is a subset of the vertices. A ‘hitting set’ $H$ is a subset of the vertices such that the intersection of $H$ with any hyper-edge is non-empty. A minimal hitting set is a hitting set which does not contain any other hitting set within it.

In other words every hyper-edge has at least one vertex which is contained in the hitting set [13]. The connection to our problem is immediately evident, the vertices are all of the Pauli operators and the hyper-edges are the failing sets. Our goal is to find the smallest minimal hitting set of this hyper-graph. The dual of the hyper-graph $G' = (V, F')$ is the same set of vertices but the hyper-edges are now the minimal hitting sets [7]. Once the hyper-graph is dualized, finding the smallest hitting set is a simple matter of searching a list of minimal hitting sets.

We could have directly fed the collection of failing sets into a hyper-graph dualization algorithm found in [22]. However since this problem is intractable, in order to save on computational time, it is ideal to start the program with as many operators already chosen as possible without losing generality. To this end we already know that any single Pauli can be chosen without loss of generality since every set of a single Pauli is Clifford equivalent to every other one. In order to reduce the problem further we made the following observations by analysing the collection of failing sets we had produced.
Observation 1. For any 3-qubit Pauli operator \( P \), let

\[
\chi(P) = \{F \in \mathcal{F} : P \in F\}.
\] (3.4)

We have the following observations for the set \( \mathcal{F} \) and function \( \chi \):

1. \(|\chi(P)| = 60\) for any Pauli operator \( P \).

2. \(|\chi(P_1) \cap \chi(P_2)| = 6\) or 0 for any two distinct Pauli operators \( P_1, P_2 \).

3. \(|\chi(P_1) \cap \chi(P_2) \cap \chi(P_3)| = 1\) or 0 for any three distinct Pauli operators \( P_1, P_2, P_3 \).

4. \(|\chi(P_1) \cap \chi(P_2) \cap \chi(P_3) \cap \chi(P_4)| = 1\) or 0 for any four distinct Pauli operators \( P_1, P_2, P_3, P_4 \).

5. \(|\chi(P_1) \cap \chi(P_2) \cap \cdots \cap \chi(P_k)| = 0\) for any \( k \) distinct Pauli operators \( P_1, \ldots, P_k \) when \( k > 4 \).

Assume \( S = \{P_1, P_2, \ldots, P_m\} \) is the smallest set which intersects any \( F \in \mathcal{F} \). Then we have \(|\chi(P_1) \cup \chi(P_2) \cup \cdots \cup \chi(P_m)| = |\mathcal{F}| = 945\).

According to the inclusion-exclusion principle [28], we also have

\[
|\chi(P_1) \cup \chi(P_2) \cup \cdots \cup \chi(P_m)| = \\
\sum_{i=1}^{m} |\chi(P_i)| - \sum_{1 \leq i < j \leq m} |\chi(P_i) \cap \chi(P_j)| + \sum_{1 \leq i < j < k \leq m} |\chi(P_i) \cap \chi(P_j) \cap \chi(P_k)| \\
- \sum_{1 \leq i < j < k < l \leq m} |\chi(P_i) \cap \chi(P_j) \cap \chi(P_k) \cap \chi(P_l)|. \quad (3.5)
\]
By combining the above two equations, we thus have

\[ 945 = \sum_{i=1}^{m} |\chi(P_i)| - \sum_{1 \leq i < j \leq m} |\chi(P_i) \cap \chi(P_j)| + \sum_{1 \leq i < j < k \leq m} |\chi(P_i) \cap \chi(P_j) \cap \chi(P_k)| - \sum_{1 \leq i < j < k < l \leq m} |\chi(P_i) \cap \chi(P_j) \cap \chi(P_k) \cap \chi(P_l)|. \]  

(3.6)

This implies that there exist \(1 \leq i, j, k \leq m\) such that \(P_i \cap P_j \cap P_k \neq \emptyset\). Without loss of generality, we can assume \(P_1, P_2, P_3\) are chosen from any \(F \in \mathcal{F}\). Let \(F = \{IIZ, IZI, ZII, ZZZ\}\). Note that any 3-tuple in \(F\) is Clifford equivalent to other 3-tuples. Again, without loss of generality, we can assume \(P_1 = IIZ, P_2 = IZI, P_3 = ZII \in S\).

We must choose some Pauli operator from \(\{IXX, IXI, ZIX, ZXI\} \in \mathcal{F}\). Observe that the following sets \(\{IIZ, IZI, ZII, IIX\}, \{IIZ, IZI, ZII, IXI\}, \{IIZ, IZI, ZII, IIX\}\) and \(\{IIZ, IZI, ZII, ZXI\}\) are Clifford equivalent. It implies that we can choose \(P_4 = IIX \in S\) without loss of generality.

Similarly, we must choose some Pauli operator from \(\{IXZ, XIZ, YZX, ZYX\} \in \mathcal{F}\). Since the following sets \(\{IXX, IIZ, IZI, ZII, IXZ\}, \{IXX, IIZ, IZI, ZII, XIX\}, \{IXX, IIZ, IZI, ZII, YZX\}\) and \(\{IXX, IIZ, IZI, ZII, ZYX\}\) are Clifford equivalent. Hence, without loss of generality, \(P_5 = IXZ \in S\).

Unfortunately, this procedure cannot continue because we cannot find another \(F \in \mathcal{F}\) such that \(\{IIZ, IZI, ZII, IIX, IXZ\} \cup \{P_6\} (P_6 \in \mathcal{F})\) is unique up to Clifford.

Hence we can fix 5 Pauli operators when running a program to find all hitting sets. Furthermore, if we want to fix 6 Pauli operators, then we have 2 cases. This greatly improves the time it takes to run the dualization program. Once finished we obtained a smallest minimal hitting set of 30 Pauli operators.
Theorem 3.2. The set

\[ \{IIX, IIX, IIZ, IXI, IXX, IXY, IYI, IYX, IYY, IZI, \\
XIZ, XXX, XXY, XYX, XYY, XZX, XZY, YXX, YXY, YXZ, \\
YYX, YYY, YYZ, YZI, ZII, ZXZ, ZYX, ZZX, ZYY, ZZZ \} \] (3.7)

and those Clifford equivalent to it are the smallest minimal hitting set of the hyper-graph constructed of the failing sets. No minimal hitting set of 29 Paulis exists.

As a result, there is no set of 34 Pauli operators for which all real linear combinations of them have at least two positive and two negative eigenvalues since any set of 34 Paulis must contain at least one failing set.

It is important to remember that it was never proved that the $I-Z$ failing set and those Clifford equivalent to it are the only failing sets. We performed many searches for other sets and also tried to prove that the $I-Z$ failing set was in fact the only failing set but none of these attempts produced any results. Therefore we must now prove that this set which we have obtained from the Hypergraph Dualization algorithm is UDA for all pure states.

Theorem 3.3. Any Hermitian operator perpendicular to

\[ \{IIX, IIX, IIZ, IXI, IXX, IXY, IYI, IYX, IYY, IZI, \\
XIZ, XXX, XXY, XYX, XYY, XZX, XZY, YXX, YXY, YXZ, \\
YYX, YYY, YYZ, YZI, ZII, ZXZ, ZYX, ZZX, ZYY, ZZZ \} \] (3.8)
must have at least two positive and two negative eigenvalues.

Proof. The proof proceeds as follows. First construct an 8-by-8 traceless Hermitian matrix $H$ which is perpendicular to all the above Pauli operators. This will be a real linear combination of every Pauli operator that is not being measured. This $H$ is then a general description of every possible Hermitian matrix in the complement of the span measured operators. We will show through a case by case analysis that if we assume $H$ only has one positive eigenvalue, then it follows that $H$ must be the zero matrix. A similar argument holds for having only one negative eigenvalue therefore $H$ must have at least two positive and two negative eigenvalues.

Let us begin by constructing $H$ which is a real linear combination of the 33 Pauli operators not being measured (excluding the identity). $H$ is then:

$$H = x_1IXZ + x_2IYZ + x_3IZX + x_4IZY + x_5IZZ + x_6XII + x_7XIX + x_8XIY + x_9XXI + x_{10}XXZ + x_{11}XYI + x_{12}XYZ + x_{13}ZXI + x_{14}ZIY + x_{15}YII + x_{16}YIX + x_{17}YIF + x_{18}YIZ + x_{19}YXI + x_{20}YYI + x_{21}YXY + x_{22}YZZ + x_{23}ZIX + x_{24}ZIY + x_{25}ZIZ + x_{26}ZXI + x_{27}ZXX + x_{28}ZXY + x_{29}ZYY + x_{30}ZYI + x_{31}ZYX + x_{32}ZYY + x_{33}ZZI.$$
Writing $H$ in matrix form will give the form:

\[
\begin{bmatrix}
  c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} & c_{17} & 0 \\
  c_{12} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} & 0 & c_{28} \\
  c_{13} & c_{23} & c_{33} & c_{34} & c_{35} & 0 & c_{37} & c_{38} \\
  c_{14} & c_{24} & c_{34} & c_{44} & 0 & c_{46} & c_{47} & c_{48} \\
  c_{15} & c_{25} & c_{35} & 0 & c_{55} & c_{56} & c_{57} & c_{58} \\
  c_{16} & c_{26} & 0 & c_{46} & c_{56} & c_{66} & c_{67} & c_{68} \\
  c_{17} & 0 & c_{37} & c_{47} & c_{57} & c_{67} & c_{77} & c_{78} \\
  0 & c_{28} & c_{38} & c_{48} & c_{58} & c_{68} & c_{78} & c_{88}
\end{bmatrix}
\]
where

\[ c_{11} = x_5 + x_{26} + x_{33}; \]  
\[ c_{22} = -x_5 - x_{26} + x_{33}; \]  
\[ c_{33} = -x_5 + x_{26} - x_{33}; \]  
\[ c_{44} = x_5 - x_{26} - x_{33}; \]  
\[ c_{55} = x_5 - x_{26} - x_{33} = c_{44}; \]  
\[ c_{66} = -x_5 + x_{26} - x_{33} = c_{33}; \]  
\[ c_{77} = -x_5 - x_{26} + x_{33} = c_{22}; \]  
\[ c_{88} = x_5 + x_{26} + x_{33} = c_{11}; \]  
\[ c_{12} = x_3 + x_{24} - i(x_4 + x_{25}); \]  
\[ c_{34} = -x_3 + x_{24} + i(x_4 - x_{25}); \]  
\[ c_{56} = x_3 - x_{24} - i(x_4 - x_{25}) = -c_{34}; \]  
\[ c_{78} = -x_3 - x_{24} + i(x_4 + x_{25}) = -c_{12}; \]  
\[ c_{13} = x_1 + x_{27} - i(x_2 + x_{30}); \]  
\[ c_{24} = -x_1 + x_{27} + i(x_2 - x_{30}); \]  
\[ c_{57} = x_1 - x_{27} - i(x_2 - x_{30}) = -c_{24}; \]  
\[ c_{68} = -x_1 - x_{27} + i(x_2 + x_{30}) = -c_{13}; \]  
\[ c_{14} = x_{28} - x_{32} - i(x_{29} + x_{31}); \]  
\[ c_{23} = x_{28} + x_{32} + i(x_{29} - x_{31}); \]  
\[ c_{58} = -x_{28} + x_{32} + i(x_{29} + x_{31}) = -c_{14}; \]  
\[ c_{67} = -x_{28} - x_{32} - i(x_{29} - x_{31}) = -c_{23}; \]  
\[ (3.30) \]
\[ \begin{align*}
c_{15} &= x_6 + x_{13} + x_{14} - i(x_{15} + x_{18} + x_{23}); \\
c_{26} &= x_6 + x_{13} - x_{14} - i(x_{15} - x_{18} - x_{23}); \\
c_{37} &= x_6 - x_{13} - x_{14} - i(x_{15} + x_{18} - x_{23}); \\
c_{48} &= x_6 - x_{13} + x_{14} - i(x_{15} - x_{18} + x_{23}) = c_{15}^* - c_{26}^* + c_{37}^*; \\
c_{16} &= x_7 - x_{17} - x_{22} - i(x_8 + x_{16} + x_{21}); \\
c_{25} &= x_7 + x_{17} + x_{22} + i(x_8 - x_{16} - x_{21}); \\
c_{38} &= x_7 - x_{17} + x_{22} - i(x_8 + x_{16} - x_{21}); \\
c_{47} &= x_7 + x_{17} - x_{22} + i(x_8 - x_{16} + x_{21}) = c_{16}^* + c_{25}^* - c_{38}^*; \\
c_{17} &= x_9 + x_{10} - x_{20} - i(x_{11} + x_{12} + x_{19}); \\
c_{28} &= x_9 - x_{10} - x_{20} - i(x_{11} - x_{12} + x_{19}); \\
c_{35} &= x_9 + x_{10} + x_{20} + i(x_{11} + x_{12} - x_{19}); \\
c_{46} &= x_9 - x_{10} + x_{20} + i(x_{11} - x_{12} - x_{19}) = c_{28}^* + c_{35}^* - c_{17}^*; \\
\end{align*} \]

Note that the main anti-diagonal is all zeros. This was by design, since any set of Pauli operators Clifford equivalent to the result from the hyper-graph dualization program is also a solution, we had the freedom to choose a set which would make the proof simpler. Choosing the set of operators which contained all Pauli operators constructed by tensoring only \( X \) operators and \( Y \) operators meant \( H \) would have zero main anti-diagonal. The only reason for choosing this set is it makes this proof a little simpler.

Here we assume \( H \) is a Hermitian matrix with only one positive eigenvalue. We
first show all diagonal entries of $H$ must be zero. Observe that $c_{55} = c_{44}$, $c_{66} = c_{33}$, $c_{77} = c_{22}$, $c_{88} = c_{11}$. In order for the traceless condition on $H$ to hold, it is then clear that $c_{11} + c_{22} + c_{33} + c_{44} = 0$. If $H$ has some nonzero diagonal entry, then at least one of $c_{11}, c_{22}, c_{33}$ and $c_{44}$ will be positive. Without loss of generality, let $c_{11} > 0$, then the submatrix of $H$ formed by the rows $(1, 8)$ and columns $(1, 8)$, which will be of the form $c_{11} \cdot I$, will have two positive eigenvalues.

**Lemma 3.1.** Cauchy’s Interlacing Theorem states[16]:

Let:

$$A = \begin{bmatrix} B & C \\ C^\dagger & D \end{bmatrix}$$

be an $n$-by-$n$ Hermitian matrix, where $B$ has size $m$-by-$m$ $(m < n)$. If the eigenvalues of $A$ and $B$ are $\alpha_1 \leq \ldots \leq \alpha_n$ and $\beta_1 \leq \ldots \leq \beta_m$ respectfully. Then:

$$\alpha_k \leq \beta_k \leq \alpha_{k+m}$$

It follows from Cauchy’s interlacing property that if a principle submatrix of $H$ has 2 positive eigenvalues then $H$ also has at least two positive eigenvalues.
Hence, $H$ must be in the following form:

$$
H = \begin{bmatrix}
0 & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} & c_{17} & 0 \\
c_{12}^* & 0 & c_{23} & c_{24} & c_{25} & c_{26} & 0 & c_{28} \\
c_{13} & c_{23}^* & 0 & c_{34} & c_{35} & 0 & c_{37} & c_{38} \\
c_{14}^* & c_{24} & c_{34}^* & 0 & 0 & c_{28}^* + c_{35} - c_{17}^* & c_{16}^* + c_{25} - c_{38}^* & c_{15} - c_{26}^* + c_{37}^* \\
c_{15}^* & c_{25}^* & c_{35}^* & 0 & 0 & -c_{34} & -c_{24} & -c_{14} \\
c_{16}^* & c_{26}^* & 0 & c_{28} + c_{35} - c_{17} & -c_{34}^* & 0 & -c_{23} & -c_{13} \\
c_{17}^* & 0 & c_{37}^* & c_{16}^* + c_{25} - c_{38} & -c_{24}^* & -c_{23}^* & 0 & -c_{12} \\
0 & c_{28}^* & c_{38}^* & c_{15} - c_{26} + c_{37} & -c_{14}^* & -c_{13}^* & -c_{12}^* & 0
\end{bmatrix}.
$$

In fact, under the assumption that $H$ has only 1 positive eigenvalue, it follows from Cauchy’s interlacing theorem that any principle submatrix of $H$ cannot have more than one positive eigenvalue. Otherwise, we will have a contradiction.

Let us look at the submatrix formed by rows 1, 2, 4, 5 and the same columns. It is a traceless Hermitian matrix with determinant $|c_{14}c_{25} - c_{15}c_{24}|^2$. Again, if the submatrix has positive determinant, then it must have exactly two positive eigenvalues. Once again by applying Cauchy’s interlacing property, $H$ will have at least two positive eigenvalues. This immediately contradictions our assumption. The above argument argument implies that, under our assumption $H$ has only 1 positive eigenvalue, we have $|c_{14}c_{25} - c_{15}c_{24}|^2 \leq 0$. It is not surprising that the inequality holds if and only if the equality holds. Then we have $c_{14}c_{25} - c_{15}c_{24} = 0$.

Similarly, by considering other 4-by-4 submatrices constructed from the rows and
columns \(a, b, 4, 5\) where \(a, b\) are any two of the remain six rows, we can show that:

\[
\begin{align*}
    c_{14}c_{35} - c_{15}c_{34} & = 0; \\
    -c_{14}c_{34}^* - c_{15}(c_{28} + c_{35}^* - c_{17}) & = 0; \\
    -c_{14}c_{24}^* - c_{15}(c_{16} + c_{25}^* - c_{38}) & = 0; \\
    -c_{14}c_{14}^* - c_{15}(c_{15}^* - c_{26} + c_{37}) & = 0; \\
    c_{24}c_{35} - c_{25}c_{34} & = 0; \\
    -c_{24}c_{34}^* - c_{25}(c_{28} + c_{35}^* - c_{17}) & = 0; \\
    -c_{24}c_{24}^* - c_{25}(c_{16} + c_{25}^* - c_{38}) & = 0; \\
    -c_{34}c_{34}^* - c_{35}(c_{28} + c_{35}^* - c_{17}) & = 0; \\
    -c_{34}c_{24}^* - c_{35}(c_{16} + c_{25}^* - c_{38}) & = 0; \\
    -c_{34}c_{14}^* - c_{35}(c_{15}^* - c_{26} + c_{37}) & = 0; \\
    -c_{24}c_{28} + c_{34}^* (c_{16} + c_{25}^* - c_{38}) & = 0; \\
    -c_{14}(c_{28} + c_{35}^* - c_{17}) + c_{34}^* (c_{16} + c_{25}^* - c_{38}) & = 0; \\
    -c_{14}^*(c_{28} + c_{35}^* - c_{17}) + c_{34}^*(c_{15}^* - c_{26} + c_{37}) & = 0; \\
    -c_{14}^*(c_{16} + c_{25}^* - c_{38}) + c_{24}^*(c_{15}^* - c_{26} + c_{37}) & = 0.
\end{align*}
\]

The above equations will imply that the 8-by-2 submatrix formed by the 4-th and 5-th columns has rank at most 1.

The same argument can be used to prove that the 8-by-2 submatrices formed by
columns (1, 8), (2, 7) or (3, 6) also have rank at most 1.

As a straightforward consequence, \( H \) has rank no more than 4.

In other words, the \( k \)-th column and the \( (9-k) \)-th column are linearly dependant.

This means that there exist \( \lambda_1, \lambda_2, \lambda_3, \lambda_4 \) such that the following equations hold:

\[
\begin{align*}
\lambda_1 \overrightarrow{C_1} + (1 - \lambda_1) \overrightarrow{C_8} &= \lambda_2 \overrightarrow{C_2} + (1 - \lambda_2) \overrightarrow{C_7} = 0 \quad (3.59) \\
\lambda_3 \overrightarrow{C_3} + (1 - \lambda_3) \overrightarrow{C_6} &= \lambda_4 \overrightarrow{C_4} + (1 - \lambda_4) \overrightarrow{C_5} = 0 \quad (3.60)
\end{align*}
\]

Here we have used \( \overrightarrow{C_k} \) to represent the \( k \)-th column of the matrix \((3.44)\).

Let us start with a special case. Let \( \lambda_1 = 0 \). Then \( c_{12} = c_{13} = c_{14} = c_{28} = c_{38} = 0 \) and \( c_{15} = c_{26}^* - c_{37}^* \). \( H \) can be simplified as the following:

\[
H = \begin{pmatrix}
0 & 0 & 0 & 0 & c_{26}^* - c_{37}^* & c_{16} & c_{17} & 0 \\
0 & 0 & c_{23} & c_{24} & c_{25} & c_{26} & 0 & 0 \\
0 & c_{23}^* & 0 & c_{34} & c_{35} & 0 & c_{37} & 0 \\
0 & c_{24}^* & c_{34}^* & 0 & 0 & c_{35} - c_{17}^* & c_{16}^* + c_{25} & 0 \\
c_{26} - c_{37} & c_{25}^* & c_{35}^* & 0 & 0 & -c_{34} & -c_{24} & 0 \\
c_{16}^* & c_{26}^* & 0 & c_{35}^* - c_{17} & -c_{34}^* & 0 & -c_{23} & 0 \\
c_{17}^* & 0 & c_{37}^* & c_{16} + c_{25}^* & -c_{24}^* & -c_{23}^* & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
\quad (3.61)
\]

If we set \( c_{23} = c_{24} = c_{34} = 0 \), then the top-left 4-by-4 submatrix is zero. In this case, the characteristic polynomial of \( H \) contains only even powers. Thus \( H \) has only one
positive eigenvalue implies $H$ has only one negative eigenvalue too. As a consequence, the top-right 4-by-4 submatrix of $H$ has rank exactly 1.

As a result, any 2-by-2 submatrix of the top-right submatrix must have determinant zero. From suitable choices of submatrices we can obtain the following equations:

\begin{align*}
    c_{26}c_{37} &= 0 \quad (3.62) \\
    c_{26}(c_{26}^* - c_{37}^*) &= c_{16}c_{25} \quad (3.63) \\
    c_{37}(c_{26}^* - c_{37}^*) &= c_{17}c_{35} \quad (3.64) \\
    c_{16}(c_{16}^* + c_{25}) + c_{17}(c_{17}^* - c_{35}) &= 0 \quad (3.65)
\end{align*}

Using the above equations we can obtain:

\begin{align*}
    0 &= c_{16}(c_{16}^* + c_{25}) + c_{17}(c_{17}^* - c_{35}) \\
    &= c_{16}c_{25} - c_{17}c_{35} + |c_{17}|^2 + |c_{16}|^2 \\
    &= c_{26}(c_{26}^* - c_{37}^*) - c_{37}(c_{26}^* - c_{37}^*) + |c_{17}|^2 + |c_{16}|^2 \\
    &= |c_{26} - c_{37}|^2 + |c_{17}|^2 + |c_{16}|^2 \quad (3.66)
\end{align*}

This implies $c_{16} = c_{17} = 0$ and $c_{26} = c_{37}$. Also since $c_{26}c_{37} = 0$ we know that $c_{26} = c_{37} = 0$. Furthermore $c_{25}(c_{16}^* + c_{25}) = 0$ and $c_{35}(c_{35} - c_{17}^*) = 0$ will guarantee $c_{25} = c_{35} = 0$. Therefore $H$ is once again the zero matrix.

We must then assume at least one of $c_{23}, c_{24}, c_{34}$ must be nonzero. If $c_{23} \neq 0$, then by considering submatrices formed by rows/columns $(1, 2, 3, k) \ (5 \leq k \leq 8)$, we have $c_{16} = c_{17} = 0$ and $c_{26} = c_{37}$. For the case that $c_{24} = 0$ or $c_{34} = 0$, we will also have
\(c_{16} = c_{17} = 0\) and \(c_{26} = c_{37}\) by considering appropriately chosen submatrices.

We are then left with \(H\) in the form:

\[
H = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & c_{23} & c_{24} & c_{25} & c_{26} & 0 & 0 \\
0 & c_{23}^* & 0 & c_{34} & c_{35} & 0 & c_{26} & 0 \\
0 & c_{24}^* & c_{34}^* & 0 & 0 & c_{35} & c_{25} & 0 \\
0 & c_{25}^* & c_{35}^* & 0 & 0 & -c_{34} & -c_{24} & 0 \\
0 & c_{26}^* & 0 & c_{35}^* & -c_{34}^* & 0 & -c_{23} & 0 \\
0 & 0 & c_{26}^* & c_{25}^* & -c_{24}^* & -c_{23}^* & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}.
\] (3.67)

Now, recall the fact that the submatrices formed by the \(k\)-th and the \((9 - k)\)-th columns will always have rank 1. From this it can be shown we will have \(H\) is a zero matrix.

Take the submatrix formed by the second and seventh columns for example. Since they are linearly dependant, the determinant of any 2-by-2 submatrix must be zero. From this we can get that \(|c_{23}|^2 + |c_{26}|^2 = 0\). Therefore \(c_{23} = c_{26} = 0\). By similar arguments on various submatrices, \(H\) can be shown to be the zero matrix.

Thus, under our assumption that \(H\) has exactly one positive eigenvalue, \(\lambda_1 \neq 0\). Similarly, we can also prove that \(\lambda_1 \neq 1, \lambda_2, \lambda_3, \lambda_4 \neq 0, 1\). We can then assume from now on that \(H\) has no zero columns or rows.

Hence, there exists certain \(\lambda_1, \lambda_2, \lambda_3\) and \(\lambda_4 \neq 0, 1\) which satisfies equation 3.59.
Let us use $\Re$ and $\Im$ to denote the real part and imaginary part of a complex number. Then the above equations can be rewritten as linear equations of real numbers.

Let us use $M(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ to denote the 48-by-30 coefficient matrix. If we can prove that the coefficient matrix always has rank 30 for any $\lambda_1, \lambda_2, \lambda_3$ and $\lambda_4$, then it will imply that all $c_{ij}$'s are zeros which will immediately contradict our assumption.

Unfortunately, we are not that lucky. $M(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ will be degenerate under certain assignment of variables ($\lambda_1, \lambda_2, \lambda_3, \lambda_4$). For example, $\text{rank}(M(\frac{1+i}{2}, \frac{1+i}{2}, \frac{1+i}{2}, \frac{1+i}{2})) = 27 < 30$. However, we can still show that $M(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ will have rank 30 except for some degenerate cases which will be dealt with separately.

$$
\begin{bmatrix}
-C_1 & O & O & O & A_1 & O & O & O & O & O & O & O & O & O & O & O \\
B_2 & O & O & O & O & C_2 & O & O & O & O & O & O & O & O & O & O \\
A_1 & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O \\
-D_2 & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O \\
O & B_3 & O & O & C_3 & O & O & O & O & O & O & O & O & O & O & O \\
O & -C_1 & O & O & A_1 & O & O & O & O & O & O & O & O & O & O & O \\
O & A_1 & O & O & O & O & O & O & O & O & O & O & O & O & O & C_1 \\
O & -D_3 & O & O & O & O & O & O & O & O & O & O & O & O & O & A_3 \\
O & O & -C_1 & A_1 & O & O & O & O & O & O & O & O & O & O & O & O \\
O & O & B_4 & C_4 & O & O & O & O & O & O & O & O & O & O & O & O \\
O & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O \\
O & O & O & O & O & B_3 & O & O & C_3 & O & O & O & O & O & O & O \\
O & O & O & O & O & A_2 & O & O & O & O & O & O & C_2 & O & O & O \\
O & O & O & O & O & O & O & O & O & O & O & O & O & O & O & A_3 & O \\
O & O & O & O & O & O & O & O & C_2 & A_2 & O & O & O & O & O & O \\
O & O & O & O & O & O & O & O & C_2 & B_4 & C_3 & O & O & O & O & O \\
O & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O \\
O & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O \\
O & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O \\
O & O & O & O & O & -B_4 & O & O & O & O & O & O & O & O & O & O & O \\
O & O & O & O & O & -B_4 & O & O & O & O & O & O & O & O & O & O & O \\
O & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O & O \\
O & O & O & O & O & B_3 & O & O & -D_4 & A_3 & O & O & O & O & O & O \\
O & O & O & O & O & D_2 & O & O & -D_4 & A_4 & O & O & O & O & O & O \\
O & O & O & O & O & D_2 & O & O & A_2 & C_2 & O & O & O & O & O & O \\
O & O & O & O & O & A_1 & C_1 & O & O & O & O & O & -D_1 & O & O & D_1 & O \\
\end{bmatrix} = 0 (3.68)
$$
where

\[
A_i = \begin{bmatrix} \Re \lambda_i & \Im \lambda_i \\ \Im \lambda_i & -\Re \lambda_i \end{bmatrix},
B_i = \begin{bmatrix} \Re \lambda_i & -\Im \lambda_i \\ \Im \lambda_i & \Re \lambda_i \end{bmatrix},
\]

\[
C_i = \begin{bmatrix} 1 - \Re \lambda_i & \Im \lambda_i \\ -\Im \lambda_i & 1 - \Re \lambda_i \end{bmatrix},
D_i = \begin{bmatrix} 1 - \Re \lambda_i & -\Im \lambda_i \\ -\Im \lambda_i & -(1 - \Re \lambda_i) \end{bmatrix}
\]

(3.69)

At least one of the following situations must happen:

1. \[
\begin{bmatrix} -C_1 & A_1 \\ B_2 & C_2 \end{bmatrix}
\]
   has full rank. This implies \( c_{12} = c_{17} = 0 \).

2. \[
\begin{bmatrix} A_1 & C_1 \\ -D_2 & A_2 \end{bmatrix}
\]
   has full rank. This implies \( c_{12} = c_{28} = 0 \).

3. \[
\begin{bmatrix} B_3 & C_3 \\ -C_1 & A_1 \end{bmatrix}
\]
   has full rank. This implies \( c_{13} = c_{16} = 0 \).

4. \[
\begin{bmatrix} A_1 & C_1 \\ -D_3 & A_3 \end{bmatrix}
\]
   has full rank. This implies \( c_{13} = c_{38} = 0 \).

5. \[
\begin{bmatrix} -C_1 & A_1 \\ B_4 & C_4 \end{bmatrix}
\]
   has full rank. This implies \( c_{14} = c_{15} = 0 \).

6. \[
\begin{bmatrix} -C_2 & A_2 \\ B_3 & C_3 \end{bmatrix}
\]
   has full rank. This implies \( c_{23} = c_{26} = 0 \).
7. \[
\begin{bmatrix}
A_2 & C_2 \\
-D_3 & A_3
\end{bmatrix}
\] has full rank. This implies \(c_{23} = c_{37} = 0\).

8. \[
\begin{bmatrix}
-C_2 & A_2 \\
B_4 & C_4
\end{bmatrix}
\] has full rank. This implies \(c_{24} = c_{25} = 0\).

9. \[
\begin{bmatrix}
-C_3 & A_3 \\
B_4 & C_4
\end{bmatrix}
\] has full rank. This implies \(c_{34} = c_{35} = 0\).

10. \[
\det\begin{pmatrix}
-C_1 & A_1 \\
B_2 & C_2
\end{pmatrix} = \det\begin{pmatrix}
A_1 & C_1 \\
-D_2 & A_2
\end{pmatrix} = \det\begin{pmatrix}
B_3 & C_3 \\
-C_1 & A_1
\end{pmatrix} \\
= \det\begin{pmatrix}
A_1 & C_1 \\
-D_3 & A_3
\end{pmatrix} = \det\begin{pmatrix}
-C_1 & A_1 \\
B_4 & C_4
\end{pmatrix} = \det\begin{pmatrix}
-C_2 & A_2 \\
B_3 & C_3
\end{pmatrix} \\
= \det\begin{pmatrix}
A_2 & C_2 \\
-D_3 & A_3
\end{pmatrix} = \det\begin{pmatrix}
-C_2 & A_2 \\
B_4 & C_4
\end{pmatrix} = \det\begin{pmatrix}
-C_3 & A_3 \\
B_4 & C_4
\end{pmatrix} = 0.
\]

With assistance of symbolic computation package like Mathematica, we find that the only solution to the above equations is \(\Re\lambda_1 = \Re\lambda_2 = \Re\lambda_3 = \Re\lambda_4 = \frac{1}{2}\).

Here we will prove that there is no Hermitian matrix in the form (3.44) with only one positive eigenvalue for every situations:
1. $c_{12} = c_{17} = 0$. Any $H$ with only one positive eigenvalue must be in the following form:

$$H = \begin{bmatrix}
0 & 0 & c_{13} & c_{14} & c_{15} & c_{16} & 0 & 0 \\
0 & 0 & c_{23} & c_{24} & c_{25} & c_{26} & 0 & c_{28} \\
c_{13}^* & c_{23}^* & 0 & c_{34} & c_{35} & 0 & c_{37} & c_{38} \\
c_{14}^* & c_{24}^* & c_{34}^* & 0 & 0 & c_{28}^* + c_{35}^* & c_{16}^* + c_{25}^* - c_{38}^* & c_{15}^* - c_{26}^* + c_{37}^* \\
c_{15}^* & c_{25}^* & c_{35}^* & 0 & 0 & -c_{34}^* & -c_{24}^* & -c_{14}^* \\
c_{16}^* & c_{26}^* & 0 & c_{28}^* + c_{35}^* & -c_{34}^* & 0 & -c_{23}^* & -c_{13}^* \\
0 & 0 & c_{37}^* & c_{16}^* + c_{25}^* - c_{38}^* & -c_{24}^* & -c_{23}^* & 0 & 0 \\
0 & c_{28}^* & c_{38}^* & c_{15}^* - c_{26}^* + c_{37}^* & -c_{14}^* & -c_{13}^* & 0 & 0 
\end{bmatrix} \tag{3.70}$$

By considering submatrices formed by row/columns $(1, 2, p, q)$ where $3 \leq p < q \leq 8$, we have that the first two rows are linearly dependent. Under our assumption that there is no row of $H$ containing only zero entries, we have $c_{28} = 0$.

Recall that the 4-th and 5-th rows are linearly dependent, thus $c_{34}(c_{34}^*) = c_{35}(c_{28} + c_{35}^*)$ which now can be simplified as $|c_{34}|^2 + |c_{35}|^2 = 0$. Hence $c_{34} = c_{35} = 0$. Then
Again, by applying our submatrix argument, we have the submatrix formed by (3, 4, 5, 6) columns must has rank 1.

If there is a zero element in the submatrix formed by rows (1, 2, 7, 8) and columns (3, 4, 5, 6), then there must be a row or a column containing only zero elements in $H$.

So, here we assume the submatrix formed by rows (1, 2, 7, 8) and columns (3, 4, 5, 6) does not contain any zero element.

Then $\frac{c_{15}}{c_{25}} = \frac{c_{14}}{c_{23}} = \frac{c_{13}}{c_{37}}$ which implies $c_{38}c_{25} = c_{37}c_{15}$.

Follows from the rank 1 condition, we have

\[ c_{15}(c_{15}^* - c_{26} + c_{37}) = -|c_{14}|^2, \quad (3.72) \]
\[ c_{25}(c_{16} + c_{25}^* - c_{38}) = -|c_{24}|^2. \quad (3.73) \]

By substituting $c_{38}c_{25} = c_{37}c_{15}$ and $c_{15}c_{26} = c_{25}c_{16}$ into the above two equations, we
have

$$|c_{15}|^2 + |c_{14}|^2 = c_{15}c_{26} - c_{15}c_{37} = c_{25}c_{16} - c_{25}c_{38} = -|c_{24}|^2 - |c_{25}|^2$$  \hspace{1cm} (3.74)

which implies $c_{15} = c_{14} = c_{24} = c_{25} = 0$. However, it contradicts our assumption that there is no zero element in the submatrix formed by $(1,2,7,8)$ rows and $(3,4,5,6)$ columns.

Similarly, we can also prove that there is no Hermitian matrix in the form 3.44 with only one positive eigenvalue if any of the following conditions apply.

2. $c_{12} = c_{28} = 0$.

3. $c_{13} = c_{16} = 0$.

4. $c_{13} = c_{38} = 0$.

5. $c_{14} = c_{15} = 0$.

6. $c_{23} = c_{26} = 0$.

7. $c_{23} = c_{37} = 0$.

8. $c_{24} = c_{25} = 0$.

9. $c_{34} = c_{35} = 0$.

Now, the only case we left is the following:

10. $\Re \lambda_1 = \Re \lambda_2 = \Re \lambda_3 = \Re \lambda_4 = \frac{1}{2}$. In this case, $\text{rank} \left( \begin{bmatrix} -C_1 & A_1 \\ B_2 & C_2 \end{bmatrix} \right) = 3$. Hence
\((\Re c_{12}, \Im c_{12}, \Re c_{17}, \Im c_{17})\) lies in the nullspace of
\[
\begin{bmatrix}
-\frac{1}{2} & -b_1 & \frac{1}{2} & b_1 \\
 b_1 & -\frac{1}{2} & b_1 & -\frac{1}{2} \\
\frac{1}{2} & -b_2 & \frac{1}{2} & b_2 \\
b_2 & \frac{1}{2} & -b_2 & \frac{1}{2}
\end{bmatrix}
\].

Thus \([c_{12} : c_{17}] = [2(b_2 - b_1) + (1 + 4b_1b_2)i : 2(b_1 + b_2) + (4b_1b_2 - 1)i]\). Similarly, we will have

\[
[c_{12} : c_{17} : c_{28}] = [2(b_2 - b_1) + (1 + 4b_1b_2)i : 2(b_1 + b_2) + (4b_1b_2 - 1)i];
\]

\[
[c_{13} : c_{16} : c_{38}] = [2(b_1 - b_3) - (1 + 4b_1b_3)i : -2(b_1 + b_3) - (4b_1b_3 - 1)i];
\]

\[
[c_{23} : c_{26} : c_{37}] = [2(b_3 - b_2) + (4b_2b_3 + 1)i : 2(b_2 + b_3) + (4b_2b_3 - 1)i];
\]

\[
[c_{14} : c_{15}] = [2(b_4 - b_1) - (4b_1b_4 + 1)i : 2(b_1 + b_4) + (4b_1b_4 - 1)i];
\]

\[
[c_{24} : c_{25}] = [2(b_4 - b_2) + (4b_2b_4 + 1)i : 2(b_2 + b_4) + (4b_2b_4 - 1)i];
\]

\[
[c_{34} : c_{35}] = [2(b_4 - b_3) + (4b_3b_4 + 1)i : 2(b_3 + b_4) + (4b_3b_4 - 1)i].
\]

Here \([q_1 : q_2 : \cdots : q_m] = [r_1 + s_1i : r_2 + s_2i : \cdots : r_m + s_mi]\] means there exists some \(\mu \in \mathbb{R}\) such that \(q_i = \mu(r_i + s_i)\) for any \(1 \leq i \leq m\).
Observe that $c_{28} = -c_{17}, c_{38} = -c_{16}, c_{37} = -c_{26}$, we thus simplify the matrix form of $H$ as the following:

$$H = \begin{bmatrix}
0 & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} & c_{17} & 0 \\
0 & c_{12} & c_{23} & c_{24} & c_{25} & c_{26} & 0 & -c_{17} \\
0 & c_{12} & c_{23} & 0 & c_{34} & c_{35} & 0 & -c_{26} & -c_{16} \\
c_{14} & c_{24} & c_{34} & 0 & 0 & c_{35} - 2c_{17}^* & c_{25} + 2c_{16}^* & c_{15} - 2c_{26}^* \\
c_{15} & c_{25} & c_{35} & 0 & 0 & -c_{34} & -c_{24} & -c_{14} \\
c_{16} & c_{26} & 0 & c_{35} - 2c_{17} & -c_{34} & 0 & -c_{23} & -c_{13} \\
c_{17} & 0 & -c_{26} & c_{25} + 2c_{16} & -c_{24} & -c_{23} & 0 & -c_{12} \\
0 & -c_{17} & -c_{16} & c_{15} - 2c_{26} & -c_{14} & -c_{13} & -c_{12} & 0
\end{bmatrix}. \quad (3.81)$$

It follows from the fact that the submatrix formed by 4-th and 5-th columns has rank exactly 1, we have $c_{14}(-c_{14}^*) = c_{15}(c_{15}^* - 2c_{26})$. Thus at least one of the following cases must happen:

(10.1) $c_{14} = c_{15} = 0$. We can still assume there is no column containing only zero elements as this is the case that we have already discussed. Thus $c_{26} = 0$ which would also lead to $c_{23} = 0$.

(10.2) $c_{26} = c_{15}^*$.

Similarly, at least one of the following conditions:

(10.I) $c_{24} = c_{25} = c_{16} = c_{13} = 0$; or

(10.II) $c_{16} = -c_{25}^*$
and one of the following conditions:

(10.A) \( c_{34} = c_{35} = c_{17} = c_{12} = 0 \); or

(10.B) \( c_{17} = c_{35}^* \)

must apply.

We have already discussed the cases that \( c_{12} = c_{17} = 0 \), \( c_{13} = c_{16} = 0 \) or \( c_{23} = c_{26} = 0 \) previously. Hence the only remaining case is \( c_{26} = c_{15}^*, c_{16} = -c_{25}^*, c_{17} = c_{35}^* \). Thus

\[
H = \begin{bmatrix}
0 & c_{12} & c_{13} & c_{14} & c_{15} & -c_{25}^* & c_{35}^* & 0 \\
c_{12}^* & 0 & c_{23} & c_{24} & c_{25} & c_{15}^* & 0 & -c_{35}^* \\
c_{13}^* & c_{23}^* & 0 & c_{34} & c_{35} & 0 & -c_{15}^* & c_{25}^* \\
c_{14}^* & c_{24}^* & c_{34}^* & 0 & 0 & -c_{35} & -c_{25} & -c_{15} \\
c_{15}^* & c_{25}^* & c_{35}^* & 0 & 0 & -c_{34} & -c_{24} & -c_{14} \\
-c_{25} & c_{15} & 0 & -c_{35}^* & -c_{34}^* & 0 & -c_{23} & -c_{13} \\
c_{35} & 0 & -c_{15} & -c_{25}^* & -c_{24}^* & -c_{23} & 0 & -c_{12} \\
0 & -c_{35} & c_{25} & -c_{15}^* & -c_{14}^* & -c_{13}^* & -c_{12}^* & 0
\end{bmatrix}
\]  

(3.82)

According to \( c_{26} = c_{15}^* \), we have \( 2(b_2 + b_3)(1 - 4b_1b_4) = (4b_2b_3 - 1)(2b_1 + 2b_4) \) which implies \( 4(b_1b_2b_3 + b_1b_2b_4 + b_1b_3b_4 + b_2b_3b_4) = b_1 + b_2 + b_3 + b_4 \).

1. \( 4b_1b_2 + 4b_1b_3 + 4b_2b_3 = 1 \). Thus \( b_1 + b_2 + b_3 = 4b_1b_2b_3 \). However, one can easy to verify that there do not exist three real numbers \( b_1, b_2, b_3 \) satisfying these two equations.
2. $4b_1b_2 + 4b_1b_3 + 4b_2b_3 \neq 1$. Hence $b_4 = \frac{b_1 + b_2 + b_3 - 4b_1b_2b_3}{4b_1b_2 + 4b_1b_3 + 4b_2b_3 - 1}$. By substituting the assignment of $b_4$ into Equation 3.75, we have

$$c_{14} = p \cdot \left[ \frac{2(1 - 4b_1^2)(b_2 + b_3) + 4b_1(1 - 4b_2b_3)}{4b_1b_2 + 4b_1b_3 + 4b_2b_3 - 1} \right] - 8b_1(b_2 + b_3) + (1 - 4b_1^2)(1 - 4b_2b_3)$$

$$c_{15} = p \cdot \left[ \frac{2(1 + 4b_1^2)(b_2 + b_3)}{4b_1b_2 + 4b_1b_3 + 4b_2b_3 - 1} \right] + (1 + 4b_1^2)(1 - 4b_2b_3)$$

$$c_{23} = p \cdot \left[ \frac{2(1 + 4b_1^2)(b_3 - b_2)}{4b_1b_2 + 4b_1b_3 + 4b_2b_3 - 1} \right] + (1 + 4b_1^2)(1 + 4b_2b_3)$$

$$c_{24} = q \cdot \left[ \frac{2(1 - 4b_1^2)(b_1 + b_3) + 4b_2(1 - 4b_1b_3)}{4b_1b_2 + 4b_1b_3 + 4b_2b_3 - 1} \right] + 8b_2(b_1 + b_3) - (1 - 4b_2^2)(1 - 4b_1b_3)$$

$$c_{25} = q \cdot \left[ \frac{2(1 + 4b_1^2)(b_1 + b_3)}{4b_1b_2 + 4b_1b_3 + 4b_2b_3 - 1} \right] + (1 + 4b_1^2)(1 - 4b_1b_3)$$

$$c_{13} = q \cdot \left[ \frac{2(1 + 4b_1^2)(b_1 - b_3)}{4b_1b_2 + 4b_1b_3 + 4b_2b_3 - 1} \right] - (1 + 4b_1^2)(1 + 4b_1b_3)$$

$$c_{34} = r \cdot \left[ \frac{2(1 - 4b_1^2)(b_1 + b_2) + 4b_3(1 - 4b_1b_2)}{4b_1b_2 + 4b_1b_3 + 4b_2b_3 - 1} \right] + 8b_3(b_1 + b_2) - (1 - 4b_3^2)(1 - 4b_1b_2)$$

$$c_{35} = r \cdot \left[ \frac{2(1 + 4b_1^2)(b_1 + b_2)}{4b_1b_2 + 4b_1b_3 + 4b_2b_3 - 1} \right] + (1 + 4b_1^2)(1 - 4b_1b_2)$$

$$c_{12} = r \cdot \left[ \frac{2(1 + 4b_1^2)(b_2 - b_1)}{4b_1b_2 + 4b_1b_3 + 4b_2b_3 - 1} \right] + (1 + 4b_1^2)(1 + 4b_1b_2)$$

Again, with assistance of symbolic computation package like Mathematica, we can verify that the characteristic polynomial of $H$ contains only even powers.

This implies $H$ has nonzero eigenvalue $\lambda$ if and only if it also has eigenvalue $-\lambda$.

Therefore, under our assumption that $H$ has only 1 positive eigenvalue, $H$ also has only 1 negative eigenvalue.

However, let us consider the 3-by-3 submatrix of $H$ formed by $(5, 7, 8)$-th rows and $(1, 2, 3)$-th columns. Its determinant is $(-i + 2b_1)(i + 2b_1)^2(1 + 2ib_2)(i + 2b_2)^2(i - 2b_3)^2(i + 2b_3)^2r((1 + 4b_1^2)p^2 + (1 + 4b_2^2)q^2 + (1 + 4b_3^2)r^2)$. It is always
nonzero unless \( p = q = r \) or \( r = 0 \). If \( r = 0 \) this implies that \( c_{12} = c_{34} = c_{35} = 0 \).

This case has already been covered, Thus \( H \) has rank at least 3 which contradicts our previous conclusion that \( H \) has only one positive eigenvalue and only one negative eigenvalue.

To summarize, under our assumption that \( H \) has only one positive eigenvalue, a contradiction always exist in every situation we studied. Hence, \( H \) must has at least 2 positive eigenvalues and at least 2 negative eigenvalues. This completes our proof.

\[ \square \]

### 3.4 Conclusion

Here we have solved the problem of finding the set of Pauli operators needed to be measured in order for any three-qubit pure state to be UDA. Through the failing set construction, an intractable graph theory problem was found which would produce a lower bound for our problem. Through application of group theory this problem was reduced to the point where we could solve it exactly with use of specific computer algorithms. We then showed that the 30 Pauli lower bound obtained from this was achievable through explicit case by case proof that the span of the complement of this set always had two positive and two negative eigenvalues, ensuring that our set of 30 Pauli operators are enough to uniquely determine any pure state among all states.
Chapter 4

Future Directions

There are several directions for which this work could go in future directions. First, a paper published by N. Linden et. al [20] shows that the two particle reduced density matrices uniquely determine almost every three qubit state. The exception being the GHZ state. In their proof of this however they only needed two of the three reduced density matrices. This is equivalent to measuring 27 Pauli operators. Those with the identity on the first qubit, and those with the identity on the second qubit (or any other choice of 2 of the 3). We have already shown that this set is not contained in set Clifford equivalent to our set of 30 Paulis. In fact they overlap with a maximum of 17 Operators. However it would be interesting to assume these 27 operators and run the Hypergraph Dualization to find the minimal set including these operators which will also measure the GHZ state.

A similar direction of investigation is to see what happens if some operators are removed from our set of 30 and how large the set of pure states which are no longer UDA is.
It may be possible to construct a general framework which will be able to explain the results of N. Linden et al and the compressed sensing works all in terms similar to our construction here. Loosening our requirement that for a set of measurements every pure state be UDA, we can find sets of pure states which are uniquely determined among themselves. If successful this framework would prove a powerful tool not only for quantum tomography but general information theory as well.

To the end of obtaining a framework which should allow us to generalize our results to any size system, it would be helpful for us to produce similar results in the 4-case in order to better understand how to properly generalize. This may be difficult since the size of the Clifford group for four-qubits is $|C_4| = 12128668876800$. As such the greatest challenge in this direction will be to reduce the problem enough to allow it to be computationally viable to solve. This will require further group and graph theoretic results to be applied to the problem such as symmetry of the graph and any underlying group structure in the problem.
Bibliography


