# EVALUATING QUANTUM STATE VERIFICATION FOR $D$-LEVEL GRAPH STATES

MATACHAN OUPATAM

A Thesis Submitted to Graduate School of Naresuan University
in Partial Fulfillment of the Requirements
for the Master of Science Program in Theoretical Physics
May 2025

Thesis entitled “Evaluating Quantum State Verification for d-Level Graph States”

by Matachan Oupatam

has been approved by the Graduate School as partial fulfillment of

the requirement for the Master of Science Program in Theoretical Physics of

Naresuan University

**Oral Defense Committee**

..... Chair

(Tanapat Deesuwan, Ph.D.)

..... Advisor

(Ninnat Dangniam, Ph.D.)

..... Internal Examiner

(Associate Professor Sikarin Yoo-Kong, Ph.D.)

**Approved**

.....

(Assistant Professor Chommanad Intajamornrak, Ph.D)

Head, Department of linguistics, Folklore, Philosophy and Region, Faculty of Humanities

Acting Dean of Graduate School

# ACKNOWLEDGMENTS

I would like to sincerely thank my advisor, Dr. Ninnat Dangniam, for his continuous guidance and valuable advice throughout this work. I am especially grateful for his patience in answering my questions, even when I repeated the same ones many times. His simple suggestion to "start with what can be done first" encouraged me to try writing Python code to test my expression in all possible cases. That process helped me discover patterns in the problem and led to a more analytic way of proving our results.

I would also like to thank my friends and colleagues at the Institute for Fundamental Study, Naresuan University, for their support and for creating a friendly and motivating research environment.

This work was supported by the Development and Promotion of Science and Technology Talents Project (DPST), which I gratefully acknowledge.

Finally, I would like to express my appreciation to the large language models that I used during this research. They played an important role in helping me write this thesis and complete the work successfully.

Matachan Oupatam

| | |
|---|---|
| **Title** | EVALUATING QUANTUM STATE VERIFICATION FOR $D$-LEVEL GRAPH STATES |
| **Author** | Matachan Oupatam |
| **Advisor** | Ninnat Dangniam, Ph.D. |
| **Academic Paper** | M.S. Thesis in Theoretical Physics, Naresuan University, 2025 |
| **Keywords** | Measurement, Graph state, Quantum state verification |


# ABSTRACT

Quantum State Verification (QSV) attempts to figure out if, at a certain confidence level, an unknown quantum state is sufficiently near to a fixed target state. The spectral gap of the verification operator is inversely proportional to the number of identical, independent copies, $N$, needed for this operation. A significant class of quantum states that often feature in quantum computing are stabilizer states. These states' structural characteristics make it easier to express and simulate quantum states mathematically. They are specified by a collection of stabilizer operators that are derived from Pauli matrices in qubit systems. These characteristics also make stabilizer states particularly suitable for local measurement-based verification processes.

Previous research by Dangniam et al. has demonstrated that the spectral gap for qubit stabilizer states cannot exceed $2/3$ when the verification operator is restricted to local measurements. Building upon their methodology, we extend these results to graph states in $d$-level systems, where $d$ is a prime number. Specifically, we establish that the spectral gap for these systems is upper-bounded by $d/(d+1)$. This problem is reduced to the case of bipartite maximally entangled $d$-level systems, for which the optimal spectral gap is known from the work of Li et al. Our derivation leverages the property that $d$-level graph states exhibit maximal entanglement across all possible bipartitions of the graph.

# LIST OF CONTENTS

**Chapter** **Page**

# LIST OF CONTENTS (CONT.)

**Chapter** **Page**

# LIST OF FIGURES

**Figure** **Page**

# CHAPTER I

# INTRODUCTION

Quantum computing has emerged as a significant paradigm in information processing, rooted in the fundamental principles of quantum mechanics. By utilizing phenomena such as superposition and entanglement, quantum systems offer a fundamentally different approach to processing information compared to classical computers.

However, realizing practical quantum computers remains challenging. Quantum information is fragile and highly sensitive to environmental interactions, which can introduce noise and lead to decoherence. As a result, one of the main tasks in quantum technologies is not only to build quantum processors but also to develop effective methods for controlling and verifying their behavior. Before using a quantum device for meaningful computation, we need reliable ways to check whether it has prepared the intended quantum state.

## 1.1 The Problem of Quantum State Tomography

A standard method to characterize an unknown quantum state is Quantum State Tomography (QST). This technique aims to reconstruct the complete density matrix of a system, offering a full description of the state. While conceptually straightforward, the practicality of QST is limited by its significant resource requirements, which scale with the dimension of the Hilbert space, $D$.

For a general mixed state, early studies showed that QST requires a number of measurements that grow polynomially with the dimension $D$. Specifically, it requires measurements from a set of $O(D)$ mutually unbiased bases [1, 2, 3] or, more generally, the outcome probabilities associated with a set of $O(d^2)$ POVM elements [4, 5, 6, 7]. This becomes quickly impractical for systems with many

particles (like qubits), as the Hilbert space dimension $d$ grows exponentially with the number of constituents $n$. For an $n$-qubit system, where $d = 2^n$, the number of POVM measurements scales as $O\left((2^n)^2\right) = O\left(4^n\right)$ [8].

Due to these scalability challenges, alternative approaches have been proposed that focus on verifying if a system is in a specific target state, rather than performing a full tomographic reconstruction of the entire quantum state.

## 1.2 A Practical Alternative: Quantum State Verification (QSV)

Quantum State Verification (QSV) offers a more scalable solution. Instead of learning the exact state, the goal is to determine whether the prepared state is sufficiently close to a known target state, or whether it deviates from it by at least some small amount $\epsilon$, typically measured using fidelity. This is framed as a hypothesis testing problem [9, 10].

A QSV protocol aims to make this distinction with a high level of confidence (at least $1 - \delta$) while using as few copies of the quantum state as possible [11, 10]. For many important families of states, including stabilizer/graph states, QSV can be performed efficiently, making it a valuable tool in quantum experiments and benchmarking [12, 11, 13].

## 1.3 The Role of the Spectral Gap

The main factor that determines the efficiency of a QSV protocol is the number of copies $N$ of the unknown state needed to reach a decision. This number is related to the spectral gap $\nu(\Omega)$ of the verification operator $\Omega$, which corresponds to the measurement used to decide whether the state passes the test [11, 9]:

$$N \approx \frac{\ln(1/\delta)}{\epsilon\, \nu(\Omega)} \tag{1.1}$$

To minimize the number of copies, it is important to design a verification operator

$\Omega$ that maximizes the spectral gap. In practical settings, it is often desirable to use local measurements—those that act on individual qudits—since they are easier to implement than global or entangled measurements. This work focuses on the efficiency of QSV under this local measurement constraint.

## 1.4 Motivation and Scope of This Study

Within the broader class of quantum states, stabilizer states are particularly important due to their applications in quantum error correction, measurement-based quantum computing, and quantum communication. A notable subclass is the family of graph states, which can be described by a graph where nodes represent qudits and edges indicate entanglement.

For qubit stabilizer states ($d = 2$), it has been shown that the largest possible spectral gap under local measurements is $2/3$ [12]. For a special class of qudit states called generalized maximally entangled states, the upper bound is known to be $d/(d + 1)$ [14]. However, for general qudit graph states, this question had not been fully answered.

This thesis addresses that open problem. We study the case where the local dimension $d$ is a prime number, which allows us to use mathematical tools from finite field. The aim is to determine whether the known upper bound $d/(d + 1)$ also applies to more general graph states under local measurements.

## 1.5 Research Questions

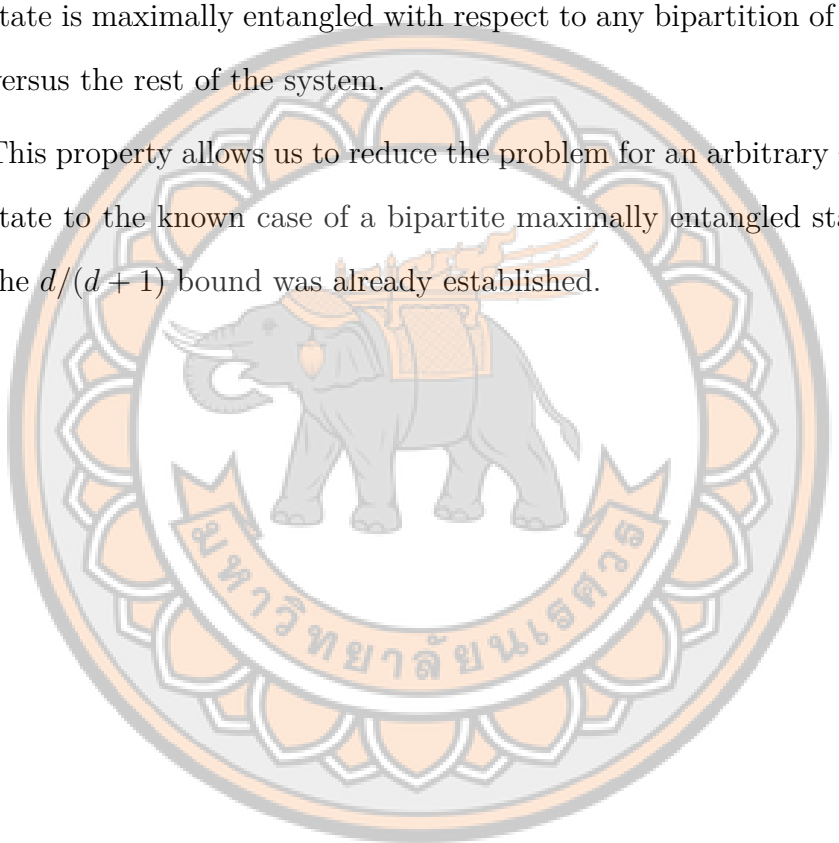
This work is driven by two main questions:

1. What is the maximum spectral gap achievable when verifying general $d$-level graph states using only local measurements?
2. Can the proof techniques used for qubit systems, which involve reducing the

problem to a simple bipartite case, be successfully generalized to the more complex qudit formalism?

The key contributions of this thesis are as follows:

1. The upper bound on the spectral gap for any $d$-level graph state (with $d$ prime) under local verification is $d/(d+1)$.
2. This result is derived by proving a key structural property: any $d$-level graph state is maximally entangled with respect to any bipartition of a single qudit versus the rest of the system.
3. This property allows us to reduce the problem for an arbitrary $n$-qudit graph state to the known case of a bipartite maximally entangled state, for which the $d/(d+1)$ bound was already established.



# CHAPTER II

# THEORETICAL FRAMEWORK

To analyze and evaluate the efficiency of quantum state verification (QSV), it is first necessary to establish the mathematical foundation of quantum information theory for multi-level systems. This chapter outlines the core physical and mathematical concepts utilized throughout this thesis. We begin by defining $d$-level quantum states (qudits), density operators, and the critical concept of entanglement. This foundational background is primarily drawn from [15, 16]. Following this, we formulate the framework of quantum measurements, starting with positive operator-valued measures (POVMs) and the restrictions imposed by local operations. Finally, we review the methodology of quantum state tomography (QST) for qudits, illustrating the exponential resource scaling that makes QSV a necessary alternative.

## 2.1 Description of Quantum State

### 2.1.1 Qubits, Qudits, and Hilbert Space

The most elementary unit of classical information is the bit, a system that can exist in one of two definite states, labeled 0 and 1 . The quantum analogue is the qubit, a two-level quantum system. Unlike a classical bit, a qubit can exist not only in the definite states $|0\rangle$ and $|1\rangle$, but also in a superposition of both. These basis states, $|0\rangle$ and $|1\rangle$, form an orthonormal basis for a two-dimensional complex vector space known as a Hilbert space, denoted $\mathcal{H}_2$. A general pure state of a qubit, $|\psi\rangle$, is a normalized vector in this space, expressed as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.1}$$

where $\alpha$ and $\beta$ are complex numbers called probability amplitudes. The normal-

ization condition, $|\alpha|^2 + |\beta|^2 = 1$, ensures that the probabilities of measuring the state to be $|0\rangle$ or $|1\rangle$ sum to one.

This concept naturally generalizes to systems with more than two levels. A qudit is a generic quantum system associated with a $d$-dimensional complex Hilbert space, denoted as $\mathcal{H}_d \cong \mathbb{C}^d$. The standard basis for this space, known as the computational basis, consists of $d$ orthonormal vectors labeled by the integers $\{0, 1, \ldots, d-1\}$:

$$\mathcal{B} = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}. \tag{2.2}$$

These basis vectors satisfy the orthonormality condition $\langle i|j\rangle = \delta_{ij}$. A general pure state $|\psi\rangle \in \mathcal{H}_d$ is a superposition of these basis vectors:

$$|\psi\rangle = \sum_{i=0}^{d-1} c_i |i\rangle, \tag{2.3}$$

where $c_i \in \mathbb{C}$ are probability amplitudes satisfying the normalization condition $\sum_k |c_i|^2 = 1$.

For a system composed of $n$ qudits, the total Hilbert space is the tensor product of the individual spaces:

$$\mathcal{H} = \mathcal{H}_d^{(1)} \otimes \mathcal{H}_d^{(2)} \otimes \cdots \otimes \mathcal{H}_d^{(n)} \cong (\mathbb{C}^d)^{\otimes n}. \tag{2.4}$$

The dimension of this composite space grows exponentially as $D = d^n$.

### 2.1.2 Density Operators

The state vector $|\psi\rangle$ provides a complete description of a pure state, which corresponds to a quantum system in a precisely defined state. However, in many practical situations, our knowledge of the system is incomplete. Consequently, the description of the system is a statistical mixture of pure states. To handle these cases, we employ a more general tool: the density operator (or density matrix), $\rho$.

When a quantum system is not described by a single state vector, its state is represented by a density operator $\rho$. This is a positive semidefinite operator with

unit trace,

$$\rho \succeq 0, \quad \mathrm{Tr}(\rho) = 1. \tag{2.5}$$

A pure state $|\psi\rangle$ corresponds to the density operator

$$\rho = |\psi\rangle\langle\psi|. \tag{2.6}$$

A general mixed state is given by a convex combination of pure states,

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad p_i \geq 0, \quad \sum_i p_i = 1. \tag{2.7}$$

The purity of a state is defined as

$$\gamma(\rho) := \mathrm{Tr}(\rho^2). \tag{2.8}$$

It satisfies

$$\frac{1}{d} \leq \gamma(\rho) \leq 1, \tag{2.9}$$

with $\gamma(\rho) = 1$ if and only if $\rho$ is pure.

### 2.1.3 Reduced Density Operator

While the density operator describes statistical mixtures arising from classical uncertainty, it plays an even more critical role in the context of composite quantum systems. When a system is composed of two parts, $A$ and $B$, that are entangled, the state of subsystem $A$ alone cannot be described by a state vector $|\psi\rangle_A$.

Even if the global state of the total system $|\Psi\rangle_{AB}$ is a definite pure state (perfect knowledge of the whole), an observer looking only at subsystem $A$ possesses incomplete knowledge. The information about $A$ is effectively lost to the correlations with $B$.

To describe this local state, we use the Reduced Density Operator, $\rho_A$. Mathematically, this is obtained by "tracing out" subsystem $B$:

$$\rho_A = \mathrm{Tr}_B(|\Psi\rangle_{AB}\langle\Psi|) \tag{2.10}$$

Just like the statistical mixtures described above, this reduced state $\rho_A$ is a mixed state. The more entangled the global system is, the more mixed the local reduced state becomes.

### 2.1.4 Schmidt Decomposition and Entanglement

#### 2.1.4.1 Schmidt Decomposition.

When analyzing correlations in bipartite quantum systems, the Schmidt decomposition provides a form that simplifies the description of pure states. It is a fundamental tool for quantifying entanglement, as it allows us to express a composite state using a minimum number of terms in an orthogonal basis.

**Theorem:** Consider a pure state $|\Psi\rangle_{AB}$ in the composite Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ with dimensions $d_A$ and $d_B$. There exist orthonormal bases $\{|u_i\rangle_A\} \subset \mathcal{H}_A$ and $\{|v_i\rangle_B\} \subset \mathcal{H}_B$, and a set of non-negative real numbers $\{\lambda_i\}$, such that the state can be written as:

$$|\Psi\rangle_{AB} = \sum_{i=1}^{r} \lambda_i |u_i\rangle_A \otimes |v_i\rangle_B$$

where $r \leq \min(d_A, d_B)$ is the Schmidt rank of the state, and the coefficients $\lambda_i$, known as Schmidt coefficients, satisfy the normalization condition $\sum_{i=1}^{r} \lambda_i^2 = 1$.

This decomposition captures the properties of the state entirely within the coefficients $\lambda_i$. If $r = 1$, the state is a product state. If $r > 1$, the state is entangled.

#### 2.1.4.2 Linking Entanglement to the Reduced Density Matrix.

We now mathematically demonstrate the relationship between the entanglement of the pure state $|\Psi\rangle_{AB}$ and the "mixedness" of its subsystem's reduced density matrix (RDM). The central insight is that the more entangled the global state is, the more mixed the reduced state becomes.

Let us compute the reduced density matrix for subsystem $A$, defined as $\rho_A = \mathrm{Tr}_B(\rho_{AB})$, starting from the Schmidt form of $|\Psi\rangle_{AB}$.

- Form the total density matrix $\rho_{AB}$:

$$\begin{aligned}\rho_{AB} &= |\Psi\rangle_{AB}\langle\Psi|_{AB} \\ &= \left(\sum_i \lambda_i |u_i\rangle_A \otimes |v_i\rangle_B\right)\left(\sum_j \lambda_j \langle u_j|_A \otimes \langle v_j|_B\right) \\ &= \sum_{i,j} \lambda_i\lambda_j \left(|u_i\rangle\langle u_j|_A \otimes |v_i\rangle\langle v_j|_B\right).\end{aligned}$$

- Apply the Partial Trace over $B$: The partial trace operation acts linearly. We trace out the $B$ components using the basis orthonormal property $\mathrm{Tr}(|v_i\rangle\langle v_j|_B) = \langle v_j|v_i\rangle_B = \delta_{ij}$.

$$\begin{aligned}\rho_A &= \mathrm{Tr}_B(\rho_{AB}) \\ &= \sum_{i,j} \lambda_i\lambda_j |u_i\rangle\langle u_j|_A \cdot \underbrace{\mathrm{Tr}(|v_i\rangle\langle v_j|_B)}_{\delta_{ij}} \\ &= \sum_i \lambda_i^2 |u_i\rangle\langle u_i|_A.\end{aligned}$$

The result shows that $\rho_A$ is diagonal in the Schmidt basis $\{|u_i\rangle_A\}$, with eigenvalues $p_i = \lambda_i^2$.

**Proof of the Entanglement-Mixedness Relationship:** The mixedness of the state can be quantified using purity. The purity of $\rho_A$ is calculated as follows:

$$\gamma(\rho_A) = \mathrm{Tr}\left(\left(\sum_i \lambda_i^2 |u_i\rangle\langle u_i|\right)^2\right) = \sum_i \lambda_i^4. \tag{2.11}$$

We now compare two extreme cases to prove the relationship:

- **Case 1: Separable State (No Entanglement).** If $|\Psi\rangle_{AB}$ is separable, the Schmidt rank is $r = 1$. There is only one coefficient $\lambda_1 = 1$.

$$\gamma(\rho_A) = 1.$$

The reduced state $\rho_A$ is a pure state. Zero entanglement corresponds to zero mixedness.

- **Case 2: Maximally Entangled State.** A state is maximally entangled if all branches of the superposition have equal weight. This implies the Schmidt

coefficients are uniform: $\lambda_i = \frac{1}{\sqrt{d}}$ for all $i = 1, \ldots, d$.

$$\gamma(\rho_A) = \sum_{i=1}^{d} \left(\frac{1}{\sqrt{d}}\right)^4 = \sum_{i=1}^{d} \frac{1}{d^2} = d \cdot \frac{1}{d^2} = \frac{1}{d}.$$

Since $d \geq 2$, $\gamma(\rho_A) = 1/d$ is the minimum for purity. The reduced state is proportional to the identity operator, $\rho_A = I/d$, which is the maximally mixed state.

## 2.2 Quantum Measurements:

Quantum measurement refers to the process of observing or measuring a quantum system to obtain information about its properties or states. In quantum mechanics, measurements are described by a collection of measurement operators, denoted as $\{\mathcal{M}_m\}$, which act on the state space of the system being measured. The index "$m$" refers to the possible measurement outcomes that may occur in the experiment.

**Postulate 3:** In quantum mechanics, measurements are characterized by a set of operators $\{\mathcal{M}_m\}$ acting on the state space of the system. The index $m$ refers to the possible measurement outcomes. These operators satisfy the completeness equation:

$$\sum_m \mathcal{M}_m^\dagger \mathcal{M}_m = I$$

If the system is in the state $|\psi\rangle$ immediately before the measurement, the probability of observing outcome $m$ is given by:

$$p(m) = \langle\psi|\mathcal{M}_m^\dagger \mathcal{M}_m|\psi\rangle$$

and the state of the system after the measurement is

$$|\psi'\rangle = \frac{\mathcal{M}_m|\psi\rangle}{\sqrt{\langle\psi|\mathcal{M}_m^\dagger \mathcal{M}_m|\psi\rangle}}.$$

This postulate captures the essence of quantum measurements: they are probabilistic and irrevocably alter the system's state. Unlike classical measurements, which reveal pre-existing values, quantum measurements create outcomes through an interaction that depends on the system's initial state and the chosen operators. This framework underpins phenomena like superposition collapse, entanglement, and the uncertainty principle, distinguishing quantum mechanics from classical physics.

### 2.2.1 Projective Measurements

Projective measurements are a specific class of quantum measurements that correspond to the general measurement operators $\{\mathcal{M}_m\}$ becoming orthogonal projectors, denoted here as $\{P_i\}$. That is, we set $\mathcal{M}_m \to P_i$, where these operators are Hermitian ($P_i^\dagger = P_i$) and idempotent ($P_i^2 = P_i$).

A projective measurement is typically described by a Hermitian operator $M$ (an observable), whose eigenvalues represent the possible measurement outcomes. This formalism ensures real-valued results. The operator $M$ encapsulates the relationship between the outcomes and the projectors through its spectral decomposition:

$$M = \sum_i \lambda_i P_i \tag{2.12}$$

where:

- $\lambda_i$ : Real eigenvalues.
- $P_i = |\lambda_i\rangle \langle\lambda_i|$ : Orthogonal projection operators onto the eigenstates $|\lambda_i\rangle$.
- $P_i P_j = \delta_{ij} P_i$ : Projectors are orthogonal ($i \neq j$) and idempotent ($P_i^2 = P_i$).
- Completeness relation : $\sum_i P_i = I$, ensuring total probability conservation (consistent with $\sum \mathcal{M}_m^\dagger \mathcal{M}_m = I$).

Note that if the spectrum of $M$ is degenerate, the projector $P_i$ is a projector with rank greater than 1, expressed as $P_i = \sum_k |\lambda_i, k\rangle\langle\lambda_i, k|$ where $k$ labels the

degenerate states.

**2.2.1.1 Probability of Outcome.** When measuring an observable $M$, the probability of obtaining a specific outcome $\lambda_i$ is determined by the projection of the system's state $|\psi\rangle$ onto the eigenspace associated with $\lambda_i$. Mathematically, this is expressed via the Born rule:

$$p(\lambda_i) = \langle\psi|P_i|\psi\rangle = \|P_i|\psi\rangle\|^2 \tag{2.13}$$

where $P_i$ is the orthogonal projection operator onto the subspace spanned by the eigenvectors corresponding to the eigenvalue $\lambda_i$.

**2.2.1.2 Post-Measurement State.** Upon obtaining the outcome $\lambda_i$, the system's state undergoes an irreversible transformation known as wavefunction collapse. The post-measurement state $|\psi'\rangle$ is given by:

$$|\psi'\rangle = \frac{P_i|\psi\rangle}{\sqrt{p(\lambda_i)}}. \tag{2.14}$$

This expression reflects two key physical principles:

- State Reduction: The system is projected onto the eigenstate $|\lambda_i\rangle$, erasing all coherence between $|\lambda_i\rangle$ and other eigenstates.
- Normalization: The denominator $\sqrt{p(\lambda_i)}$ ensures the resulting state $|\psi'\rangle$ is properly normalized ($\langle\psi' \mid \psi'\rangle = 1$).

This collapse postulate distinguishes quantum measurements from classical observations, as the act of measurement fundamentally alters the system's state.

**2.2.1.3 Expectation Value of the Observable.** The expectation value $\langle M\rangle$, representing the statistical average of outcomes over many repeated measurements, is derived as:

$$\langle M\rangle = \langle\psi|M|\psi\rangle = \sum_i \lambda_i p(\lambda_i) \tag{2.15}$$

Here, the Hermitian nature of $M$ ensures $\langle M\rangle$ is real, aligning with the physical requirement that measurable quantities yield real-valued results. The expectation

value bridges quantum theory and experimental observation, offering a statistical summary of measurement outcomes before any single result is realized.

### 2.2.2 General Measurements

The Positive Operator-Valued Measure (POVM) formalism generalizes the concept of quantum measurement beyond standard projective measurements. Unlike projective measurements, which are associated with observables and numerical eigenvalues, POVM elements describe the statistics of measurement outcomes without necessarily assigning them physical values. Consequently, this formalism does not yield expectation values in the traditional sense, nor does it uniquely determine the post-measurement state of the system.

The ambiguity of the post-measurement state arises from the mathematical structure of the measurement operators. A POVM is defined by a set of operators $\{E_i\}$ such that $E_i = M_i^\dagger M_i$, where $M_i$ is the measurement operator. From the polar decomposition theorem, measurement operator can be written as:

$$M_i = U_i \sqrt{E_i}, \tag{2.16}$$

where $U_i$ is an arbitrary unitary operator. While the probability of an outcome is determined solely by $E_i$ (since $M_i^\dagger M_i = \sqrt{E_i} U_i^\dagger U_i \sqrt{E_i} = E_i$), the state of the system after measurement depends explicitly on the choice of $U_i$:

$$|\psi'\rangle = \frac{M_i|\psi\rangle}{\sqrt{\langle\psi|E_i|\psi\rangle}} = \frac{U_i\sqrt{E_i}|\psi\rangle}{\sqrt{\langle\psi|E_i|\psi\rangle}}. \tag{2.17}$$

Since the unitary operator $U_i$ affects the state evolution but leaves the POVM element $E_i$ unchanged, the POVM formalism is sufficient for tasks relying only on measurement statistics, such as quantum state tomography and verification, while remaining agnostic about the specific post-measurement dynamics.

Formally, a POVM is defined by a set of operators $\{E_i\}$ acting on the Hilbert space of the system, satisfying two key properties:

- **Positivity:** Each element must be a positive semi-definite operator, denoted as $E_i \succeq 0$. This ensures that the measurement probabilities are always non-negative.
- **Completeness:** The sum of all elements must resolve to the identity operator, ensuring that the probabilities of all mutually exclusive outcomes sum to unity:

$$\sum_i E_i = I. \tag{2.18}$$

For a quantum system in a state described by the density matrix $\rho$, the probability $p(m)$ of obtaining the outcome $m$ is given by the Born rule:

$$p(m) = \mathrm{Tr}(E_m \rho). \tag{2.19}$$

The definition above provides the physical intuition behind general measurements. However, to rigorously analyze quantum information protocols, it is necessary to examine the mathematical structure of the set of all possible measurements. Specifically, the set of all POVMs forms a convex set, a property that corresponds physically to the ability to mix different measurement strategies probabilistically.

#### 2.2.2.1 Convex Structure of the POVM.

Formally, let $\mathcal{H}_d$ be a finite-dimensional Hilbert space of dimension $d$. We consider the set of measurements with a fixed number of outcomes $n \geq 1$. Based on the properties of positivity and completeness defined previously, we denote the set of all such $n$-outcome POVMs as $\mathsf{POVM}_n(\mathcal{H}_d)$.

An element $\mathbb{M} \in \mathsf{POVM}_n(\mathcal{H}_d)$ is an $n$-tuple of operators $\mathbb{M} = \{E_i\}_{i=1}^n \subset \mathcal{L}(\mathcal{H}_d)$ satisfying the POVM properties. This set possesses a convex structure [17, 18].

While general convex combinations of measurements can be defined in various ways, here we focus on the element-wise convex combination. This specific structure models a randomized measurement [17], where an experimenter chooses

between measurement settings probabilistically, but the outcome labels remain fixed. This formalism is essential for constructing the verification operator $\Omega$ in the Quantum State Verification protocol discussed later in this work.

Let $\mathbb{M}^{(1)} = \{E_i^{(1)}\}_{i=1}^n$ and $\mathbb{M}^{(2)} = \{E_i^{(2)}\}_{i=1}^n$ be two elements of $\mathsf{POVM}_n(\mathcal{H}_d)$, and let $p \in [0,1]$ be a mixing probability. The convex combination of $\mathbb{M}^{(1)}$ and $\mathbb{M}^{(2)}$ is defined as the $n$-tuple:

$$\mathbb{M} = p\mathbb{M}^{(1)} + (1-p)\mathbb{M}^{(2)} := \left\{pE_i^{(1)} + (1-p)E_i^{(2)}\right\}_{i=1}^n. \tag{2.20}$$

**Convexity of $\mathsf{POVM}_n(\mathcal{H})$):** The set $\mathsf{POVM}_n(\mathcal{H})$ is convex [18]. That is, for any $\mathbb{M}^{(1)}, \mathbb{M}^{(2)} \in \mathsf{POVM}_n(\mathcal{H})$ and any $p \in [0,1]$, the effective measurement $p\mathbb{M}^{(1)} + (1-p)\mathbb{M}^{(2)}$ is also a valid POVM in $\mathsf{POVM}_n(\mathcal{H})$.

*Proof:* We verify that the two defining properties of a POVM are preserved under convex combination.

1. Positivity: For each outcome $i$, the operators $E_i^{(1)}$ and $E_i^{(2)}$ are positive semi-definite by assumption. Since the cone of positive semi-definite operators is closed under non-negative linear combinations, we have

$$pE_i^{(1)} + (1-p)E_i^{(2)} \geq 0 \quad \forall\, i,$$

because $p \geq 0$ and $1-p \geq 0$.

2. Completeness: Summing the elements of the convex combination yields

$$\sum_{i=1}^n \left[pE_i^{(1)} + (1-p)E_i^{(2)}\right] = p\sum_{i=1}^n E_i^{(1)} + (1-p)\sum_{i=1}^n E_i^{(2)} = pI + (1-p)I = I.$$

Since both properties hold, $p\mathbb{M}^{(1)} + (1-p)\mathbb{M}^{(2)} \in \mathsf{POVM}_n(\mathcal{H})$.

### 2.2.3 Local Measurements and Separable Measurements

The fundamental challenge in designing state verification protocols is determining the optimal verification operator $\Omega$. If an experimenter had access

to unlimited technological capabilities, the optimal strategy would simply be to choose a single measurement setting where the "pass" POVM element is the global projector onto the target state $\Omega = |\psi\rangle\langle\psi|$ itself.

Therefore, practical QSV optimization is subject to experimental restrictions. We must restrict our accessible measurement settings to those that can be implemented via Local Operations and Classical Communication (LOCC), or mathematically, the set of separable measurements defined in this part.

#### 2.2.3.1 Local Operations and Classical Communication (LOCC).

In a multipartite quantum system, a local measurement is defined operationally by how it is implemented, rather than solely by the mathematical form of its measurement operators.

A measurement is considered local if it can be implemented using Local Operations and Classical Communication (LOCC). Each party acts only on their own subsystem (e.g., Alice on (A), Bob on (B)), and no joint entangling operations across the partition (A:B) are allowed. However, the parties may exchange classical information. For example, Alice may measure her subsystem, send her outcome to Bob, and Bob may adapt his measurement accordingly. Since only classical information is transmitted, the protocol remains local.

If the measurement requires joint quantum operations, bringing subsystems together, or exchanging quantum particles, it is classified as non-local.

An essential feature of local measurements is classical post-processing. If Alice obtains outcome (a) and Bob obtains outcome (b), they may compute a function

$$y = f(a, b) \tag{2.21}$$

to define the final reported outcome. Thus, the measurement outcome need not be the pair $(a, b)$, but any classical function of these local results.

#### 2.2.3.2 Separable measurements.

Now consider a bipartite system with Hilbert space $\mathcal{H} = \mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)}$. A POVM $\{E_k\}$ is called separable if each element $E_k$ can be written as a sum of product operators. That is:

$$E_k = \sum_j M_{k,j}^{(1)} \otimes M_{k,j}^{(2)} \tag{2.22}$$

where $M_{k,j}^{(1)}$ and $M_{k,j}^{(2)}$ are positive semi-definite operators acting on subsystem 1 and 2 respectively, satisfying $0 \preceq M_{k,j}^{(n)} \preceq I$.

## 2.3 Quantum State Tomography (QST) 101

Quantum state tomography aims to reconstruct an unknown density operator $\rho$ from measurement statistics. Because $\rho$ is an operator on a $D = d^n$ dimensional space, tomography typically requires resources that scale quickly with $n$. This scalability issue is one of the main motivations for using verification instead of tomography.

Tomography requires measurement settings that are informationally complete, meaning the resulting probabilities uniquely determine $\rho$. Since the density matrix $\rho$ is a Hermitian operator with unit trace, it contains $D^2 - 1$ independent real parameters. Therefore, to reconstruct $\rho$, one must perform measurements in a sufficient number of bases to resolve these independent real parameters [19, 15]. Operationally, one chooses a set of measurement settings $s \in \mathcal{S}$, where each setting corresponds to a POVM $\{E_m^{(s)}\}_m$. Repeating setting $s$ many times yields estimates of

$$p(m|s) = \mathrm{Tr}(E_m^{(s)}\rho).$$

Because these probabilities depend linearly on the unknown entries of $\rho$, reconstruction can be performed by solving a linear inversion problem, often followed by a physicality-enforcing procedure (e.g., maximum likelihood estimation) to ensure positivity.

To formulate this linear inversion problem explicitly, it is convenient to express $\rho$ as a linear combination of an orthogonal operator basis. Specifically, we can choose an orthonormal basis $\{\omega_i\}$ for the space of Hermitian operators acting on a single qudit (with $i = 0, 1, \ldots, d^2 - 1$, where $\omega_0 = I$ is the identity The set

$$\mathcal{B}_n = \{B_{\mathbf{i}} = \omega_{i_1} \otimes \cdots \otimes \omega_{i_n} \mid i_j \in \{0, 1, \ldots, d^2 - 1\}\} \tag{2.23}$$

forms a complete orthogonal basis for the space of Hermitian operators acting on $n$ qudits, satisfying

$$\mathrm{Tr}(B_{\mathbf{i}} B_{\mathbf{j}}) = D\delta_{\mathbf{i},\mathbf{j}}. \tag{2.24}$$

Therefore, the density matrix can be expanded as:

$$\rho = \frac{1}{D} \sum_{i_1,\ldots,i_n=0}^{d^2-1} c_{i_1 \ldots i_n}\, \omega_{i_1} \otimes \cdots \otimes \omega_{i_n} \tag{2.25}$$

where the real-valued coefficients are given by the expectation values:

$$c_{i_1 \ldots i_n} = \langle \omega_{i_1} \otimes \cdots \otimes \omega_{i_n} \rangle = \mathrm{Tr}\big(\rho \cdot \omega_{i_1} \otimes \cdots \otimes \omega_{i_n}\big). \tag{2.26}$$

Two commonly used operator bases for qudit systems are:

- **Generalized Gell-Mann (GGM) basis:** Consists of symmetric off-diagonal operators $\Lambda^s_{jj'} = |j\rangle\langle j'| + |j'\rangle\langle j|$, anti-symmetric off-diagonal operators $\Lambda^a_{jj'} = -i|j\rangle\langle j'| + i|j'\rangle\langle j|$, and diagonal operators $\Lambda^d_l$ that generalize the Pauli $Z$ operator.
- **Heisenberg–Weyl observable (HWO) basis:** Constructed from linear combinations of generalized shift and clock operators, which will be defined rigorously in Chapter 4.

### 2.3.1 Example of a Single-Qubit Case ($d = 2$)

To find the expectation value of a Pauli operator, such as X, for a general

1-qubit state, we compute the following:

$$\langle X \rangle = \mathrm{Tr}(X\rho) = \mathrm{Tr}(X\frac{1}{2}(I + r_x X + r_y Y + r_z Z)) \tag{2.27}$$

$$= \frac{1}{2}(\mathrm{Tr}(X) + r_x \,\mathrm{Tr}(I) + r_y \,\mathrm{Tr}(XY) + r_z \,\mathrm{Tr}(XZ)) \tag{2.28}$$

$$= 0 + r_x + 0 + 0 \tag{2.29}$$

$$= r_x \tag{2.30}$$

By determining the expectation values for all three Pauli operators, the state is reconstructed as:

$$\rho = \frac{1}{2}(I + r_x X + r_y Y + r_z Z) \tag{2.31}$$

where $r_i = \langle i \rangle$ for $i \in \{X, Y, Z\}$.

The following algorithm provides a demonstration of the quantum tomography process. The methodology consists of the following steps:

- A set of identical single-qubit quantum states is randomly prepared.
- Measurements are subsequently performed using the $X$, $Y$, and $Z$ observables, with 1,000 samples collected for each basis.
- Finally, the quantum state is reconstructed according to Equation (2.31). The result of this reconstruction is depicted in Figure 1.

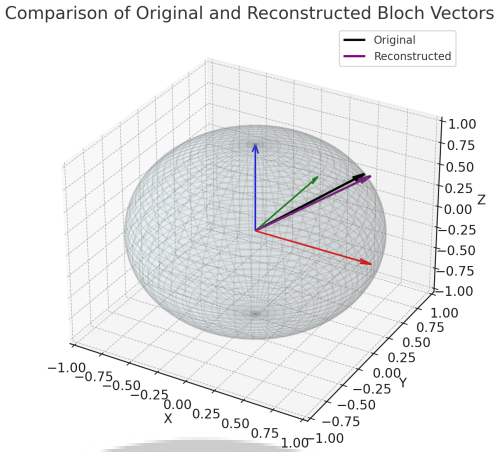



**Figure 1 Example of comparison of original and reconstructed state via Python simulation**

QST enables complete reconstruction of an unknown quantum state, but its sample complexity grows rapidly with the Hilbert-space dimension. Even under sample-optimal tomography with collective measurements, Haah et al.[20] show that achieving trace-distance accuracy $\epsilon$ for a rank-$r$ state requires $O((dr/\epsilon^2)\log(d/\epsilon))$ copies. This improves upon the earlier $O(dr^2/\epsilon^2)$ scaling in the low-rank regime, but retains a linear dependence on the dimension $d$.

This dependence becomes prohibitive for $n$-qudit systems, where the dimension grows exponentially with the number of qudits. By contrast, quantum state verification (QSV) does not attempt to reconstruct the state $\rho$, but instead certifies that it is close to a known target state. As a result, its copy complexity scales as $N \approx \ln(\delta^{-1})/(\epsilon v(\Omega))$ [11, 9], and is governed primarily by the verification gap $v(\Omega)$ rather than by the full number of state parameters.

# CHAPTER III

# QUANTUM STATE VERIFICATION

As demonstrated in the previous chapter, fully reconstructing a quantum state via tomography becomes highly impractical as the system size grows. This chapter transitions from the general measurement formalisms of Chapter 2 to the specific theoretical framework of Quantum State Verification (QSV) [11, 9]. Unlike tomography, QSV does not attempt to learn the exact state; rather, it asks a simple yes-or-no question: is the prepared state sufficiently close to the target state? Here, we formalize QSV as a statistical hypothesis testing problem. We detail the protocol's decision rules, error rates, and sample complexity. Crucially, we introduce the concept of the spectral gap of the verification operator, establishing it as the primary mathematical quantity that dictates the efficiency and resource requirements of any QSV protocol.

Building upon this foundational framework, researchers have successfully designed efficient verification strategies for a wide variety of physically significant quantum states. To date, previous efficient QSV results have been established for general bipartite states [21], qubit stabilizer states including graph states [12, 11, 22], hypergraph states [23], qudit GHZ states [14], (phased) Dicke states including antisymmetric states [24, 25], and ground states of frustration-free Hamiltonians [26].

## 3.1 Hypothesis Testing

A statistical technique called hypothesis testing is used to ascertain if the observed data from a quantum system confirms a certain theory on the quantum state. The process entails developing a null hypothesis and an alternative hypothesis, after which statistical tests are performed to assess each hypothesis's viability

in light of the data. Finding out if a certain quantum state is near or far from a target state is frequently the aim of hypothesis testing. According to the null hypothesis ($H_0$), the quantum state is either not the target state or differs from it in a substantial way. The alternative hypothesis ($H_1$), on the other hand, contends that the quantum state is either the target state or very near to it.

For example, suppose you want to verify if a quantum system has been prepared in a specific state, say $|\Psi\rangle$. You can perform measurements on the system and collect data. Based on the data, you will then perform a hypothesis test to determine which of the following hypotheses is more likely:

- Null hypothesis ($H_0$): The quantum state is not $|\Psi\rangle$ (or significantly different from $|\Psi\rangle$).
- Alternative hypothesis ($H_1$): The quantum state is $|\Psi\rangle$ (or very close to $|\Psi\rangle$).

When conducting a hypothesis test, there are two possible types of errors that can be made: Type I errors (false positive) and Type II errors (false negative). These errors can arise due to various factors, such as imperfections in the quantum system.

- False positives, or type I errors, happen when the null hypothesis is disproved while it is true. A Type I mistake in the scenario described above would be determining falsely that the quantum state is near the target state while in fact it is not. The test's significance level, or $\delta$, represents the likelihood of committing a Type I mistake.
- False negatives, or type II errors (represented by $\beta$), happen when the null hypothesis is accepted when it is not true. Erroneously determining that the quantum state is not near the target state when in fact it is constitutes a Type II mistake.

To perform hypothesis testing, we need a decision rule that defines the criteria for accepting or rejecting a particular hypothesis. The decision rule is typically based

on the statistical properties of the measurement outcomes.

### 3.1.1 Statistical Verification

The QSV protocol aims to verify whether a quantum device produces a specific target state $|\psi\rangle$. The device generates a sequence of independent states $\sigma_1, \sigma_2, ..., \sigma_k$. In the context of hypothesis testing, the two hypotheses are defined as follows:

- Null hypothesis ($H_0$, non-target state): $\sigma_k \in S_\varepsilon = \{\rho \ |\langle\psi|\rho|\psi\rangle \leq 1-\varepsilon\} \ \ \forall_k$
- Alternative hypothesis ($H_1$, target state): $\sigma_k \in S = \{|\psi\rangle\langle\psi|\} \ \ \forall_k$

where $S$ and $S_\varepsilon$ are sets of the target state and non-target states that are far away from the target state at least $1-\varepsilon$, respectively, as illustrated in Figure 2.

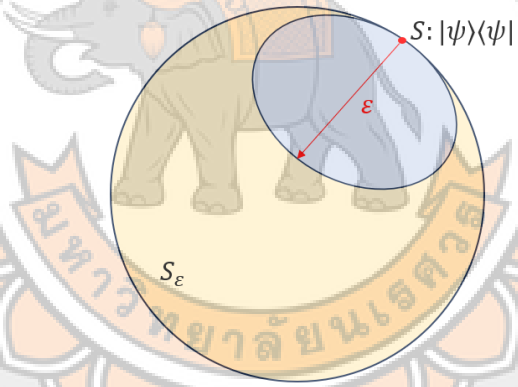



**Figure 2 A schematic representation of a hypothesis testing configuration.**

For each state $\sigma_k$ produced by the device, the verifier selects one measurement setting from a collection of $m$ possible settings. The $j$th setting is chosen with probability $p_j$, where $j = 1, \ldots, m$. Each setting is described by a two-outcome POVM $\{\Omega_j, I - \Omega_j\}$. The outcome corresponding to $\Omega_j$ is declared "pass", whereas the outcome corresponding to $I - \Omega_j$ is declared "fail".

In standard quantum state verification protocols, it is a common design choice to require perfect completeness, meaning that a correctly functioning device

producing the ideal target state $|\psi\rangle$ is never rejected [11]. This assumption is imposed to avoid the false rejection of an ideal source due to the inherent randomness of quantum measurements; if the target state had even a small probability of failing, repeated testing would eventually reject a perfect device. To ensure this, the probability of false rejection is set to zero for every verification test $j$, which imposes the constraint:

$$\langle\psi|\Omega_j|\psi\rangle = 1. \tag{3.1}$$

Since the measurement effects satisfy $0 \leq \Omega_j \leq I$, this condition mathematically implies that the target state $|\psi\rangle$ must be an eigenstate of every pass effect $\Omega_j$ with an eigenvalue of exactly 1. Within this framework, the verification proceeds through a sequence of measurements where any "fail" outcome results in the immediate acceptance of the null hypothesis $H_0$ [11], asserting that the states were not the intended target. Conversely, a "pass" allows the verifier to proceed to the next state $\sigma_{k+1}$ and repeat the test. By ensuring that the target state passes with certainty, the optimization of the protocol focuses entirely on minimizing the Type I error $\delta$ for a specified precision $\epsilon$. These two parameters, $\delta$ and $\epsilon$, ultimately dictate the number of samples $N$ required to achieve a confidence level of $1 - \delta$, providing an asymptotically optimal strategy for high-precision verification.

**The Decision Rule:**

- If the measurement outcome corresponds to $I - \Omega_j$, the verifier accepts $H_0$ (rejects the device).
- If all $N$ copies yield outcomes corresponding to $\Omega_j$, the verifier rejects $H_0$ in favor of $H_1$, concluding the device produces $|\psi\rangle$.

Accordingly, the decision rule can be represented as a flowchart as shown in Figure 3.

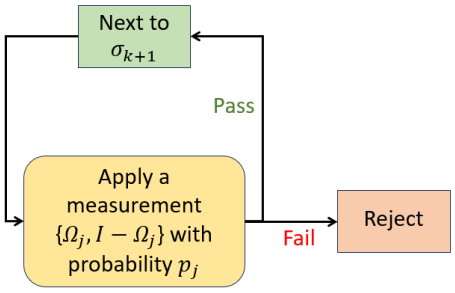



**Figure 3 A flowchart illustrating the sequence of actions governed by the decision rule.**

To evaluate the Type I error, we consider the worst-case failure probability for each run. Assuming $H_0$ is true, the worst-case passing probability can be expressed as (see Note 1):

$$\max_{\langle\psi|\sigma|\psi\rangle\leq 1-\varepsilon} \mathrm{Tr}(\Omega\sigma) = 1 - \varepsilon v(\Omega) \tag{3.2}$$

where $v(\Omega)$ represents the spectral gap between the largest eigenvalue ($\lambda_1 = 1$) and the second-largest eigenvalue ($\lambda_2 = \beta(\Omega)$) of $\Omega$. Here, $\Omega = \sum p_j \Omega_j$ is a verification strategy or verification operator, where the $j$-th measurement is performed with probability $p_j$. Since the verifier rejects $H_0$ only if all $N$ independent sample states pass the test, the Type I error is bounded by:

$$\delta \leq (1 - \varepsilon v(\Omega))^N \tag{3.3}$$

To achieve a given confidence level of $1 - \delta$, it is sufficient to take $N = ln(\delta)/\ln(1 - \varepsilon v(\Omega))$ sample states from the quantum device. In the high precision limit ($\varepsilon, \delta \to 0$), the scaling of N becomes:

$$N \approx \frac{\ln(\delta^{-1})}{\varepsilon v(\Omega)} \tag{3.4}$$

Equation (3.5) reveals the central thesis of QSV optimization: to minimize the number of required state copies $N$, we must design a verification operator $\Omega$ that maximizes the spectral gap $v(\Omega)$.

**Note 1: Worst-case Scenario**

We want to find the maximum value of $\mathrm{Tr}(\Omega\sigma)$ under the condition that $\sigma$ is not the target state, meaning it has fidelity less than or equal to $1-\varepsilon$. Let $\{|\phi_i\rangle\}_i$ be an orthonormal eigenbasis of $\Omega$ with eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots$, where

$$\lambda_1 = 1, \quad |\phi_1\rangle = |\psi\rangle,$$

since $\Omega|\psi\rangle = |\psi\rangle$.

By the spectral theorem, the verification operator $\Omega$ can be decomposed as:

$$\Omega = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|.$$

The passing probability for an arbitrary state $\sigma$ is then given by the trace:

$$\mathrm{Tr}(\Omega\sigma) = \mathrm{Tr}\left(\sum_i \lambda_i |\phi_i\rangle\langle\phi_i|\sigma\right) = \sum_i \lambda_i \langle\phi_i|\sigma|\phi_i\rangle = \sum_i \lambda_i p_i$$

where $p_i = \langle\phi_i|\sigma|\phi_i\rangle$ represents the probability distribution satisfying $p_i \geq 0$ and $\sum_i p_i = 1$.

To find the worst-case pass probability, we maximize this sum subject to the fidelity constraint $p_1 = \langle\psi|\sigma|\psi\rangle \leq 1-\varepsilon$. Since $\lambda_1 > \lambda_2 \geq \lambda_i$ for $i > 2$, the objective function is maximized by assigning the maximum allowed weight to the largest eigenvalue $\lambda_1$ and the remaining weight to the second-largest eigenvalue $\lambda_2 = \beta(\Omega)$. Specifically, we set $p_1 = 1-\varepsilon$ and $p_2 = \varepsilon$, yielding:

$$\begin{aligned}
\max_{\langle\psi|\sigma|\psi\rangle \leq 1-\varepsilon} \mathrm{Tr}(\Omega\sigma) &= \lambda_1(1-\varepsilon) + \beta(\Omega)\varepsilon \\
&= 1(1-\varepsilon) + \beta(\Omega)\varepsilon \\
&= 1 - \varepsilon(1-\beta(\Omega)) \\
&= 1 - \varepsilon\nu(\Omega)
\end{aligned}$$

where $\nu(\Omega) = 1-\beta(\Omega)$ is the spectral gap of the verification operator.

The primary challenge in designing a quantum state verification protocol is

finding the optimal verification operator $\Omega$ that maximizes the spectral gap $\nu(\Omega)$, thereby minimizing the number of state copies required.

If there are no experimental restrictions, the best strategy is to perform a global measurement that projects directly onto the target state, $\Omega = |\psi\rangle\langle\psi|$. This strategy is optimal because it achieves the maximum possible spectral gap of $\nu(\Omega) = 1$, which perfectly distinguishes the target state from any orthogonal state.

However, implementing such global projective measurements is often experimentally infeasible for large multi-partite systems. Consequently, the optimization of $\Omega$ is practically subject to locality restrictions [11, 9]. Specifically, the accessible measurements are typically limited to local measurements or separable measurements (as previously defined in Section 2.2.3), requiring us to find the optimal $\Omega$ within these restricted sets.

# CHAPTER IV

# BACKGROUND FOR STABILIZER AND GRAPH STATES

While Chapter 3 established the general framework for Quantum State Verification, the efficiency of any QSV protocol is fundamentally dictated by its spectral gap, which relies heavily on the target state's mathematical structure. Consequently, this chapter focuses on a significant class of quantum states: qudit stabilizer and graph states. A key reason for introducing stabilizer states is that graph states serve as their canonical representatives. Specifically, in systems of prime dimension $d$, every stabilizer state is equivalent to a graph state under local Clifford unitaries [27]. Since local unitaries strictly preserve entanglement across any bipartition, the verification frameworks established for graph states can naturally be extended to all stabilizer states.

This chapter provides the essential algebraic background to support this connection. For prime dimensions $d$, we introduce the generalized Weyl-Heisenberg operators, define the stabilizer group, and outline the construction of graph states [28, 29]. Finally, we review the derivation for the transformation of these states under local Z-measurements and calculate the reduced density matrix, following the approach of [12, 30]. To the best of our knowledge, the resulting form of the reduced density matrix—central to the main proof in the subsequent chapter—is new.

## 4.1 Generalized Pauli Operators and the $n$-qudit Pauli Group for Prime Dimensions

For a $d$-level system, using the computational basis $|0\rangle, |1\rangle, \ldots, |d-1\rangle$, we

can define the single-qudit generalized Pauli operators as follows:

$$X = \sum_{j=0}^{d-1} |j + 1 (\mathrm{mod}\, d)\rangle\langle j| \tag{4.1}$$

and

$$Z = \sum_{j=0}^{d-1} \omega^j |j\rangle\langle j| \tag{4.2}$$

where $\omega = e^{2\pi i/d}$. These operators satisfy the Weyl commutation relation: $ZX = \omega XZ$.

Following [28], we define the generalized Pauli operators for an $n$-qudit system via the tensor product. Let $v \in \mathbb{Z}_d^{2n}$ be a vector representing the exponents of $X$ and $Z$ on each qudit. We define the map $P : \mathbb{Z}_d^{2n} \to \mathbb{C}^{d^n \times d^n}$ as:

$$P(v) := X^{v_0} Z^{v_n} \otimes X^{v_1} Z^{v_{n+1}} \otimes \cdots \otimes X^{v_{n-1}} Z^{v_{2n-1}}. \tag{4.3}$$

We denote the set of all such operators as $P_n := P(v) : v \in \mathbb{Z}_d^{2n}$.

Similar to the qubit Paulis, the set $P_n$ does not form a group under standard matrix multiplication. Multiplying two elements generally yields a complex phase factor involving $\omega$ that is not captured within the definition of $P(v)$. To formulate a proper group, we must include these phase factors. Thus, the $n$-qudit Pauli group (or generalized Weyl-Heisenberg group) is defined as:

$$\overline{P_n} := \{\omega^j P(v) \mid v \in \mathbb{Z}_d^{2n}, j \in \mathbb{Z}_d\}. \tag{4.4}$$

For any two elements $\omega^j P(u)$ and $\omega^k P(v)$ in $\overline{\mathcal{P}_n}$, their commutation relation is given by:

$$P(u)P(v) = \omega^{u^T \Lambda v} P(v)P(u), \quad \Lambda = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \tag{4.5}$$

where $\Lambda$ is expressed in four $n \times n$ blocks. Consequently, two Pauli operators $P(u), P(v) \in \mathcal{P}_n$ commute if and only if $u^T \Lambda v \equiv 0 \pmod{d}$.

## 4.2 Generalized Stabilizer Group and Stabilizer Code

Following the definition of the generalized Pauli group $\overline{\mathcal{P}_n}$, we now formally define the generalized stabilizer group $\mathcal{S}$. A stabilizer group $\mathcal{S}$ is an Abelian subgroup of the Pauli group ($\mathcal{S} \subseteq \overline{\mathcal{P}_n}$) that satisfies two key conditions:

1. Abelian: All elements within $\mathcal{S}$ mutually commute.

2. No Non-Trivial Phases: The intersection of $\mathcal{S}$ with the set of global phases contains strictly the identity operator, i.e., $\{\omega^j I \mid j \in \mathbb{Z}_d\} \cap \mathcal{S} = \{I\}$.

The second condition ensures the existence of a valid, non-trivial quantum state stabilized by $\mathcal{S}$: a simultaneous $+1$-eigenstate of all operators within the group:

$$S|\psi\rangle = |\psi\rangle, \quad \forall S \in \mathcal{S} \tag{4.6}$$

Suppose the group $\mathcal{S}$ contained a non-trivial phase element, such as $\omega I$. Applying this operator to the state $|\psi\rangle$ would yield the equation $\omega I|\psi\rangle = |\psi\rangle$, which simplifies to $\omega|\psi\rangle = |\psi\rangle$. Since $\omega \neq 1$, this equation holds true if and only if $|\psi\rangle = 0$ (the null vector). Therefore, to prevent the formalism from stabilizing a non-physical zero state, the group $\mathcal{S}$ must exclude all complex phase factors other than the identity.

The vectors stabilized by all elements in the stabilizer group $\mathcal{S}$ form a subspace called the stabilizer code or codespace, denoted by $V_S$. The dimension of this codespace is given by $d^n/|\mathcal{S}|$.

The projection operator onto the codespace $V_S$ can be explicitly written as:

$$\mathbb{P}_S = \frac{1}{|\mathcal{S}|} \sum_{S \in \mathcal{S}} S = \prod_{j=1}^{k} \left( \frac{1}{d} \sum_{i=0}^{d-1} g_j^i \right) \tag{4.7}$$

where $|\mathcal{S}|$ is the order of the group $\mathcal{S}$, and $g_j$ represents the $j$-th generator of the stabilizer group such that $\mathcal{S} = \langle g_1, g_2, \ldots, g_k \rangle$.

The operator $\mathbb{P}_S$, which projects states onto the stabilized subspace, is an orthogonal projector. This implies it must be both idempotent (self-squaring) and Hermitian. The idempotency arises naturally because $\mathbb{P}_S$ is constructed as the

uniform average over all elements of the subgroup $\mathcal{S}$. Applying the operator twice yields the same result as applying it once ($\mathbb{P}_S^2 = \mathbb{P}_S$), as demonstrated below:

$$\mathbb{P}_S^2 = \left(\frac{1}{|\mathcal{S}|}\sum_{S'\in\mathcal{S}} S'\right)\left(\frac{1}{|\mathcal{S}|}\sum_{S\in\mathcal{S}} S\right) \tag{4.8}$$

$$= \frac{|\mathcal{S}|}{|\mathcal{S}|^2}\sum_{S\in\mathcal{S}} S \tag{4.9}$$

$$= \mathbb{P}_S \tag{4.10}$$

Furthermore, to be a valid orthogonal projector, it must be Hermitian ($\mathbb{P}_S^\dagger = \mathbb{P}_S$). Since the elements of the stabilizer group are unitary operators, we have $S^\dagger = S^{-1}$. By the definition of a group, if an element $S$ exists in $\mathcal{S}$, its unique inverse $S^{-1}$ must also belong to $\mathcal{S}$. Consequently, summing over the inverses of all group elements is mathematically equivalent to summing over the elements themselves. This gives:

$$\mathbb{P}_S^\dagger = \left(\frac{1}{|\mathcal{S}|}\sum_{S\in\mathcal{S}} S\right)^\dagger \tag{4.11}$$

$$= \frac{1}{|\mathcal{S}|}\sum_{S\in\mathcal{S}} S^\dagger \tag{4.12}$$

$$= \frac{1}{|\mathcal{S}|}\sum_{S\in\mathcal{S}} S^{-1} \tag{4.13}$$

$$= \frac{1}{|\mathcal{S}|}\sum_{S'\in\mathcal{S}} S' = \mathbb{P}_S \tag{4.14}$$

To rigorously demonstrate that the resulting state indeed resides within the codespace $V_S$, we must prove that for any arbitrary quantum state $|\phi\rangle$, the projected state $|\psi\rangle = \mathbb{P}_S|\phi\rangle$ satisfies the stabilization condition for all elements in

$\mathcal{S}$ (i.e., $h|\psi\rangle = |\psi\rangle$ for all $h \in \mathcal{S}$). This can be shown as follows:

$$h|\psi\rangle = h(\mathbb{P}_S|\phi\rangle) \tag{4.15}$$

$$= h\left(\frac{1}{|\mathcal{S}|}\sum_{S\in\mathcal{S}} S\right)|\phi\rangle \tag{4.16}$$

$$= \left(\frac{1}{|\mathcal{S}|}\sum_{S\in\mathcal{S}} hS\right)|\phi\rangle \tag{4.17}$$

$$= \left(\frac{1}{|\mathcal{S}|}\sum_{S'\in\mathcal{S}} S'\right)|\phi\rangle = |\psi\rangle \tag{4.18}$$

The substitution $S' = hS$ is valid due to the rearrangement theorem of groups; multiplying all elements of a group by a fixed group element simply permutes the elements, leaving the overall sum unchanged.

**Note 2: Codespace dimension**

The dimension of the codespace can be determined directly from the trace of its corresponding projection operator using the relation Dimension $=$ $\mathrm{Tr}(\mathbb{P}_S)$. Therefore, we evaluate the trace as:

$$\mathrm{Tr}(\mathbb{P}_S) = \mathrm{Tr}\left(\frac{1}{|\mathcal{S}|}\sum_{S\in\mathcal{S}} S\right)$$

$$= \frac{1}{|\mathcal{S}|}\sum_{S\in\mathcal{S}} \mathrm{Tr}(S)$$

$$= \frac{1}{|\mathcal{S}|}\left(\mathrm{Tr}(I) + \sum_{S\in\mathcal{S}\setminus\{I\}} \mathrm{Tr}(S)\right)$$

$$= \frac{1}{|\mathcal{S}|}(d^n + 0) = \frac{d^n}{|\mathcal{S}|}$$

For an $n$-qudit system, if the stabilizer group is a maximal stabilizer group, it is generated by exactly $n$ independent and mutually commuting generators—the maximum possible number of independent constraints for such a quantum system. This maximal set of constraints ensures that there is only one unique quantum state that satisfies all stabilization conditions simultaneously. Consequently, a maximal

stabilizer group uniquely identifies a single quantum state, characterized by a one-dimensional subspace ($d^n/|\mathcal{S}| = d^n/d^n = 1$). This unique state is formally defined as a stabilizer state.

## 4.3 Graph State and Its Manipulation

### 4.3.1 Qubit Graph State

A graph state is a specific type of multi-qubit state which is associated with a mathematical graph. Each vertex in the graph represents a qubit, and each edge represents an entangling operation between qubits. A graph state corresponds to a graph $G = (V, E)$, where $V$ is the set of vertices and $E$ is the set of edges. Each vertex in $V$ corresponds to a qubit, and each edge in $E$ corresponds to a two-qubit entangling operation.

Given a graph $G$, the associated graph state $|G\rangle$ is prepared starting from the state $|+\rangle^{\otimes|V|}$, where $|V|$ is the number of vertices (and hence the number of qubits), and $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. The state is then transformed by applying a controlled-Z ($CZ$) operation between each pair of qubits corresponding to an edge in $E$. The controlled-Z gate, denoted $CZ_{a,b}$, acts on two qubits by applying a Pauli-$Z$ gate to the second qubit if and only if the first qubit is in the state $|1\rangle$. Mathematically, this is expressed as:

$$CZ_{a,b} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z. \tag{4.19}$$

So, to generate a graph state, for each edge $(a, b) \in E$, apply a controlled-Z operation between the a-th and b-th qubits. The final state after applying all these operations is the graph state $|G\rangle$, as shown below:

$$|G\rangle = \prod_{(a,b)\in E} CZ_{a,b}|+\rangle^{\otimes|V|} \tag{4.20}$$

The stabilizer group of a graph state is particularly interesting. Given a graph state $|G\rangle$, its stabilizer group is generated by the operators $g_v$, where each $g_v$ is

associated with a vertex $v \in V$ and is defined as:

$$g_v = X_v \prod_{u \in \text{neighbors}(v)} Z_u \tag{4.21}$$

where $X_v$ is a Pauli X operation on the $v$-th qubit, $Z_u$ is a Pauli Z operation on the $u$-th qubit, and the product is over all $u$ such that there is an edge between $u$ and $v$ in G. The graph state $|G\rangle$ is a simultaneous $+1$ eigenstate of all these stabilizer generators, i.e., $g_v|G\rangle = |G\rangle$ for all $v \in V$.

### 4.3.2 Qudit Graph State

The concept of graph states can be generalized to $d$-level quantum systems, where we assume $d$ is a prime number. Consider a weighted graph $G = (V, E, w)$, which has a set of vertices $V$, a set of edges $E$, and a weight function $w(e) \in \{0, 1, \ldots, d-1\}$ assigning an integer to each edge [29].

We can associate a quantum state, called a graph state $|G\rangle$, with this graph. If the graph has $n = |V|$ vertices, the state will have $n$ qudits. The graph state is constructed as follows:

- Initial State: All $n$ qudits begin in the uniform superposition state $|+\rangle^{\otimes n}$, where:

$$|+\rangle = \frac{1}{\sqrt{d}} \sum_{j}^{d-1} |j\rangle \tag{4.22}$$

- Entangling Operation: For each edge $(a, b) \in E$, a weighted generalized controlled-Z gate, $\left(CZ_{\{a,b\}}\right)^{w((a,b))}$, is applied. The fundamental $CZ$ gate is defined as:

$$CZ_{\{a,b\}} = \sum_{j=0}^{d-1} |j\rangle_a\langle j| \otimes Z_b^j \tag{4.23}$$

The operator $Z_b$ is the generalized Pauli-Z gate, which acts as $Z_b|j\rangle_b = \omega^j|j\rangle_b$ with $\omega = e^{\frac{2\pi i}{d}}$ and $j \in \{0, 1, \ldots, d-1\}$.

Combining these steps, the final graph state is:

$$|G\rangle = \prod_{(a,b)\in E} CZ_{\{a,b\}}^{w((a,b))} |+\rangle^{\otimes n} \tag{4.24}$$

The graph's structure can also be described by its $n \times n$ adjacency matrix $\Gamma$ (as shown in Fig.4), where the entry $\Gamma_{ab}$ is the weight of the edge between vertices $a$ and $b$. If no edge exists, $\Gamma_{ab} = 0$.

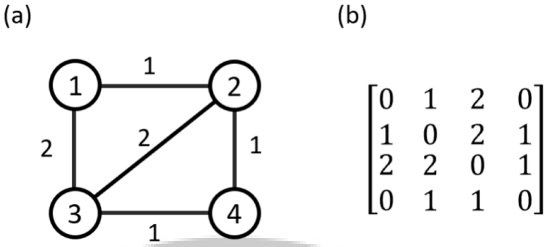



**Figure 4 A graph representation of $G$ is shown in (a), and the adjacency matrix $\Gamma$ that represents the graph $G$ is shown in (b).**

The stabilizer generators for qudit graph states are constructed using the generalized Pauli operators $X$ and $Z$ as discussed in the previous section. For each vertex $v \in V$, the corresponding stabilizer generator $g_v$ is defined as:

$$g_v = X_v \prod_{u \in \text{neighbors}(v)} Z_u^{\Gamma_{vu}} \tag{4.25}$$

where the power of the $Z$ operator depends on the edge weight $\Gamma_{vu}$ modulo $d$. The $n$-qudit graph state $|G\rangle$ is the unique state stabilized by the group $\mathcal{S} = \langle g_1, g_2, \ldots, g_n \rangle$.

## 4.4 Local Z-Measurements on Graph States

The core of our proof involves understanding how the graph state transforms under local measurements [30]. Here, we analyze the effect of a projective measurement on a single qudit $b$ in the computational basis.

We first write the graph state in a way that clearly separates the $b$ part and the rest, denoted $G - \{b\}$:

$$|G\rangle = \prod_{(b,c)\in E} CZ_{\{b,c\}}^{w((b,c))} |+\rangle_b \otimes \prod_{(a\neq b, d\neq b)\in E} CZ_{\{a,d\}}^{w((a,d))} |+\rangle^{\otimes |V|-1} = \prod_{(b,c)\in E} CZ_{\{b,c\}}^{w((b,c))} |+\rangle_b \otimes |G-\{b\}\rangle. \tag{4.26}$$

The full derivation can be found in appendix A.

The total effect of all generalized controlled- $Z$ operations acting nontrivially on a given qudit $b$ can be compactly expressed as

$$\prod_{(b,c)\in E} CZ_{\{b,c\}}^{w((b,c))} = \sum_{j=0}^{d-1} |j\rangle_b\langle j| \otimes \left(Z^{N^w(b)}\right)^j \tag{4.27}$$

where the operator $Z^{N^w(b)}$ denotes the tensor product of weighted Pauli- $Z$ operators acting on the neighborhood of $b$, explicitly given by

$$Z^{N^w(b)} := \bigotimes_{c\in N(b)} Z_c^{w(b,c)} \tag{4.28}$$

with $N(b) = \{c \mid (b,c) \in E\}$ denoting the set of neighbors of $b$. Applying the projection operator $P_{\omega^j,b} = |j\rangle_b\langle j|$, which projects onto the eigenspace corresponding to eigenvalue $\omega^j$, the state $|G\rangle$ becomes

$$P_{\omega^j,b}|G\rangle = \langle j \mid_b + \rangle |j\rangle_b \otimes \left(Z^{N^w(b)}\right)^j |G - \{b\}\rangle = \frac{1}{\sqrt{d}} |j\rangle_b \otimes \left(Z^{N^w(b)}\right)^j |G - \{b\}\rangle, \tag{4.29}$$

where we have used the identity $\langle j \mid + \rangle = 1/\sqrt{d}$ for the equal superposition state $|+\rangle$.

After we determine the effect of the measurement, we use this result to compute the reduced density matrix in the next section.

## 4.5 The Reduced Density Matrix of a Graph State

To understand the entanglement of a single qudit, let us call it $A$, with the rest of the graph, $B$, we compute its reduced density matrix, $\rho_A$. To do so, we extend to the qudit setting the method from [30], in which $\rho_A$ is obtained by averaging the post-measurement states resulting from Z-basis measurements on all qudits in B, taken over all possible outcomes. Let $\mathbf{j} \in \mathbb{F}_d^{|B|}$ denote a dit string corresponding to a measurement outcome, and let $p(\mathbf{j})$ be the probability of that outcome. Then we obtain:

$$\mathrm{Tr}_B \left( \sum_{\mathbf{j}\in\mathbb{F}_d^{|B|}} p(\mathbf{j}) \frac{|\mathbf{j}\rangle\langle\mathbf{j}|\rho_{AB}|\mathbf{j}\rangle\langle\mathbf{j}|}{p(\mathbf{j})} \right) = \sum_{\mathbf{j}\in\mathbb{F}_d^{|B|}} \langle\mathbf{j}|\rho_{AB}|\mathbf{j}\rangle \otimes \mathrm{Tr}_B(|\mathbf{j}\rangle\langle\mathbf{j}|) = \sum_{\mathbf{j}\in\mathbb{F}_d^{|B|}} \langle\mathbf{j}|\rho_{AB}|\mathbf{j}\rangle = \rho_A \tag{4.30}$$

which yields the reduced state of subsystem $A$.

To determine the effect of measuring all qudits $b \in B$, we apply the result of Equation (3.6) to each qudit in $B$. This yields:

$$\frac{1}{\sqrt{d^{|B|}}} \prod_{b\in B} \left(Z^{N^w(b)}\right)^{j_b} |G-B\rangle_A \otimes |\mathbf{j}\rangle_B = \frac{1}{\sqrt{d^{|B|}}} \prod_{b\in B} \left(Z^{N^w_A(b)}\right)^{j_b} \left(Z^{N^w_B(b)}\right)^{j_b} |G-B\rangle_A \otimes |\mathbf{j}\rangle_B \tag{4.31}$$

$$= \frac{1}{\sqrt{d^{|B|}}} Z^{\sum_{b\in B} N^w_A(b) j_b} |G[A]\rangle_A \otimes Z^{\sum_{b\in B} N^w_B(b) j_b} |\mathbf{j}\rangle_B \tag{4.32}$$

$$= \frac{1}{\sqrt{d^{|B|}}} Z^{\Gamma_{AB}\mathbf{j}} |G[A]\rangle_A \otimes Z^{\sum_{b\in B} N^w_B(b) j_b} |\mathbf{j}\rangle_B, \tag{4.33}$$

where $j_b$ denotes the $b$-th dit of the outcome string $\mathbf{j}$, and $Z^{N^w_A(b)}$ (respectively, $Z^{N^w_B(b)}$ ) denotes the component of the operator $Z^{N^u(b)}$ that acts on subsystem $\mathcal{H}_A$ (respectively, $\mathcal{H}_B$ ). The notation $G[A]$ refers to the subgraph of $G$ induced on the set $A$, and $\Gamma_{AB}$ denotes the $|A| \times |B|$ submatrix of the adjacency matrix $\Gamma$ corresponding to the edges between subsystems $A$ and $B$. As a result, the reduced state on subsystem $A$ becomes

$$\rho_A = \frac{1}{d^{|B|}} \sum_{\mathbf{j}\in\mathbb{F}_d^{|B|}} Z^{\Gamma_{AB}\mathbf{j}} |G[A]\rangle_A \langle G[A]| Z^{\Gamma_{AB}\mathbf{j}}. \tag{4.34}$$

We will now show that the expression for $\rho_A$ simplifies to the maximally mixed state. This demonstrates that qudit $A$ is maximally entangled with the rest of the graph. Our derivation assumes that the qudit dimension $d$ is a prime number. This is a critical assumption because it means that the set of integers modulo $d$, denoted $\mathbb{Z}_d$, forms a finite field, $\mathbb{F}_d$. The defining property of a field that is crucial here is that every non-zero element has a unique multiplicative inverse. This allows for division and the guaranteed solvability of linear equations, which is not true for a composite $d$, where $\mathbb{Z}_d$ is only a ring.

Let's analyze the sum in the expression for $\rho_A$. The term $Z^{\Gamma_{AB}\mathbf{j}}|+\rangle\langle+|Z^{\Gamma_{AB}\mathbf{j}}$

appears for each outcome vector $\mathbf{j}$. Let $c = \Gamma_{AB}\mathbf{j} = \sum_{k=1}^{d} \Gamma_k j_k$. Our goal is to count how many times each possible value of $c \in F_d$ appears as we sum over all $d^{|B|}$ possible vectors $\mathbf{j}$.

Suppose that $\Gamma_1 \neq 0$ for a given graph. For any fixed value of $c$, Equation $\sum_{k=1}^{d} \Gamma_k j_k = c$ can be inverted to solve for $j_1$ as follows:

$$j_1 = \left( c - \sum_{k=2}^{|B|} \Gamma_k j_k \right) \cdot \Gamma_1^{-1} \tag{4.35}$$

This inversion is valid because all arithmetic is performed over the finite field $\mathbb{F}_d$, where every nonzero element admits a multiplicative inverse. In contrast, such inversion may not be possible over general rings or real numbers if $\Gamma_1$ is not invertible.

Since each $j_k \in \mathbb{F}_d$ can independently take on $d$ possible values, there are $d^{|B|-1}$ distinct choices of the vector $\mathbf{j} \in \mathbb{F}_d^{|B|}$ that yield the same value of $c$. Therefore, each state $Z^i|+\rangle$, where $i \in \mathbb{F}_d$, appears exactly $d^{|B|-1}$ times in the ensemble. This implies that the reduced state $\rho_A$ is a uniform mixture over all such phase-shifted states:

$$\rho_A = \frac{1}{d^{|B|}} \sum_{\mathbf{j} \in \mathbb{F}_d^{|B|}} Z^{\Gamma_{AB}\mathbf{j}} |G[A]\rangle_A \langle G[A]| Z^{\Gamma_{AB}\mathbf{j}} \propto d^{|B|-1} \left( \sum_{i=0}^{d-1} Z^i |+\rangle\langle+| Z^i \right) \propto I_{d\times d} \tag{4.36}$$

Hence, $\rho_A$ is proportional to the identity operator on $H_A$, confirming that it is a maximally mixed state. This explicit formula for the RDM of a subsystem within a graph state is the foundational equation we will analyze in the next chapter.

# CHAPTER V

# MAIN RESULT

In Chapter 3, quantum state verification was formulated as a hypothesis-testing problem, and the efficiency of a verification strategy was shown to be governed by the spectral gap of the verification operator. In Chapter 4, the algebraic structure of qudit graph states was introduced, and a key structural property was established: for a suitable one-qudit-versus-the-rest bipartition, the reduced density matrix of the chosen qudit is maximally mixed. The purpose of the present chapter is to combine these ingredients and derive the main theorem of this thesis, namely an upper bound on the spectral gap of any local verification strategy for prime-$d$ graph states. To identify the maximal bipartite entanglement in the graph state, we first partition the system into two parties: party A containing a single qudit and party B containing the remaining $n-1$ qudits. Consequently, this reduces the verification problem to the well-known bipartite maximally entangled case.

## 5.1 Problem Statement

Let $|G\rangle$ be an $n$-qudit graph state of local dimension $d$, where $d$ is prime, associated with a connected weighted graph $G$. Suppose that $\Omega$ is a verification operator for $|G\rangle$ constructed from local measurements, with perfect completeness,$\Omega|G\rangle = |G\rangle$. The goal is to determine how large the spectral gap $\nu(\Omega)$ can be under this locality restriction. This is the natural quantity to optimize, as the number of copies required for verification scales inversely with $\nu(\Omega)$. In the i.i.d. verification setting discussed earlier, one has the standard asymptotic relation:

$$N \approx \frac{\ln(1/\delta)}{\varepsilon\nu(\Omega)}.$$

Thus, an upper bound on $\nu(\Omega)$ immediately yields a lower bound on the best possible efficiency of verification.

The first observation is that local measurements are automatically separable across any chosen bipartition. Let the full Hilbert space be decomposed as $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, where $A$ consists of a single qudit and $B$ contains the remaining $n-1$ qudits. A local measurement on the full $n$-qudit system is implemented by measuring each qudit locally and then combining the outcomes via classical post-processing. Therefore, every effect associated with such a measurement is a sum of tensor-product positive operators across the cut $A|B$. Hence, any verification operator $\Omega$ built from local measurements is separable with respect to the bipartition $A|B$. This immediately implies that the local-verification problem can be bounded from above by the more general class of separable verification strategies across the chosen bipartition. In other words, if a bound holds for separable verification operators across $A|B$, then it certainly holds for local verification operators, as explained in Note 3.

**Note 3:**

Let $LO$, $LOCC$, and $SEP$ denote the sets of Local Operations, Local Operations and Classical Communication, and Separable Measurement Operations, respectively, as defined in Chapter 2. It is well-established that $SEP$ represents a broader class of operations than $LOCC$, which in turn encompasses $LO$. This hierarchical relationship is expressed as [31]

$$LO \subset LOCC \subset SEP$$

A fundamental principle of optimization dictates that the maximum value of a function over a given set can never exceed its maximum value over a larger set containing it. In other words, expanding the search space through more options can only yield an equal or superior result, never a worse one. Applying this principle to the spectral gap, $\nu(\Omega)$, we obtain the following inequality:

$$\max_{\Omega \in LO} \nu(\Omega) \leq \max_{\Omega \in LOCC} \nu(\Omega) \leq \max_{\Omega \in SEP} \nu(\Omega)$$

This inequality demonstrates that the optimal spectral gap achievable through local operators, which are subject to more stringent constraints, cannot exceed the optimal spectral gap attainable within the broader class of separable operators.

Therefore, our objective is to demonstrate that the graph state $|G\rangle$ is maximally entangled across a suitable bipartition. Subsequently, we apply the established spectral-gap upper bound for the separable verification of bipartite maximally entangled states.

## 5.2 Reduction Strategy

To demonstrate that the graph state $|G\rangle$ is maximally entangled across a suitable bipartition, we utilize the second key ingredient established in Chapter 4. Upon partitioning the system into subsystems $A$ and $B$, the reduced density

matrix for subsystem $A$ is given by:

$$\rho_A = \frac{1}{d^{|B|}} \sum_{\mathbf{j}\in\mathbb{F}_d^{|B|}} Z^{\Gamma_{AB}\mathbf{j}} |G[A]\rangle_A \langle G[A]| Z^{\Gamma_{AB}\mathbf{j}} \propto d^{|B|-1} \left( \sum_{i=0}^{d-1} Z^i |+\rangle\langle +| Z^i \right) \propto I_{d\times d} \tag{5.1}$$

This demonstrates that subsystem $A$ is maximally mixed. For a pure bipartite state, this is equivalent to maximal entanglement across the bipartition $A|B$. Indeed, according to the Schmidt decomposition, there exist orthonormal bases $\{|j\rangle_A\}_{j=0}^{d-1}$ in $\mathcal{H}_A$ and $\{|\phi_j\rangle_B\}_{j=0}^{d-1}$ in $\mathcal{H}_B$ such that:

$$|G\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_A \otimes |\phi_j\rangle_B. \tag{5.2}$$

Since the Schmidt coefficients are all equal to $1/\sqrt{d}$, the state is maximally entangled across the chosen cut, as shown in Note 4. Alternatively, we can state that it is locally unitary (LU) equivalent to a standard maximally entangled state.

**Note 4: Claim**

If the reduced state under the bipartition $A|B$ is proportional to the identity matrix, then the state is maximally entangled across that cut.

Proof: Suppose that this graph state is maximally entangled. This implies that it can be expressed in the Schmidt form as:

$$|G\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_A \otimes |\phi_j\rangle_B.$$

Subsequently, by tracing out subsystem $B$, we obtain the reduced density matrix for subsystem $A$:

$$\begin{aligned}
\rho_A = \mathrm{Tr}_B(|G\rangle\langle G|) &= \mathrm{Tr}_B \left( \frac{1}{d} \sum_{i,j=0}^{d-1} |j\rangle\langle i|_A \otimes |\phi_j\rangle\langle\phi_i|_B \right) \\
&= \frac{1}{d} \sum_{i,j=0}^{d-1} |j\rangle\langle i|_A \delta_{ij} \\
&= \frac{1}{d} \sum_{j=0}^{d-1} |j\rangle\langle j|_A \\
&\propto I_{d\times d}
\end{aligned}$$

This result is perfectly consistent with the initial claim.

We have established that our graph state is maximally entangled across the bipartition $A|B$. However, before directly claiming the spectral gap bound for the verification operator of a maximally entangled state, we must address a dimensional discrepancy. Note that our graph state resides in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^d \otimes \mathbb{C}^{d^{n-1}}$, whereas the standard protocol for a maximally entangled state is formulated in $\mathbb{C}^d \otimes \mathbb{C}^d$. In the following section, we will demonstrate that the original spectral gap bound remains completely valid. From the previous setup, our target graph state in $\mathbb{C}^d \otimes \mathbb{C}^{d^{n-1}}$ can be expressed as in Eq. (5.2):

$$|G\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_A \otimes |\phi_j\rangle_B.$$

We now define an isometry, $V$, to map the standard maximally entangled

state, $|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_A \otimes |j\rangle_B$, into the larger space. Specifically,

$$V : \mathbb{C}^d \to \mathbb{C}^{d^{n-1}}$$

is defined by its action on the basis states as $V|j\rangle = |\phi_j\rangle$, satisfying the isometry condition $V^\dagger V = I_{d\times d}$. Therefore, we can write:

$$(I \otimes V)|\Phi_d\rangle = (I \otimes V)\left(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_A \otimes |j\rangle_B\right) \tag{5.3}$$

$$= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_A \otimes V|j\rangle_B \tag{5.4}$$

$$= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_A \otimes |\phi_j\rangle_B \tag{5.5}$$

$$= |G\rangle \tag{5.6}$$

In other words, under this bipartition, $|G\rangle$ behaves exactly like the standard maximally entangled state simply embedded within a larger Hilbert space. Consequently, we can directly apply the known spectral gap result for the generalized maximally entangled state, which is $d/(d+1)$. Crucially, the spectral gap does not increase as the dimension of subsystem $B$ expands, as explained in Note 5.

**Note 5: Claim**

For a separable verification operator $\Omega \in SEP$,

$$\max_{\Omega|G\rangle=|G\rangle} \nu(\Omega) \leq \max_{\Omega'|\Phi_d\rangle=|\Phi_d\rangle} \nu(\Omega')$$

where $\Omega$ is the verification operator for the graph state $|G\rangle$, and $\Omega'$ is the compressed verification operator for the maximally entangled state $|\Phi_d\rangle$.

Proof: For a separable verification operator $\Omega$ designed for $|G\rangle$ acting on the larger space $\mathbb{C}^d \otimes \mathbb{C}^{d^{n-1}}$, we define the compressed verification operator $\Omega'$ as:

$$\Omega' = (I \otimes V^\dagger)\Omega(I \otimes V)$$

First, we must verify that $\Omega'$ is a valid verification operator for $|\Phi_d\rangle$. Applying it to the state yields:

$$\begin{aligned}
\Omega'|\Phi_d\rangle &= (I \otimes V^\dagger)\Omega(I \otimes V)|\Phi_d\rangle \\
&= (I \otimes V^\dagger)\Omega|G\rangle \\
&= (I \otimes V^\dagger)|G\rangle \\
&= (I \otimes V^\dagger)(I \otimes V)|\Phi_d\rangle \\
&= |\Phi_d\rangle
\end{aligned}$$

Thus, $\Omega'$ perfectly preserves $|\Phi_d\rangle$, thereby constituting a valid verification operator.

Returning to the optimization problem, the maximum eigenvalue for states orthogonal to the target state is defined as:

$$\beta(\Omega) = \max_{|\varphi\rangle \perp |G\rangle} \langle\varphi|\Omega|\varphi\rangle \quad , \quad \nu(\Omega) = 1 - \beta(\Omega)$$

where $|\varphi\rangle$ is any state in the full Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^{d^{n-1}}$. This can be viewed as an optimization problem over the larger space. Similarly, for the compressed operator $\Omega'$, we have:

$$\beta(\Omega') = \max_{|\alpha\rangle \perp |\Phi_d\rangle} \langle\alpha|\Omega'|\alpha\rangle \quad , \quad \nu(\Omega') = 1 - \beta(\Omega')$$

where $|\alpha\rangle$ represents any state in the smaller subspace, specifically $|\alpha\rangle \in \mathbb{C}^d \otimes \mathcal{K}$, with $\mathcal{K} = \text{span}(\{|\phi_j\rangle\}_{j=0}^{d-1})$. This relation, $\mathbb{C}^d \otimes \mathcal{K} \subset \mathbb{C}^d \otimes \mathbb{C}^{d^{n-1}}$, indicates that this can be conceptually viewed as a search problem restricted to a smaller space.Because $V$ is an isometry, we can establish the following relationship:

$$\langle G|\varphi\rangle = 0 = \left(\langle\Phi_d|(I \otimes V^\dagger)\right)\left((I \otimes V)|\alpha\rangle\right) = \langle\Phi_d|\alpha\rangle$$

Following the optimization logic previously discussed in Note 3, finding a maximum over a restricted subspace cannot yield a value greater than maximizing over the entire space. Therefore:

$$\max_{|\alpha\rangle \perp |\Phi_d\rangle} \langle\alpha|\Omega'|\alpha\rangle \leq \max_{|\varphi\rangle \perp |G\rangle} \langle\varphi|\Omega|\varphi\rangle \implies \beta(\Omega') \leq \beta(\Omega)$$

Consequently, for the spectral gaps, we obtain:

$$\nu(\Omega) = 1 - \beta(\Omega) \leq 1 - \beta(\Omega') = \nu(\Omega')$$

This concludes the proof that $\nu(\Omega) \leq \nu(\Omega')$.

# CHAPTER VI

# CONCLUSION AND DISCUSSION

This thesis studied quantum state verification for prime $d$ qudit graph states under local measurement restrictions. The main objective was to determine how large the spectral gap of a local verification operator can be for this class of target states, since the spectral gap directly controls the efficiency of the verification protocol.

The main result obtained in this thesis is the upper bound

$$\nu(\Omega) \leq \frac{d}{d+1},$$

where $\Omega$ is a local verification operator for the target graph state and $\nu(\Omega)$ denotes its spectral gap. This shows that no local verification strategy for the graph states considered here can achieve a spectral gap larger than $d/(d+1)$.The proof was based on the entanglement structure of qudit graph states. First, the reduced density matrix of a suitable single qudit was shown to be maximally mixed. This implies that the graph state is maximally entangled across a bipartition of one qudit versus the remaining $n-1$ qudits. Using this property, the verification problem was reduced to the known bipartite maximally entangled case, from which the bound $d/(d+1)$ follows.

## 6.1 Discussion

It is worth noting that our proof method is exclusively applicable to cases where $d$ is a prime number. This limitation arises because the proof relies on the mathematical structure of a finite field, which guarantees the existence of multiplicative inverses. Consequently, this approach cannot be directly generalized to scenarios where $d$ is a composite number. This is demonstrated by the following

counterexample: consider a 4-qudit graph state where $d = 4$, with the adjacency matrix given by:

$$\begin{bmatrix} 0 & 2 & 2 & 0 \\ 2 & 0 & 2 & 2 \\ 2 & 2 & 0 & 2 \\ 0 & 2 & 2 & 0 \end{bmatrix}$$

Upon computing the reduced density matrix for subsystem $A$ of this specific graph structure, we obtain:

$$\rho_A \propto |0\rangle\langle 0| + |2\rangle\langle 2| \neq I_{d\times d}$$

As is evident, this reduced density matrix does not take the form of an identity matrix. Therefore, we cannot conclude that the spectral gap bounds established for prime dimensions will universally apply to composite dimensions.

One of the remaining open problems is whether it is always possible to identify specific measurements that saturate the established spectral gap bounds. While our current framework provides a theoretical lower bound for prime dimensions, future research could investigate the existence of optimal measurements that achieve equality in these bounds across all graph state configurations.

# REFERENCES

# REFERENCES


1. DURT T, ENGLERT BG, BENGTSSON I, ˙ZYCZKOWSKI K. ON MUTUALLY UNBIASED BASES. Int J Quantum Inform. 2010;08(04):535-640. Available from: https://doi.org/10.1142/S0219749910006502.

2. Wootters WK, Fields BD. Optimal state-determination by mutually unbiased measurements. Ann Phys. 1989;191(2):363-81. Available from: https://www.sciencedirect.com/science/article/pii/0003491689903229.

3. Adamson RBA, Steinberg AM. Improving Quantum State Estimation with Mutually Unbiased Bases. Phys Rev Lett. 2010;105(3):030406. Available from: https://link.aps.org/doi/10.1103/PhysRevLett.105.030406.

4. Wang J, Han ZY, Wang SB, Li Z, Mu LZ, Fan H, et al. Scalable quantum tomography with fidelity estimation. Phys Rev A. 2020;101(3). Available from: http://dx.doi.org/10.1103/PhysRevA.101.032321.

5. Czerwinski A. Quantum state tomography with informationally complete POVMs generated in the time domain. Quantum Inf Process. 2021;20(3):105. Available from: https://doi.org/10.1007/s11128-021-03045-9.

6. Flammia ST. On SIC-POVMs in prime dimensions. J Phys A Math Gen. 2006;39(43):13483. Available from: https://dx.doi.org/10.1088/0305-4470/39/43/007.

7. Appleby DM, Dang HB, Fuchs CA. Symmetric Informationally-Complete Quantum States as Analogues to Orthonormal Bases and Minimum-Uncertainty States. Entropy. 2014;16(3):1484-92. Available from: https://www.mdpi.com/1099-4300/16/3/1484.

8. Smith AWR, Gray J, Kim MS. Efficient Quantum State Sample Tomography with Basis-Dependent Neural Networks. PRX Quantum. 2021;2(2):020348. Available from: https://link.aps.org/doi/10.1103/PRXQuantum.2.020348.

9. Yu XD, Shang J, Gühne O. Statistical Methods for Quantum State Verification and Fidelity Estimation. Adv Quantum Technol. 2022;5(5). Available from: http://dx.doi.org/10.1002/qute.202100126.

10. Zhu H, Hayashi M. Efficient Verification of Pure Quantum States in the Adversarial Scenario. Phys Rev Lett. 2019;123(26). Available from: http://dx.doi.org/10.1103/PhysRevLett.123.260504.

11. Pallister S, Linden N, Montanaro A. Optimal Verification of Entangled States with Local Measurements. Phys Rev Lett. 2018;120(17):170502. Available from: https://link.aps.org/doi/10.1103/PhysRevLett.120.170502.

12. Dangniam N, Han YG, Zhu H. Optimal verification of stabilizer states. Phys Rev Res. 2020;2(4). Available from: http://dx.doi.org/10.1103/PhysRevResearch.2.043323.

13. Zhang WH, Zhang C, Chen Z, Peng XX, Xu XY, Yin P, et al. Experimental Optimal Verification of Entangled States Using Local Measurements. Phys Rev Lett. 2020;125(3). Available from: http://dx.doi.org/10.1103/PhysRevLett.125.030506.

14. Li Z, Han YG, Zhu H. Optimal Verification of Greenberger-Horne-Zeilinger States. Phys Rev Appl. 2020;13(5). Available from: http://dx.doi.org/10.1103/PhysRevApplied.13.054002.

15. Nielsen MA, Chuang IL. Quantum Computation and Quantum Information. 10th ed. Cambridge: Cambridge University Press; 2010.

16. Watrous J. The Theory of Quantum Information. Cambridge University Press; 2018.

17. Bengtsson I, Życzkowski K. Geometry of Quantum States: An Introduction to Quantum Entanglement. 2nd ed. Cambridge University Press; 2017. Chapter 10, Section 10.1, p. 251.

18. Qiskit Community. Randomization of quantum measurements — POVM Toolbox Documentation [Internet]; 2024. [cited 2026 May 4]. Available from: https://qiskit-community.github.io/povm-toolbox/explanations/randomization.html.

19. Altepeter JB, Jeffrey ER, Kwiat PG. Photonic State Tomography. In: Berman PR, Lin CC, editors. Advances in Atomic, Molecular, and Optical Physics. vol. 52. Elsevier; 2005. p. 105-59.

20. Haah J, Harrow AW, Ji Z, Wu X, Yu N. Sample-optimal tomography of quantum states. IEEE Trans Inf Theory. 2017;63(9):5628-41.

21. Yu XD, Shang J, Gühne O. Optimal verification of general bipartite pure states. npj Quantum Inf. 2019;5(1):112.

22. Xu Q, Tan X, Ou Y, Bao D, Huang R. Efficient verification of two-colorable graph states. Phys Rev A. 2024;110(1):012606.

23. Zhu H, Hayashi M. Efficient verification of hypergraph states. Phys Rev Appl. 2019;12(5):054047.

24. Li Z, Han YG, Sun HF, Shang J, Zhu H. Verification of phased Dicke states. Phys Rev A. 2021;103(2):022601.

25. Liu YC, Yu XD, Shang J, Zhu H, Zhang X. Efficient verification of Dicke states. arXiv:190401979 [quant-ph] [Internet]. 2019. [cited 2026 May 10]. Available from: https://arxiv.org/abs/1904.01979.

26. Zhu H, Li Y, Chen T. Efficient verification of ground states of frustration-free Hamiltonians. Quantum. 2024;8:1221.

27. Hostens E, Dehaene J, De Moor B. Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic. Phys Rev A. 2005;71(4):042315.

28. Sarkar R, Yoder TJ. The qudit Pauli group: non-commuting pairs, non-commuting sets, and structure theorems. Quantum. 2024;8:1307.

29. Keet A, Fortescue B, Markham D, Sanders BC. Quantum secret sharing with qudit graph states. Phys Rev A. 2010;82(6):062315. Available from: https://link.aps.org/doi/10.1103/PhysRevA.82.062315.

30. Hein M, Dür W, Eisert J, Raussendorf R, Nest MVd, Briegel HJ. Entanglement in graph states and its applications. arXiv:quant-ph [Internet]. 2006. [cited 2026 May 10]. Available from: https://arxiv.org/abs/quant-ph/0602096.

31. Chitambar E, Leung D, Mančinska L, Ozols M, Winter A. Everything You Always Wanted to Know About LOCC (But Were Afraid to Ask). Commun Math Phys. 2014;328(1):303-26. Available from: https://doi.org/10.1007/s00220-014-1953-9.

# APPENDIX

# APPENDIX A DETAILED DERIVATION OF Z MEASUREMENT

We provide here a step-by-step derivation of Eqs. (4.26) through (4.29) in the main text, which describe the decomposition of a graph state with respect to a subset of qudits $B \subset V$. The goal is to understand the effect of measuring qudits in $B$ in the computational basis.

Let us isolate the operations involving a specific qudit $b \in B$. The graph state $|\mathrm{G}\rangle$ can be decomposed by separating the controlled- $Z$ gates (denoted $CZ$ ) acting on $b$ from those that do not:

$$|G\rangle = \prod_{(b,c)\in E} CZ_{\{b,c\}}^{w((b,c))} |+\rangle_b \otimes \prod_{(a\neq b, d\neq b)\in E} CZ_{\{a,d\}}^{w((a,d))} |+\rangle^{\otimes |V|-1} \tag{A.1}$$

$$= \prod_{(b,c)\in E} CZ_{\{b,c\}}^{w((b,c))} |+\rangle_b \otimes |G - \{b\}\rangle \tag{A.2}$$

where $|G - \{b\}\rangle$ is the graph state with qudit $b$ removed, and $CZ_{\{a,b\}}^{w}$ denotes the generalized controlled-$Z$ gate of weight $w \in \mathbb{F}_d$. We now examine the term $\prod_{(b,c)\in E} CZ_{\{b,c\}}^{w((b,c))}$. The product of these gates can be expanded as:

$$\prod_{(b,c)\in E} CZ_{\{b,c\}}^{w((b,c))} = (|0\rangle_b\langle 0| \otimes I_{c_0} + |1\rangle_b\langle 1| \otimes Z_{c_0}^{w((b,c_0))} + \ldots) \tag{A.3}$$

$$(|0\rangle_b\langle 0| \otimes I_{c_1} + |1\rangle_b\langle 1| \otimes Z_{c_1}^{w((b,c_1))} + \ldots) \tag{A.4}$$

$$(|0\rangle_b\langle 0| \otimes I_{c_2} + |1\rangle_b\langle 1| \otimes Z_{c_2}^{w((b,c_2))} + \ldots) \ldots \tag{A.5}$$

Computing just the first two terms explicitly, we obtain:

$$(\text{First})(\text{Second}) = (|0\rangle_b\langle 0| \otimes I_{c_0c_1} + |1\rangle_b\langle 1| \otimes Z_{c_0}^{w(b,c_0)} Z_{c_1}^{w(b,c_1)} + \ldots) \tag{A.6}$$

Continuing this pattern across all $m = |N_b|$ neighbors of $b$, the result is as follows:

$$|0\rangle_b\langle 0| \otimes I_{c_0c_1\ldots c_{m-1}} + |1\rangle_b\langle 1| \otimes Z_{c_0}^{w(b,c_0)} Z_{c_1}^{w(b,c_1)} \ldots Z_{c_{m-1}}^{w(b,c_{m-1})} + |2\rangle_b\langle 2| \otimes Z_{c_0}^{2w(b,c_0)} Z_{c_1}^{2w(b,c_1)} \ldots Z_{c_{m-1}}^{2w(b,c_{m-1})} + \ldots \tag{A.7}$$

This expression can be compactly written as:

$$\prod_{(b,c)\in E} CZ_{\{b,c\}}^{w((b,c))} = \sum_{j=0}^{d-1} |j\rangle_b\langle j| \otimes \left(Z^{N^w(b)}\right)^j \tag{A.8}$$

Now consider the projection of the full graph state $|G\rangle$ onto the eigenspace corresponding to eigenvalue $\omega^k$. We define the projector $P_{\omega^k,b} = |k\rangle_b\langle k|$, yielding:

$$P_{\omega^k,b}|G\rangle = (|k\rangle_b\langle k|)((\sum_{j=0}^{d-1} |j\rangle_b\langle j| \otimes \left(Z^{N^w(b)}\right)^j)|+\rangle_b \otimes |G - \{b\}\rangle) \tag{A.9}$$

$$= ((\sum_{j=0}^{d-1} \langle k|j\rangle|k\rangle_b\langle j| \otimes \left(Z^{N^w(b)}\right)^j)|+\rangle_b \otimes |G - \{b\}\rangle) \tag{A.10}$$

$$= (|k\rangle_b\langle k| \otimes \left(Z^{N^w(b)}\right)^k)|+\rangle_b \otimes |G - \{b\}\rangle) \tag{A.11}$$

$$= \langle k\,|_b\,+\rangle|k\rangle_b \otimes \left(Z^{N^w(b)}\right)^k |G - \{b\}\rangle \tag{A.12}$$

$$= \frac{1}{\sqrt{d}}|k\rangle_b \otimes \left(Z^{N^w(b)}\right)^k |G - \{b\}\rangle \tag{A.13}$$

which matches the corresponding equations presented in the main text.