Device-Independent Framework for Self-testing Quantum states and measurements

A Thesis

submitted to

Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
Master of Science in Quantum Technology

by

Khushi Sharma

Indian Institute of Science Education and Research Pune

April, 2026

Supervisor: Prof. Ujjwal Sen

Certificate

This is to certify that this dissertation entitled "Device-Independent Framework for Self-testing Quantum states and measurements" submitted towards the partial fulfilment of the Master of Science in Quantum Technology represents study/work carried out by Khushi Sharma from Indian Institute of Science Education and Research Pune under the supervision of Prof. Ujjwal Sen (Harish Chandra Research Institute, Allahabad) during the academic year 2025–2026.

Ujjwal Sen.

Signature of Supervisor (Prof. Ujjwal Sen) Date: 24/04/26

Signature of Advisory Member (Prof. TS Mahesh) Date: ________

Declaration

I hereby declare that the matter embodied in the report entitled "Device-Independent Framework for Self-testing Quantum states and measurements" are the results of the work carried out by me at the Harish Chandra Research Institute, Allahabad under the supervision of Prof. Ujjwal Sen (Harish Chandra Research Institute, Allahabad) and the same has not been submitted elsewhere for any other degree.

Khushi

Signature of the Author (Khushi Sharma) Date: 24-04-2026

Abstract

Quantum Key Distribution protocols are proven secure in theory, as their security relies on the concepts of quantum mechanics. It includes the disturbance created by the measurement and the No-cloning theorem. But in real experiments, there may be some imperfections in the devices (detectors or the photon source) which deviates them from the ideal behavior.

To deal with this, we move to the scenario where we treated the devices as black-boxes. Self-testing is a method which is independent of any specific device and can identify the properties of a [1] physical device without knowing its internal structure or the [1] Hilbert space dimension. Here we present a detailed proof of the self-testing method of entangled two-qubit state [2] and three qubit W state in device-independent scenario. In self-testing, we only observe the probabilities $p(a_1a_2|x_1x_2)$. Violation of the Bell inequalities [3] allows to keep the correlations outside of the local polytope, ensuring that the correlations are produced by some quantum state.

Acknowledgements

I would like to sincerely thank Prof. Ujjwal Sen for his constant support, mentoring, and for giving me the opportunity to work on this thesis. His expertise, mentorship, and patience have played an important role in shaping my understanding of the subject. I am also very grateful to Prof. T.S. Mahesh for being my advisory supervisor and for his constant support throughout my thesis.

I would like to thank the Indian Institute of Science Education and Research (IISER) Pune for providing me a supportive academic environment, and the Harish-Chandra Research Institute (HRI), Allahabad for offering a motivating research atmosphere during the course of this thesis. I would also like to thank my seniors for their help, discussions, and guidance along the way.

Lastly, I am deeply thankful to my parents and all my friends for their constant support, encouragement, and belief in me.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In the recent years, Quantum Technologies are rapidly shaping the field of *Communication*, *Cryptography*, *Computation* and also providing a benefit of Quantum over classical systems. However, the most difficult challenge one faces is to determine accurately the Quantum states and the choices of measurement device. Most of the cryptography protocols assumes the internal working of the devices are completely trusted and are well-known. But in real experiment, there is always some level of noise present or some imperfections in the devices. To overcome this problem, we moves toward the device independent scenario ie., to treat the devices as black boxes. *Self-testing* is a strongest tool for certifying a quantum state and measurement only based on the correlations in the DI scenario. It also plays a significant role in the applications such as the Quantum key Distribution, the DI random number generation, and the verification of Quantum devices. In this thesis, we present the self-testing of specific quantum states and measurement in the device-independent framework, also including their behaviour in real experimental situation.

The **Chapter 2** provides the background for this work. We start with discussing the foundations of Quantum Mechanics and introduce some important concepts: The Schmidt Decomposition, Quantum Entanglement, and the (EPR) paradox. Then moves to the Bell inequalities, describing how their classical correlations are different from the quantum correlations. We give an overview of the Quantum Cryptography, which includes the well-known protocols: BB84 and Ekert 91, and explains the motivation of Device-Independent QKD (DIQKD), explaining its advantages over the standard QKD.

The **Chapter 3** mainly focuses on self-testing in a device-independent framework. We explain how quantum states and measurements can be tested only from the observed correlations, without even relying on the assumptions about the internal details of the devices. The chapter explains the use of Bell inequalities to certify entanglement and to enable the self-testing. We also discuss the construction of local isometries and how they are used to describe the underlying quantum state. We present the statements of the robustness of self-testing of states and applications of the (SOS) decomposition techniques.

In **Chapter 4** we present the main results of our work.We examine the constraints when measurements are compatible and prove the necessity of measurement incompatibility for self-testing. Detailed proof of the self-testing of entangled two-qubit states and the three-qubit W state are provided. The **Chapter 5** concludes the thesis by summarizing about the key findings and results.

Chapter 2

Background and Literature Review

2.1 Foundations of Quantum Mechanics

2.1.1 Physical State a system

The system's physical state is explained by a state vector or by density operator. A state vector is usually describe by $|\Psi\rangle$ which is point in Hilbert space. All the information about the system for any given time (t) denoted by the state vector $|\Psi(t)\rangle$.

Dirac Notations

By convention, the bra $\langle b|$ is a row vector and the ket $|b\rangle = (\langle b|)^\dagger$ which the adjoint (transpose + complex conjugate) of $\langle b|$. The inner product $\langle b \mid b\rangle = 1$ for normalized vectors. If a vector $|b_{\text{un}}\rangle$ is not normalized, then the normalized vector is

$$|b\rangle = \frac{|b_{\text{un}}\rangle}{\sqrt{\langle b_{\text{un}} \mid b_{\text{un}}\rangle}}. \tag{2.1}$$

For the two orthogonal vectors, $|b\rangle$ and $|b^{\perp}\rangle$, the inner product

$$\langle b \mid b^{\perp}\rangle = 0$$

Basis Representation

In quantum mechanics, basis is a set of linearly independent, mutually orthogonally unit vectors that spans the Hilbert space. Any [8] quantum state $|\psi'\rangle$ can also be expressed as unique superposition of these basis vectors. For any basis vectors

$$\langle g|h\rangle = \delta_{g,h} \quad \text{(orthonormality)} \quad \text{and} \quad \sum_g |g\rangle\langle g| = 1 \quad \text{(completeness)},$$

$\delta_{g,h}$ is called Kronecker delta.

A complete basis can express any arbitrary state $|\Psi'\rangle$ in the form

$$|\Psi'\rangle = \sum_{g=1}^{N} c_g|g\rangle \quad \text{or} \quad \langle\Psi'| = \sum_{g=1}^{N} c_g^*\langle g| \tag{2.2}$$

where c_g are the complex scalar coefficients such that $|c_g|^2$ are the probability amplitudes and $\sum_{k=1}^{N} |c_g|^2 = 1$. If a projector $\mathbb{P}_g$ acts on $|\Psi'\rangle$, then it picks out a component

$$\mathbb{P}_g|\Psi\rangle = \sum_{h=1}^{N} c_h|h\rangle\langle h|g\rangle = \sum_{l=1}^{N} c_h|g\rangle\delta_{gh} = c_g|g\rangle. \tag{2.3}$$

The Density Matrix [9]

Considering a well-defined quantum state represented as $|\psi_1\rangle$. The density matrix ρ [10] is denoted by an outer product:

$$\rho = |\psi_1\rangle\langle\psi_1|. \tag{2.4}$$

The matrix elements [11] of ρ are:

$$\langle g|\rho|h\rangle = \langle g|\psi_1\rangle\langle\psi_1|h\rangle. \tag{2.5}$$

The expectation value of an operator [12] G is expressed as :

$$\langle\hat{G}\rangle = \langle\psi_1|\hat{G}|\psi_1\rangle = \mathrm{Tr}(\rho\hat{G})$$

2.1.2 Observables

Observable [13] is defined as a measurable property of the physical system. In quantum mechanics observables are the self-adjoint operator. Operators are the linear maps that takes vectors to vectors [14].

The adjoint of an operator [15] G is:

$$\langle\phi_*|G|\psi_*\rangle = \langle G^\dagger\phi_*|\psi_*\rangle \tag{2.6}$$

for all states $|\psi_*\rangle$ and $|\phi_*\rangle$.

In a Hilbert space $\mathcal{H}$, a self-adjoint operator [10] has spectral representation, and its eigenstates forms a full orthonormal basis in $\mathcal{H}$. The expression for self-adjoint operator O is:

$$G = \sum_n a_n P_n \tag{2.7}$$

Here a_n are the eigenvalues of G, and P_n are the orthogonal projection. The P_n

satisy:

$$\begin{aligned} P_n P_m &= \delta_{nm} P_n, \\ P_n^\dagger &= P_n, \\ \sum_n P_n &= I \end{aligned} \tag{2.8}$$

It is the projection onto the same eigenvector if a_n is nondegenerate.

$$P_n = |n\rangle\langle n| \tag{2.9}$$

2.1.3 Measurement

Measuring the observable [15] G for a system in state [10]$|\psi_*\rangle$ gives an eigenvalue a_n having the probability:

$$p(a_n) = \langle P_{a_n} \rangle_{\Psi_*} = \langle \Psi_* | P_{a_n} | \Psi_* \rangle = \| P_{a_n} | \Psi_* \rangle \|^2 \tag{2.10}$$

This is known as Born rule. The normalized quantum state becomes as follows if the result a_n is obtained:

$$\frac{P_{a_n} |\Psi_*\rangle}{\| P_{a_n} |\Psi_*\rangle \|} = \frac{P_{a_n} |\Psi_*\rangle}{\sqrt{\langle \Psi_* | P_{a_n} | \Psi_* \rangle}} \tag{2.11}$$

2.1.4 Dynamics

The evolution of quantum system with time, which is the system's Hamiltonian is unitary. The Schrödinger equation governs it :

$$i\hbar \frac{d}{dt} |\psi_1'(t)\rangle = \mathcal{H} |\psi_1'(t)\rangle, \tag{2.12}$$

[16] H is the Hamiltonian.

2.2 Schmidt Decomposition

[17] A bipartite pure state written as:

$$|\psi_1\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$$

Schmidt decomposition [15] says, any state can be decomposed in form:

$$|\psi_1\rangle_{AB} = \sum_{k,l} \alpha_{k,l} \, |k\rangle_A \otimes |l\rangle_B,$$

where [17] $|k\rangle_A$ is the orthonormal basis in the subsystem A and $|l\rangle_B$ is the orthonormal basis in the subsystem B.

Then, the reduced density matrix of two subsystems are:

$$\rho_A = \sum_k \alpha_k^2 \, |k\rangle\langle k|$$

$$\rho_B = \sum_l \alpha_l^2 \, |l\rangle\langle l|$$

Number of non-zero[18] α is called the Schmidt Rank. It is used for detecting Entanglement, ie., for more than one non zero α (Schmidt coefficient), state is entangled.

2.3 Quantum Entanglement

A bipartite pure state is said to be entangled state when more than one Schmidt coefficient is non-zero, else it is called separable state.[19]

When one can write : $|\psi_1'\rangle_{AB} = |\psi_1'\rangle_A \otimes |\psi_1'\rangle_B$, in this form, then it is a separable state.

Other way, when it is written as : $|\psi_1'\rangle_{AB} \neq |\psi_1'\rangle_A \otimes |\psi_1'\rangle_B$, it is called an entangled state.

2.4 Einstein-Podolsky-Rosen (EPR) Pairs, Bell's inequality

In Classical physics, objects have pre-assigned values irrespective of whether they are measured or not. Measurement on them just revealed their pre-assigned values. But this is not the same in quantum mechanics. Assuming a qubit with state: [20]

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right) \tag{2.13}$$

Now measuring the qubit in Z basis, gives $|0\rangle$ with eigenvalue (+1) with probability 1/2 and gives $|1\rangle$ with eigenvalue (-1) with probability 1/2. We can't infer this probability as 1/2 before experiment.

On applying Hadamard operator to $|\psi\rangle$, we get:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.14}$$

$$H|\psi\rangle = |0\rangle \tag{2.15}$$

Hence, Born rule says measuring a qubit [21] that is in state $|\psi\rangle$ gives $|0\rangle$ having probability 1. Suppose we assume that, before measurement, the state $|\psi\rangle$ is either $|0\rangle$ or $|1\rangle$, each having probability $\frac{1}{2}$. Applying the Hadamard operator H to $|0\rangle$ gives

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$

and applying it to $|1\rangle$ gives

$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

Since each case occurs with probability $\frac{1}{2}$, [11] in computational basis the measurement gives $|0\rangle$ and $|1\rangle$ each having similar probability $\frac{1}{2}$. However, this contradicts Eq.(2.15), which predicts that the measurement outcome is $|0\rangle$ with probability 1.

So Quantum mechanics says that the outcomes are in-deterministic until measurement.

2.4.1 EPR Experiment

Albert Einstein, Boris Podolsky and Nathan Rosen, the physicists in year 1935 put a thought experiment ie., Einstein-Podolsky-Rosen (EPR) paradox which states that the Quantum mechanics is incomplete, there must be a hidden variable determining the outcome.

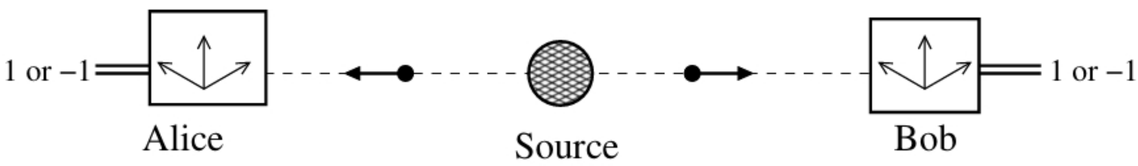

Figure 2.1: Setup of EPR experiment [4]

In this experiment, there is a source in between two party namely Alice and Bob, which are spatially distant apart, which is emits pair of qubits (photons) prepared in an entangled bell state say,

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \tag{2.16}$$

Suppose they both independently perform measurement on their qubits (ie. photon) in computational Z basis. If Alice gets +1 ie., state in $|0\rangle$, similarly Bob gets -1 ie., state in $|1\rangle$ or the vice versa, there result are always anti-correlated. If they both measure in any direction along the Bloch sphere, defined by θ, ϕ, they will get anti-correlated result, if they measure in same direction, regardless of which direction they have choosen for measurement. In each run, they randomly choose the measurement direction and for each measurement they record the outcome as +1 or -1.

- **Locality Assumption:** EPR assumed when two particles are separated far away, so [22] measurement on one particle cannot instantaneously affect the other particle. (" No spooky action at a distance").

- **Realism Assumption** Particles have definite properties independent of whether we measure them or not.

Einstein thought may be Quantum Mechanics is incomplete if Local Realism is true, because it cannot describe the definite values that EPR showed must exist. It was assumed that particles may contain some secret information (hidden variable) that determines the result.

2.4.2 Bell's Inequality

[23] Bell inequalities gives a way to distinguish among the classical theory and the quantum mechanics predictions. In a Bell experiment, the two parties, one party Alice and other party Bob performs measurement on the shared system. Each of them chooses a measurement setting x_1, x_2 and outcome outcome as a_1, a_2.

Alice chooses input setting as $x_1 \in \{0, 1\}$ corresponds to outcome as $a_1 \in \{-1, 1\}$ and Bob chooses input setting as $x_2 \in \{0, 1\}$ and corresponds to outcome $a_2 \in \{-1, 1\}$. The correlations are determined by probability $p(a_1, a_2|x_1, x_2)$.

CHSH Inequality:

It is the most important Bell inequality, written as [24]:

$$S = \left| \sum_{x_1, x_2 \in \{0,1\}} (-1)^{x_1 x_2} E(x_1, x_2) \right|,$$

and the correlators are given by [25]:

$$E(x_1, x_2) = \sum_{a_1, a_2, x_1, x_2} a_1.a_2 \, p(a_1, a_2 \mid x_1, x_2) \tag{2.17}$$

In presence of any local hidden variable (LHV) model, the CHSH inequality satisfies

$$|S| \leq 2 \tag{2.18}$$

This bound is called classical bound.

Quantum Violation:

Quantum mechanics predicts those correlations that violates this classical bound.

Assuming one party Alice and other party Bob shares maximally entangled state such as:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right), \tag{2.19}$$

with the right choice of measurement, one can achieve

$$|S| > 2. \tag{2.20}$$

This violation explains the non-local nature of [26] quantum mechanics stating that any hidden variable cannot be able to explain it.

2.5 The No Cloning Theorem

[21] According to the No Cloning theorem, creating an identical copies and independent copies [26] of any arbitrary unknown quantum state is not possible.

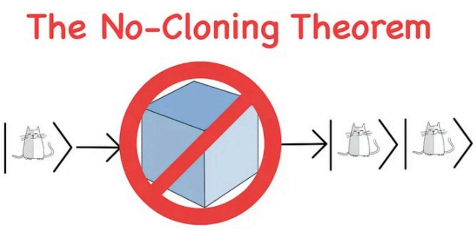

Figure 2.2: No cloning theorem (source:/Wikipedia)

Can there be any quantum operation U that copies the unknown quantum state $|\phi\rangle$.

$$U\,|\phi\rangle \otimes |0\rangle = |\phi\rangle \otimes |\phi\rangle? \tag{2.21}$$

Let's assume there is a cloning operator U and consider two arbitrary unknown quantum states α and ω such that:

$$\begin{aligned}
U\,|\alpha\rangle \otimes |0\rangle &= |\alpha\rangle \otimes |\alpha\rangle, && (2.22)\\
U\,|\omega\rangle \otimes |0\rangle &= |\omega\rangle \otimes |\omega\rangle, && (2.23)\\
\langle\alpha, 0|U^\dagger U|\omega, 0\rangle &= \langle\alpha, \alpha|\omega, \omega\rangle && (2.24)\\
&= \left(\langle\alpha|\omega\rangle\right)^2, && (2.25)\\
\Rightarrow \quad \langle\alpha|\omega\rangle\left(1 - \langle\alpha|\omega\rangle\right) &= 0, && (2.26)\\
\Rightarrow \quad \langle\alpha|\omega\rangle &= 0 \;\text{ or }\; 1. && (2.27)
\end{aligned}$$

So, α and ω are not the arbitrary states, either they are orthogonal or identical, which is contradiction to our assumption. Hence, there cannot be any cloning operator U.

2.6 Overview of Quantum Cryptography

2.6.1 Quantum Key Distribution

It is a [26] secure communication method based on laws of Quantum mechanics such as Quantum Entanglement, Quantum Measurement and the No-Cloning theorem. A random secret key is produced among the two parties and then the [26] produced key is used for encryption and decryption of the messages. This secure communication allows the two parties for [27] detecting the presence of an Eavesdropper who can tries to gain knowledge about the produced key.

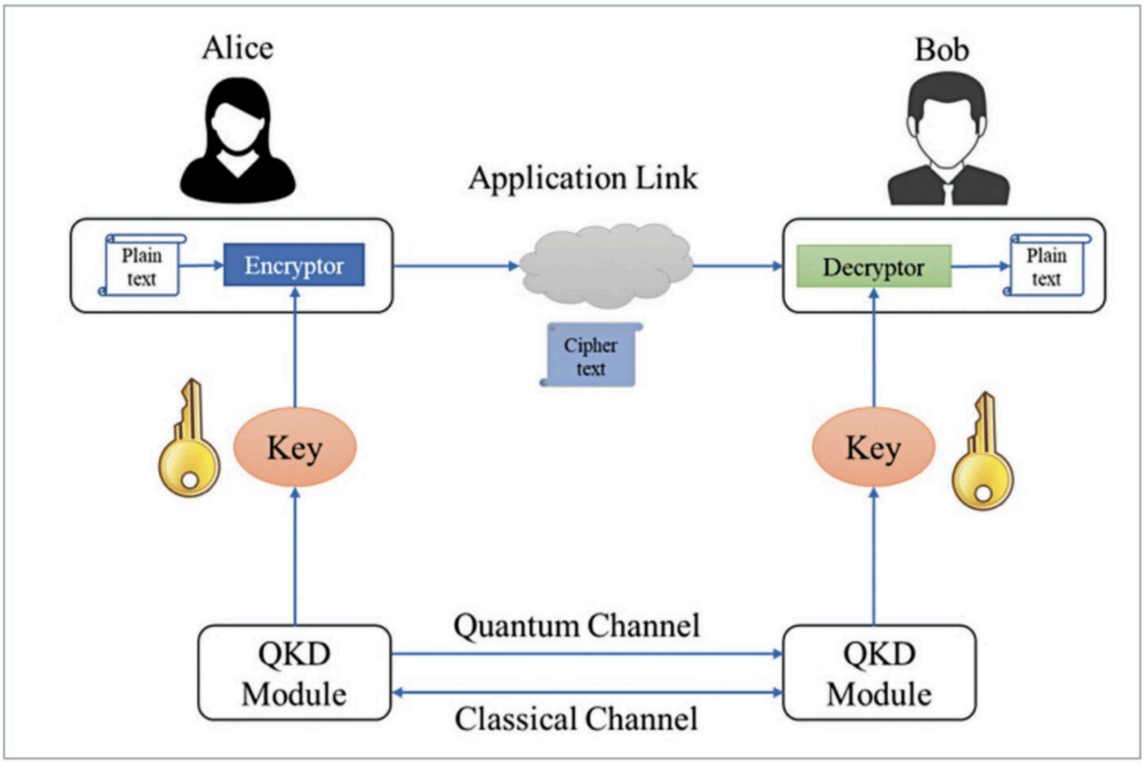

Figure 2.3: Basic QKD setup (source:/Wikipedia)

2.6.2 One Time Pad

One Time Pad, it is also known as single use of key, in which the randomly generated private key is used for encryption and decryption of a message. Both the transmitter and the receiver must have identical copies of the key before communication. For an unbreakable encryption method, the four conditions must be satisfied:

1. The secret key must be used only once.
2. It must be at least as lengthy as the message.
3. The key must be truly randomly.
4. Key must be secured between the sender and receiver.

Message	T				E				X				T			
Binary Words	1	0	0	1	1	1	0	0	0	1	0	1	1	0	0	1
Key (Randomly selected)	0	1	0	1	1	0	1	0	1	1	0	1	0	0	1	0
Encrypted Message	1	1	0	0	0	1	1	0	1	0	0	0	1	0	1	1
Key (same as above)	0	1	0	1	1	0	1	0	1	1	0	1	0	0	1	0
Binary Words	1	0	0	1	1	1	0	0	0	1	0	1	1	0	0	1
Decrypted message	T				E				X				T			

Figure 2.4: Example of encryption-decryption of message using Random Private key

2.6.3 BB84 Protocol

In the [10] BB84 protocol, the two parties, one party Alice and other party Bob, they generates a secret key by using the principle of the Quantum mechanics. In this protocol, [10] information is usually represented in the polarization state of a single photon using two polarization bases:

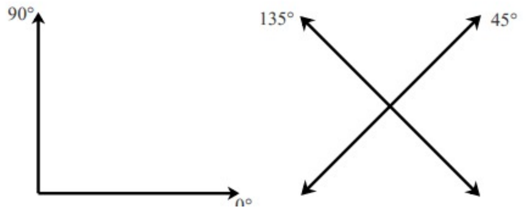

Figure 2.5: Photon polarization states in BB84 protocol [5]

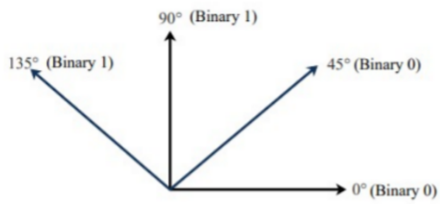

Figure 2.6: Bits encoding in BB84 protocol [5]

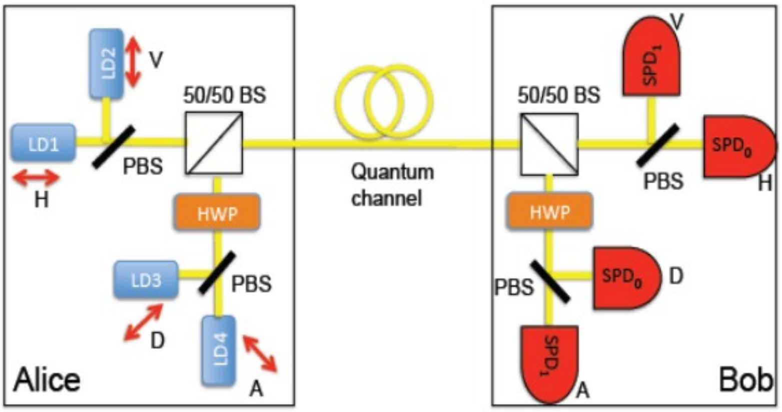

Figure 2.7: Free Space BB84 QKD setup(source:/Wikipedia)

Steps of the protocol preparation (Performed by Alice):

- Alice chooses randomly a bit either 0 or 1 and a basis either rectilinear or diagonal.

- She then generates a photon in the corresponding polarization state: Bit 0 $\rightarrow$ 0° (H) or 45° Bit 1 $\rightarrow$ 90° (V) or 135°

Transmission of photons

- Alice transmits the series of polarized photons to Bob with the help of a quantum channel.

Measurement (Performed by Bob):

- Bob also selects randomly measurement basis (that can be rectilinear or diagonal) for each photon received and documents his measurement result. The resulting sequence is referred to as the sifted key.

Basis Comparison (Public Channel):

- Both the parties publicly discuss the bases they each used (not the bit values). They retain only that instances when their bases coincide and discard the others.

Security and error Checking

- From the subset of the sifted key, they discard say $n/4$ key-bits for detecting the presence of eavesdropper and the remaining bits forms a key.

An example of BB84 protocol is shown below:

Alice's random bits	1	1	0	1	0	0	1	1	0	1	0	0
Alice's measuring bases	+	×	×	+	+	×	+	×	×	+	+	×
Photon polarization states	V	135°	45°	V	H	45°	V	135°	45°	V	H	45°
Bob's measuring bases	+	+	+	+	+	×	+	+	×	×	+	×
Bob's bits (Raw key)	1	0	0	1	0	0	1		0		0	0
Bob send his measuring bases to Alice	+	+	+	+	+	×	+		×		+	×
Alice confirm the measuring bases	T	F	F	T	T	T	T		T		T	T
Sifted key	1			1	0	0	1		0		0	0
Bob reveals some bits at random				1		0						
Alice confirm the bits				OK		OK						
Secret key	1				0		1		0		0	0

Figure 2.8: Example of BB84 protocol [5]

2.6.4 The Ekert 91 Protocol

This QKD protocol was setup by Artur Ekert in 1991 stated as follows:

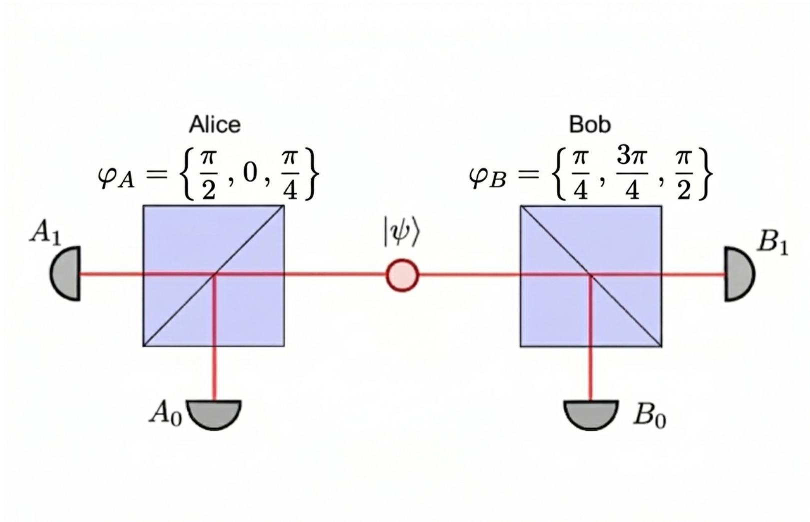

Figure 2.9: Setup of Ekert protocol, adapted from (source:/Wikipedia)

1. Here, two parties [28] one is Alice and other is Bob shares a singlet state $|\Psi\rangle$ through a Quantum channel.

2. Alice randomly selects a measurement setting as φ_A= $\frac{\pi}{2}$, 0, $\frac{\pi}{4}$, while Bob independently selects as φ_B $\frac{\pi}{4}$, $\frac{3\pi}{4}$, $\frac{\pi}{2}$.

3. Both of them randomly switch their measurement directions. After the measurement, they publicly compared the sequences of measurement settings and divided the data into two groups:

- **Public Group**: It consists of all measurements in which they choose different directions. It is used for checking the security of key.

- **Private Group**:It consists of all measurements where they choose the same directions. It is used to produce correlated key.

2.7 Literature Review

[32] Quantum Key Distribution protocols (BB84 protocol) are proven secure in theory, as their security [33] is based on the concepts of QM, that includes the disturbance caused by the measurement and the No-cloning theorem. But in real experiment, there may be some imperfections in the devices (detectors or the photon source) which deviates them from there ideal behavior. There can be **Side Channel attack**, the method in which an Eavesdropper exploits the real-world device imperfections to extract the information of the secret key without violating the Quantum theory.

Some common examples of side channel attacks in Quantum Key Distribution are: Photon Number Splitting (PNS) Attack (Brassard et al.)[29], Detector Blinding Attack (Lydersen et al.), Time Shift Attack (Qi et al.), Trojan Horse Attack (Gisin et al.). This highlights a significant gap between the theoretical security and the real-world implementations of QKD. To prevent this, Acín et al. and Pironio et al.proposed a counter measure as DI- QKD, ie., untrusting the Quantum devices and the security is based on the violation of specific Bell inequality. This leads to the concept of self-testing where certification of states and measurements is possible based on the correlations.

2.7.1 How DIQKD is different from usual QKD protocol?

The usual QKD protocol is different from the DIQKD Protocol as:

	Standard QKD Protocol	**Device-Independent QKD (DIQKD)**
Nature of device	In usual QKD, devices are trusted and they are well characterized.	In DIQKD, devices are untrusted and treated as black boxes.
Security basis	The security is assumed on the quantum devices.	The security basis is the Violation of the Bell inequality.
Hilbert space dimension	Fixed and known dimension [30] of Hilbert space.	Unknown dimension of the Hilbert space. [31]
Key Rate	The key rate is usually higher for shorter distances and decreases with increase in distance.	Even small loss can destroy the correlation. The key rate drops to zero more sharply.

Table 2.1: A comparison table for Standard QKD and Device-Independent QKD

Chapter 3

Methods

3.1 Self-testing in Device Independent Scenario

Self-testing is a method which is independent of any specific device and can identify the properties of a [1] physical device without knowing its internal structure or the [1] the Hilbert space dimension. The required information includes the count of measurement settings, the outputs for each measurement settings, and the statistics produced by those measurements.

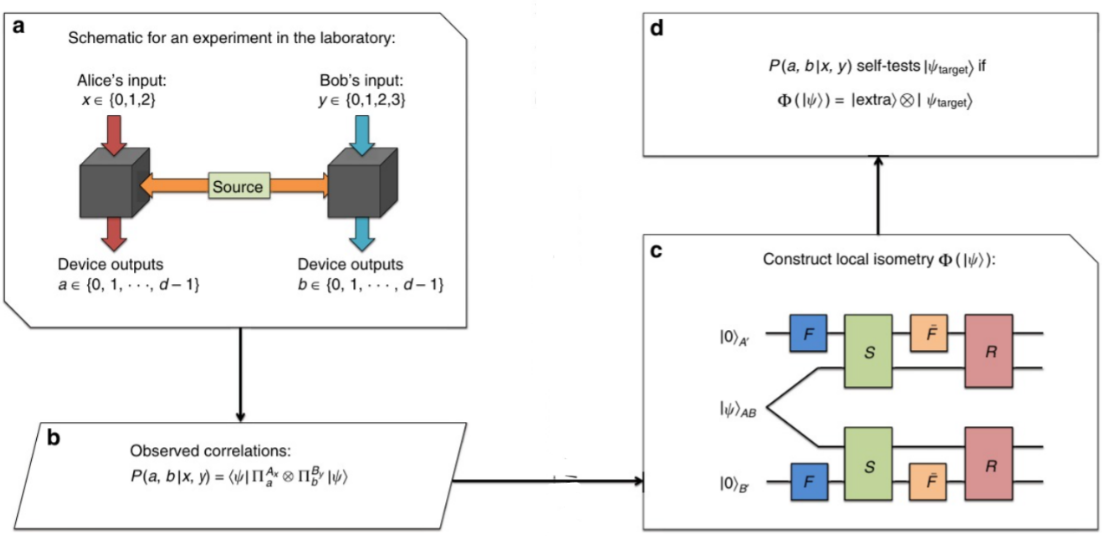

Figure 3.1: Self-testing scheme [6]

Here in the construction of the Isometry,

(i) F= It corresponds to a flip or measurement dependent Unitary. It behaves as a controlled operation based on measurement outcome.

(ii) F'= It is similar to F but based on different measurement outcome.

(iii) S= It acts as a swap operation between the unknown state and the extra ancillas.

(iv) R= It is a local correction unitary, which ensures that the extracted state matches well to the target state.

The two parties, one is Alice and other is Bob are unknown about the physical quantum state, measurement, dimension of the Hilbert space thus trying different settings for many times and collecting the statistics. From the statistics they can estimate the probabilities,

$$P(a_1 a_2|x_1 x_2) \tag{3.1}$$

which gives the probability of getting the result a_1 with input setting x_1 and result a_2 with input setting x_2 (it is also called correlation). They can get the probabilities even when they lack knowledge of the fundamental physics; experiments can be conducted on electrons, atoms, or any other system. Therefore, this situation is referred to as a device-independent scenario. From Born rule, there must exist a quantum state ρ, such that trρ =1.

$$p(a_1 a_2|x_1 x_2) = \mathrm{tr}\left(\rho\, M_{a_1|x_1} \otimes N_{a_2|x_2}\right) \tag{3.2}$$

Even with this knowledge, they are still able to conclude that the source emits an entangled states by exploiting Bell non-locality. Bell inequalities, a tool for detecting the Bell non-local correlations through their violation [8], can be written as:

$$I(p(a_1 a_2|x_1 x_2)) \leq \beta$$

This Bell inequality [8] are be violated by an entangled source. For some entangled source, we can have:

$$I(p(a_1 a_2|x_1 x_2)) > \beta.$$

If the violation occurs, then the source is entangled. So without even knowing about the experiment, they are able to conclude that the source is entangled. This is said to be device-independent certification of entanglement. However, self-testing goes beyond detecting entanglement. They hope to determine the state vector $|\psi'\rangle$ of the source.

3.1.1 Necessity of Bell inequalities in Self-testing

Classical theories are not able to explain the correlations that quantum mechanics predicts. The role of Bell inequalities in self-testing are better understood by geometry of set of a quantum and a classical correlations. A convex set, also known as local set, is formed by a set of correlations that are explained by some hidden variable theory. The convexity arises because any probabilistic combinations of the local strategies also remains a valid local strategy. The local set has the structure of a convex polytope which is referred as the local polytope. Bell inequalities defines the facets of this polytope and provides a complete set of linear constraints that all classical correlations must satisfy. Any observed correlation which lies outside this polytope necessarily violates at least one Bell inequality and are not explained by any local hidden variable model. Beyond this local polytope, there exist a set of quantum correlations that are not a polytope, they are convex set and has a curved boundary. All the correlations which are obtained by local measurement on the shared quantum state are included in this set.

As in self-testing, we only observe the probabilities $p(a_1a_2|x_1x_2)$. So, violation [32] of the Bell inequality allows to keep the correlations outside of the local polytope, ensuring that the correlations are produced by some quantum state.

Convex combination of Correlations:

A correlation is said to be a convex combination of correlations, if there exist two correlations G_1 and G_2, such that they can be written as:

$$G = \alpha G_1 + (1-\alpha)G_2, \tag{3.3}$$

given $0 \leq \alpha \leq 1$

3.1.2 Bell inequalities as a supporting hyperplane

A linear functional known as Bell inequality is represented by:

$$B[p] = \sum_{a_1a_2x_1x_2} c_{a_1a_2x_1x_2}\, p(a_1a_2|x_1x_2) \leq \beta_c, \tag{3.4}$$

Here the "Classical bound" is given by:

$$\beta_c = \max_{p\in\mathcal{L}} B[p] = \max_{\lambda\in\det} B[p_\lambda], \tag{3.5}$$

Here, $\mathcal{L}$ denotes the classical (local) set, $c_{a_1a_2x_1x_2}$ are the Bell coefficients, and p_λ represent deterministic strategies.

The quantum bound (Tsirelson bound) is given by:

$$\beta_q = \sup_{p\in\mathcal{Q}} B[p], \tag{3.6}$$

Q is the Quantum set. The behavior achieves a maximal violation of Bell inequality if:

$$B[p^*] = \beta_q \tag{3.7}$$

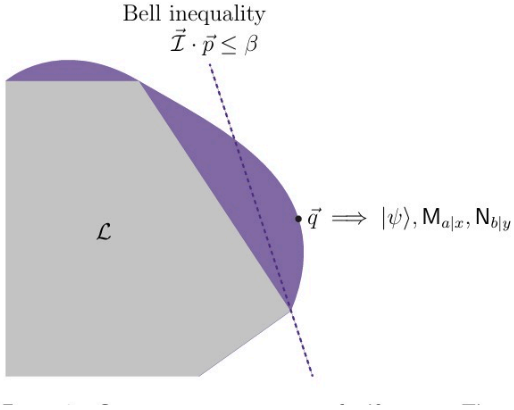

Figure 3.2: Geometric representation of self-testing [7]

3.1.3 Extremal Point Correlations

A correlation is extremal if it cannot be written as:

$$G' = \alpha G'_1 + (1 - \alpha) G'_2, \tag{3.8}$$

given $0 \leq \alpha \leq 1$ and $G'_1 \neq G'_2$.

It cannot be reproduced by mixing of any different quantum correlations. Extremal correlations corresponds to the pure state realisation.

Necessity of Extremal Correlations

If there exists $P*$ which self tests a pure state, then for the Quantum set Q [32], $P*$ must be an extremal point. For Self-testing of a quantum state, maximum Bell violation as well as extremal correlations are necessary. The extremal points of Q do not all corresponds to the [33] maximal Bell violation of same inequality.

Assume, the [33] correlations $p_\theta(a_1 a_2 x_1 x_2)$, obtained from a [33] maximally entangled state and projective measurements, form extremal points of the quantum set.

$$p_\theta(a_1 a_2 x_1 x_2) = \langle \phi^+ | \left(M_{a_1}^{x_1}(\theta) \otimes N_{a_2}^{x_2}(\theta) \right) | \phi^+ \rangle, \tag{3.9}$$

with some rotated measurements.

The CHSH value is:

$$\beta_{\text{CHSH}}(\theta) = 2\sqrt{2}\, \sin(2\theta) + 2\cos(2\theta) \tag{3.10}$$

At $\theta = \frac{\pi}{4}$,

$$\beta_{\text{CHSH}} = 2\sqrt{2}, \tag{3.11}$$

But for each p_θ at $\theta \neq \frac{\pi}{4}$, is still extremal but it does not maximally violates the CHSH inequality. This implies maximal Bell violation selects a unique extremal point.

3.2 Isometry

In Device independent scenario, in actual experiment Alice and Bob didn't assume that the state shared among them is pure. The state is given as: $\rho_{ab} = \mathrm{Tr}_E\,[\,|\psi\rangle\langle\psi|\,]$, where the self-testing does not use the environment. Tracing out the environment by using $|\psi\rangle_{abE}$ is comparable to ρ_{ab}.

Assume we have to self-test a [33] pure state $|\psi\rangle'_{ab}$ and the [33] projective measurements $\{M'_{a_1|x_1},\, N'_{a_2|x_2}\}$ [33], call them the targeted state and the measurement operators. In the actual set up we have the physical state as ρ_{ab} and the measurements as $\{M_{a_1|x_1},\, N_{a_2|x_2}\}$. It is not possible to know the target state and measurements only from the correlation due to the following reasons:

1. The statistics which is obtained from a quantum state remain unaltered under local unitary transformations due to unitary invariance of the trace. In other sense, for some state $|\psi'\rangle$ and for measurements $\{M'_{a_1|x_1}\}$ and $\{N'_{a_2|x_2}\}$, one can also have the transformed state

   $$(U \otimes \hat{V})|\psi'\rangle$$

   along with the measurements

   $$\{\,UM'_{a_1|x_1}U^\dagger\,\}, \quad \{\,VN'_{a_2|x_2}V^\dagger\,\}$$

   where U and V are the unitary operators.

   These transformations leave all observable probabilities invariant. Also, the underlying state cannot be uniquely identified as $|\psi'\rangle$, since it can be equally of the form $(U \otimes V)|\psi'\rangle$.

2. To exclude [32] any extra degrees of freedom through which the measurement act trivially is not possible[32]. Considering an extended state of the form

   $$|\psi'\rangle \otimes |\omega\rangle\,,$$

   together with measurements

   $$\{\,M'_{a_1|x_1} \otimes \mathbb{I}\,\}, \quad \{\,N'_{a_2|x_2} \otimes \mathbb{I}\,\},$$

   where identity operator act on the ancillary system associated with $|\omega\rangle$. Such a construction produces the same observable correlations as those obtained from the state $|\psi'\rangle$ with measurements $\{M'_{a_1|x_1}\}$ and $\{N'_{a_2|x_2}\}$. Consequently, the observed statistics are not sensitive to the [34] presence of these additional degrees of freedom.

So, for identifying the state and measurement in device-independent scenario, one must account for the local unitaries and the extra degrees of freedom, by using the local isometry [32] . A linear transformation on the quantum states [32] is called a **Isometry** $\Phi : \mathcal{H}_{A_1} \to \mathcal{H}_{A_2}$ that maintain inner product. It can expand the dimension of space when thought of as a unitary operator.

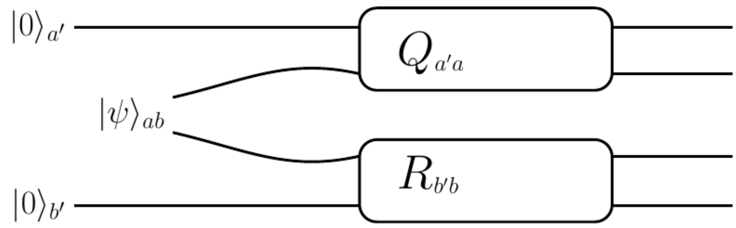

Figure 3.3: Local Isometry, adapted from [7]

From the above figure, it is written as:

$$\Phi_a \otimes \Phi_b\Big[\,|\psi\rangle_{ab}\Big] = Q_{a'a} \otimes R_{b'b}\Big[\,|00\rangle_{a'b'} \otimes |\psi\rangle_{ab}\Big]. \tag{3.12}$$

3.3 Self-testing of pure states

Any correlations $p(a_1a_2|x_1x_2)$ are considered to self-verify a state $|\psi'\rangle_{a'b'}$, given that for any state ρ_{ab} that aligns to the $p(a_1a_2|x_1x_2)$, there is existence a local isometry

$$\Phi_a \otimes \Phi_b : H_a \otimes H_b \to H_{a'} \otimes H_{b'} \otimes |\omega\rangle \tag{3.13}$$

So that,

$$(\Phi_a \otimes \Phi_b \otimes I_E)\,[|\psi\rangle_{abE}] = |\psi'\rangle_{a'b'} \otimes |\omega\rangle_{\bar{a}\bar{b}E}, \tag{3.14}$$

for a certain state $|\omega\rangle_{\bar{a}\bar{b}E}$.

3.4 Self-testing of Measurements

The correlations denoted by $P(a_1a_2|x_1x_2)$ are said to demonstrate the [35] state and measurements $|\psi'\rangle_{a'b'}$, $\{M'_{a_1|x_1}\}$, and $\{N'_{a_2|x_2}\}$ if this condition is satisfied: for a given state ρ_{ab} and for measurements $\{M_{a_1|x_1}\}$, $\{N_{a_2|x_2}\}$ that are consistent to the probability $P(a_1a_2|x_1x_2)$, and for some purification $|\psi\rangle_{abE}$ of ρ_{ab}, there exist local isometries $\Phi_a \otimes \Phi_b$ that fulfill the following equation:

$$(\Phi_a \otimes \Phi_b \otimes \mathbb{I}_E)\left[\left(M_{a_1|x_1} \otimes N_{a_2|x_2} \otimes \mathbb{I}_E\right)|\psi\rangle_{abE}\right] = \left(M'_{a_1|x_1} \otimes N'_{a_2|x_2}\right)|\psi'\rangle_{a'b'} \otimes |\omega\rangle_{\bar{a}\bar{b}E}, \tag{3.15}$$

for every combination of $a_1a_2x_1x_2$, and for an auxiliary state $|\xi\rangle_{\bar{a}\bar{b}E}$.

3.4.1 Can Mixed state be self-tested in DI setting?

Mixed state cannot be self-tested in a standard device-independent scenario, because any correlation $p(a_1a_2|x_1x_2)$ produced by a [32] mixed state also be produced by some pure state of the equivalent dimension[32]. However, by expanding it to the Network Scenario where independent sources are assumed, mixed state can be self-tested.

To Prove: Any correlations $p(a_1a_2|x_1x_2)$ that are produced by any Mixed states also can be produced by some pure state.

Let's assume a bell state:

$$\left|\phi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

In computational basis:

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$$

Assuming Alice and Bob performs measurement in σ_z and σ_x basis respectively.

Projective measurements in X and Z basis

Projectors in X basis

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

$$P_{x+} = |+\rangle\langle+| = \frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}$$

$$P_{x-} = |-\rangle \langle -| = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

Projectors in Z basis

$$P_{z+} = |0\rangle \langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad P_{z-} = |1\rangle \langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Case I. When Alice and Bob [36] chooses Z+ and X+ basis:

$$p(a_1, a_2|x_1, x_2) = \left\langle \phi^+ \right| \left(M_{a_1}^{(x_1)} \otimes N_{a_2}^{(x_2)} \right) \left| \phi^+ \right\rangle$$

$$p(+, +|z, x) = \left\langle \phi^+ \right| (P_{z+} \otimes P_{x+}) \left| \phi^+ \right\rangle$$

$$(P_{z+} \otimes P_{x+}) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$(P_{z+} \otimes P_{x+}) \left| \phi^+ \right\rangle = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$p(+, +|z, x) = \left\langle \phi^+ \right| (P_{z+} \otimes P_{x+}) \left| \phi^+ \right\rangle = \frac{1}{4}$$

Case II. When Alice and Bob chooses Z+ and X- basis [36]:

$$p(+, -|z, x) = \left\langle \phi^+ \right| (P_{z+} \otimes P_{x-}) \left| \phi^+ \right\rangle = \frac{1}{4} \tag{3.16}$$

Case III. When Alice and Bob chooses Z- and X+ basis [36]:

$$p(-, +|z, x) = \left\langle \phi^+ \right| (P_{z-} \otimes P_{x+}) \left| \phi^+ \right\rangle = \frac{1}{4} \tag{3.17}$$

Case IV. When Alice and Bob chooses Z- and X- basis [36]:

$$p(-, -|z, x) = \left\langle \phi^+ \right| (P_{z-} \otimes P_{x-}) \left| \phi^+ \right\rangle = \frac{1}{4} \tag{3.18}$$

ie.,

$$p(+, +|z, x) = p(-, -|z, x) = p(+, -|z, x) = p(-, +|z, x) = \frac{1}{4}$$

Lets assume a mixed state:

$$\rho_A = \frac{1}{2}\left|0\right\rangle\left\langle 0\right| + \frac{1}{2}\left|1\right\rangle\left\langle 1\right|$$

$$\rho_B = \frac{1}{2}\left|0\right\rangle\left\langle 0\right| + \frac{1}{2}\left|1\right\rangle\left\langle 1\right|$$

In computational basis,

$$\rho_A = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \frac{I}{2}$$

$$\text{Similarly, } \rho_B = \frac{I}{2}$$

$$\rho_{AB} = \rho_A \otimes \rho_B = \frac{I}{2} \otimes \frac{I}{2} = \frac{I}{4}$$

$$\rho_{AB} = \frac{1}{4}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$$

Assuming Alice and Bob performs measurement in σ_z and σ_z basis respectively:
Projectors in Z basis

$$P_{z+} = \left|0\right\rangle\left\langle 0\right| = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \quad P_{z-} = \left|1\right\rangle\left\langle 1\right| = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$$

$$p(a_1 a_2|x_1 x_2) = \operatorname{tr}\left(\rho_{ab}\, M_{a_1|x_1} \otimes N_{a_2|x_2}\right) \tag{3.19}$$

After all measurement settings, we get results as:

$$p(+,+|z,z) = p(-,-|z,z) = p(+,-|z,z) = p(-,+|z,z) = \frac{1}{4}$$

We have shown that the correlations produced by mixed states can also be reproduced by pure state of same dimension.

Detailed derivation is given in Appendix A.2.

3.5 Robust self-testing

For proving the self-testing statement from the experimental data, one can encounter the following problems:

(i) All the experiments includes a degree of noise which reduces the correlation, but it can be validated through Robust self-testing.

(ii) Because of the finite size of sample, the exact value of $p(a_1 a_2|x_1 x_2)$ will be unpredictable.

3.5.1 Robust self-testing of states

The correlations $p(a_1 a_2|x_1 x_2)$ tests a state $|\psi'\rangle_{a'b'}$ through self-testing with a distance of δ in vector norm $\|\cdot\|$, [37] there is an existence of a local isometry $\Phi = \Phi_a \otimes \Phi_b$:

$$\left\|\Phi \otimes \mathbb{I}_E \left(|\psi\rangle_{abE}\right) - |\psi'\rangle_{a'b'} \otimes |\omega\rangle \, \bar{a}\bar{b}E\right\| \leq \delta \tag{3.20}$$

3.6 SOS Decomposition

For each Bell inequality that are structured as $\sum_{a_1 a_2 x_1 x_2} c_{a_1 a_2 x_1 x_2}\, p(a_1 a_2|x_1 x_2)$, one can associate a corresponding Bell operator

$$\mathcal{B} = \sum_{a_1 a_2 x_1 x_2} c_{a_1 a_2 x_1 x_2}\, M_{a_1|x_1} \otimes N_{a_2|x_2}. \tag{3.21}$$

The violation of such Bell inequality given by $\beta = \mathrm{tr}(\rho\,\mathcal{B})$. Shifted Bell operator can be described as:

$$\beta_Q \mathbb{I} - \mathcal{B}.$$

where β_Q is the maximum quantum violation. This shifted operator is positive semi-definite. [38] That is, for any state $|\psi\rangle$,

$$\langle\psi|\left(\beta_Q \mathbb{I} - \mathcal{B}\right)|\psi\rangle \geq 0. \tag{3.22}$$

Assuming the shifted operator can be written as

$$\beta_Q \mathbb{I} - \mathcal{B} = \sum_{\lambda} P_\alpha^\dagger P_\alpha,$$

where each P_α is a polynomial in the measurement operators $\{M_{a_1|x_1}\}$ and $\{N_{a_2|x_2}\}$.

This is known as the (SOS) decomposition of the shifted Bell operator.

These SOS decompositions are very powerful because they allows to extract important information about the quantum state $|\psi\rangle$ and the measurement operators which achieves the maximal violation.

From the decomposition, if the maximal violation is achieved, then

$$\langle\psi|\left(\beta_Q \mathbb{I} - \mathcal{B}\right)|\psi\rangle = 0.$$

This implies

$$\sum_{\alpha} \|P_\alpha|\psi\rangle\|^2 = 0,$$

and hence

$$P_\alpha|\psi\rangle = 0 \quad \text{for all } \alpha.$$

Since each P_α depends on the measurement operators that achieves the maximal violation, these conditions impose a strong constraints on the underlying quantum realization.

If one observes a non-maximal violation $\beta_Q - \varepsilon$, the approximate relation is of the form

$$\|P_\alpha|\psi\rangle\| \leq O(\sqrt{\varepsilon}) \quad \text{for all } \alpha. \tag{3.23}$$

Chapter 4

Results and Discussion

4.1 Limitations of self-testing with Compatible Measurements

A set of POVMs [39] is a set of positive semi-definite operators $M'_{a'|x}$, here x is defined as the choice of input and a' is defined as the output [40]. It follows:

$$M'_{a'|x} \geq 0 \quad \forall\, a', x, \qquad \sum_{a'} M'_{a'|x} = \mathbb{I} \quad \forall\, x \tag{4.1}$$

(i) A set of POVMs $M'_{a'|x}$ is compatible or is jointly measurable when expressed as:

$$M'_{a'|x} = \sum_k p(a'|x,k)\, G_k, \quad \forall\, a', x \tag{4.2}$$

where G_k is called mother POVM and follows:

$$G_k \geq 0 \quad \forall\, k, \qquad \sum_k G_k = \mathbb{I} \tag{4.3}$$

The functions $p(a'|x,k)$ represents the conditional distribution of probability ie.,

$$p(a'|x,k) \geq 0, \qquad \sum_{a'} p(a'|x,k) = 1 \quad \forall\, x, k. \tag{4.4}$$

A set of measurements is said to be incompatible if it is not jointly measurable(JM).

(ii) A behaviour $\{p(a'_1 \dots a'_N \mid x_1 \dots x_N)\}$ is called N-partite Bell local if it can be decomposed as:

$$p(a'_1 \dots a'_N \mid x_1 \dots x_N) = \sum_k p(k) \prod_{n=1}^{N} p_n(a'_n \mid x_n, k), \tag{4.5}$$

where $\{p(k)\}$ is the probability distribution and $p_n(a'_n \mid x_n, k)$ are conditional distribution of probability for each party n.

4.1.1 Is it possible to self-test the Quantum realizations which involves compatible measurement on a single party of the multipartite system?

Let us assume N parties, namely $A, B, C, D, \ldots$. Denote party A as Alice, that performs measurements $\{M'_{a'|x}\}$, and the rest as $R = (B, C, D, \ldots)$, that perform measurements $\{E_{r|y}\}$. Assuming one party Alice which performs a compatible measurement:

$$M'_{a'|x} = \sum_k p(a'|x,k)\, G_k, \quad \forall\, a', x \tag{4.6}$$

where G_k is called mother POVM represented as $G_k = |k\rangle\langle k|$.

Proof 1. Assume the state shared among the parties is an Entangled state ρ. The probabilty distribution:

$$p(a', r|x, y) = \mathrm{Tr}\left(\rho_{AR}\, M'_{a'|x} \otimes E_{r|y}\right) \tag{4.7}$$

$$p(a', r|x, y) = \mathrm{Tr}_{AR}\left[\rho_{AR}\left(\sum_k p_A(a'|x,k)\, |k\rangle\langle k|\right) \otimes E_{r|y}\right] \tag{4.8}$$

Let,

$$\mathcal{T} = \mathrm{Tr}_{AR}\left[\rho_{AR}\, |k\rangle\langle k| \otimes E_{r|y}\right]$$

$$\mathcal{T} = \mathrm{Tr}_{R}\left[\mathrm{Tr}_A\Big(\rho_{AR}|k\rangle\langle k| \otimes I_R\Big)\, E_{r|y}\right]$$

Defining

$$\tilde{\sigma}_R^k = \mathrm{Tr}_A\Big(\rho_{AR}|k\rangle\langle k| \otimes I_R\Big)$$

To normalize,

$$\sigma_R^k = \frac{\tilde{\sigma}_R^k}{p_k}$$

$$\mathcal{T} = \mathrm{Tr}_R\left(\tilde{\sigma}_R^k\, E_{r|y}\right)$$

Thus,

$$p(a'r|xy) = \sum_k p_A(a'|x,k)\, \mathcal{T})$$

$$p(a'r|xy) = \sum_k p_A(a'|x,k)\, \mathrm{Tr}_R\Big(\tilde{\sigma}_R^k \otimes E_{r|y}\Big) \tag{4.9}$$

$$p(a'r|xy) = \sum_k p_k p_A(a'|x,k)\,\mathrm{Tr}_R\Big(\sigma_R^k \otimes E_{r|y}\Big) \tag{4.10}$$

Proof 2. Assuming the state shared among them is ρ_{sep}:

$$\rho = \sum_j p_j\,|j\rangle\langle j| \otimes \sigma_R^j$$

Alice performs compatible measurement on her system as:

$$\sum_{a'} M'_{a'|x} = \sum_k p_A(a'|x,k) G_k = \sum_k p_A(a'|x,k)|k\rangle\langle k|$$

The probability distribution written as:

$$p'(a'r|xy) = \mathrm{Tr}\Big[\rho(M'_{a'|x} \otimes E_{r|y})\Big]$$

$$p'(a'r|xy) = \mathrm{Tr}\left[\left(\sum_j p_j|j\rangle\langle j| \otimes \sigma_R^j\right)\left(\sum_k p_A(a'|x,k)|k\rangle\langle k| \otimes E_{r|y}\right)\right]$$

$$p'(a'r|xy) = \mathrm{Tr}\left[\sum_{j,k} p_j p_A(a'|x,k)|j\rangle\langle j|\,|k\rangle\langle k| \otimes (\sigma_R^j \otimes E_{r|y})\right]$$

Using orthonormality condition of δ_{jk}

$$p'(a'r|xy) = \sum_k p_k p_A(a'|x,k)\,\mathrm{Tr}_R\Big(\sigma_R^k E_{r|y}\Big)$$

$$p'(a'r|xy) = p(a'r|xy)$$

From the Proof 1 and Proof 2, we have shown that the correlations produced when an Entangled state is shared among the N parties is similar to the correlations produced when the state shared is a separable state. In self-testing, we guarantee about the underlying state and measurement from the observed correlations. Hence, it is not possible to self-test the Quantum realizations which involves compatible measurement on a single party of the multipartite system.

4.2 Measurement Incompatibility as a necessary but not sufficient condition for Self-testing

To show that self-testing requires incompatible measurements but the same is not sufficient, we assume the two parties which are named as Alice and Bob shares a singlet state and possess incompatible measurement operators:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \tag{4.11}$$

Assuming Alice's measurement operators are:

$$\begin{aligned} A_0 &= Z \\ A_1 &= X \end{aligned} \tag{4.12}$$

Bob's measurement operators are [41]:

$$\begin{aligned} B_0 &= \cos(\xi')\,Z + \sin(\xi')\,X \\ B_1 &= \cos(\xi')\,Z - \sin(\xi')\,X \end{aligned} \tag{4.13}$$

Computing the CHSH value:

$$\langle \mathcal{B}_{\text{CHSH}} \rangle = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \tag{4.14}$$

$$(i)\ \langle A_0 B_0 \rangle = -\cos(\xi') \qquad (ii)\ \langle A_0 B_1 \rangle = -\cos(\xi') \tag{4.15}$$

$$(iii)\ \langle A_1 B_0 \rangle = -\sin(\xi') \qquad (iv)\ \langle A_1 B_1 \rangle = -\sin(\xi') \tag{4.16}$$

Detailed derivation is given in Appendix A.1.
So, $\langle \mathcal{B}_{\text{CHSH}} \rangle = |\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle|$

$$\langle \mathcal{B}_{\text{CHSH}} \rangle = |-\cos(\xi') - \cos(\xi') - \sin(\xi') - \sin(\xi')| \tag{4.17}$$

$$\langle \mathcal{B}_{\text{CHSH}} \rangle = |-2\cos(\xi') - 2\sin(\xi')| \tag{4.18}$$

$$\langle \mathcal{B}_{\text{CHSH}} \rangle = \ (2\cos(\xi') + 2\sin(\xi'))$$

$$\langle \mathcal{B}_{\text{CHSH}} \rangle = 2\cos(\xi') + 2\sin(\xi')$$

[28] On substituting $\xi' = \frac{2\pi}{3}$,

$$\cos\left(\frac{2\pi}{3}\right) = -\frac{1}{2}, \quad \sin\left(\frac{2\pi}{3}\right) = \frac{\sqrt{3}}{2}$$

$$\langle \mathcal{B}_{\text{CHSH}} \rangle = 2\left(-\frac{1}{2}\right) + 2\left(\frac{\sqrt{3}}{2}\right)$$

$$= -1 + \sqrt{3}$$

$$\therefore \quad \langle \mathcal{B}_{\text{CHSH}} \rangle = \sqrt{3} - 1$$

Hence, we observe that CHSH value is less than 2 implies there is no Bell violation. Since, self-testing relies on the violation of Bell inequality. So, this measurement setting does not allows for self-testing. This proves that incompatible measurements are necessary but they are not sufficient.

4.3 Self-testing of a single party in DI scenario

Self-testing of a single party in DI scenario is a difficult task because the statistics $P(a|x)$ can be produced by any classical device. For a single party we can write: $P(a \mid x) = \text{Tr}(M_{a|x}\, \rho)$, where ρ is the state and $(M_{a|x})$ is the measurement operator.

(i) To show the statistics can be produced by any classical device
Assume any classical device which has a probability distribution $\{p_a\}$ in memory. For a given input setting x, the device gives an output a with probability $P(a \mid x)$, which implies:

$$P(a \mid x) = \sum_k p(k)\, D(a \mid x, k)$$

where k is some classical random variable and $D(a \mid x, k) \in \{0, 1\}$ is a deterministic function.

Thus, any statistics $P(a \mid x)$ that are produced by a quantum device can also be reproduced by a classical device.

(ii) Different Quantum states can produce the same correlation
Assume $\rho_1 = |\psi\rangle\langle\psi|$ and $\rho_2 = |\phi\rangle\langle\phi|$.

- When we have $(\rho_1, \{M_a^x\})$, the correlation we get,

$$\text{Tr}(M_a^x\, \rho_1) = P(a \mid x) \quad \forall\, a, x. \tag{4.19}$$

- For $(\rho_2, \{N_a^x\})$, the correlation we get,

$$\text{Tr}(N_a^x\, \rho_2) = P(a \mid x) \quad \forall\, a, x. \tag{4.20}$$

We concluded that both the states gives the same statistics with different measurement settings. Thus, from the statistics $P(a|x)$ alone, we cannot certify the state uniquely.

So, for self-testing of a single party we need to move from Device-independent Scenario to a Semi-device Independent Scenario, where we make some assumption about dimension.

4.4 Self-testing of Entangled two-qubit state

To show [42] that the target state is:

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Suppose a state $|\Psi'\rangle$ and measurement operators $M_{a_1|x_1}$, $N_{a_2|x_2}$ are shared among the two parties Alice and Bob, which are known as the physical state and physical measurement. They are unknown about dimension of the state and treated the devices as a black boxes. Alice's input setting is x_1= (0,1) with outcome a_1= (+1,-1) and Bob's input setting is x_2= (0,1) with outcome a_2= (+1,-1).

$$A'_{x_1} = M_{+|x_1} - M_{-|x_1},\ B'_{x_2} = N_{+|x_2} - N_{-|x_2}, \tag{4.21}$$

where $M_{a_1|x_1}$, $N_{a_2|x_2}$ are the physical measurement operators, they are projective. The operators A'_{x_1} and B'_{x_2} are Hermitian and Unitary.

$${A'}^{\dagger}_{x_1} = {A'}_{x_1}, \quad {A'}^{2}_{x_1} = 1, \quad {B'}^{\dagger}_{x_2} = {B'}_{x_2}, \quad {B'}^{2}_{x_2} = 1 \tag{4.22}$$

Step 1: To show that $\{A'_0, A'_1\}\,|\psi'\rangle = 0$ and $\{B'_0, B'_1\}\,|\psi'\rangle = 0$

To show this, we assume SOS decomposition:

$$2\sqrt{2} - B_{\text{CHSH}} = \frac{1}{\sqrt{2}}\left[\left(\frac{A'_0 + A'_1}{\sqrt{2}} - B'_0\right)^2 + \left(\frac{A'_0 - A'_1}{\sqrt{2}} - B'_1\right)^2\right] \tag{4.23}$$

For some state $|\psi'\rangle$ that leads to $B_{\text{CHSH}} = 2\sqrt{2}$, we get

$$\frac{A'_0 \pm A'_1}{\sqrt{2}}\,|\psi'\rangle = B'_{0/1}\,|\psi'\rangle \tag{4.24}$$

Lets assume the vectors as :

$$a'_0 = \frac{A'_0 + A'_1}{\sqrt{2}} |\psi'\rangle \qquad\qquad a'_0 = B'_0 |\psi'\rangle \tag{4.25}$$

$$a'_1 = \frac{A'_0 - A'_1}{\sqrt{2}} |\psi'\rangle \qquad\qquad a'_1 = B'_1 |\psi'\rangle \tag{4.26}$$

The Cauchy- Schwarz inequality says:

$$|a'_i|\, |b'_i| \geq 1 \quad \text{for } i = 0, 1, \tag{4.27}$$

where $|a'_i| = \sqrt{a'_i \cdot {a'_i}^{\dagger}}$ and vectors b_0 an b_1 has unit norms. This inequality saturates so the vectors a'_i and b'_i are parallel ie., $a'_i = b'_i$.

$$\begin{aligned}
\{B'_0, B'_1\}|\psi'\rangle &= (B'_0 B'_1 + B'_1 B'_0)|\psi'\rangle \\
&= \frac{(A'_0 - A'_1)B'_0 + (A'_0 + A'_1)B'_1}{\sqrt{2}} |\psi'\rangle \\
&= \frac{(A'_0 - A'_1)(A'_0 + A'_1) + (A'_0 + A'_1)(A'_0 - A'_1)}{2} |\psi'\rangle \\
&= \frac{2A'^2_0 - 2A'^2_1}{2} |\psi'\rangle \\
&= 0,
\end{aligned} \tag{25}$$

which shows that B'_0 and B'_1 anti commute on support of state $|\Psi'\rangle$.
Similarly, for observables A'_0 and A'_1. $\{A'_0, A'_1\} |\psi'\rangle = 0$ (as $a'_i \parallel b'_i$).
Hence, we deduce the results $\{A'_0, A'_1\} |\psi'\rangle = 0$ **and** $\{B'_0, B'_1\} |\psi'\rangle = 0$**.**

Step 2: Isometry- Swap gate

Isometry is required to make equivalence of the physical state $|\Psi'\rangle_{ab}$ to the targeted state $|\Phi^+\rangle$. When the physical state [3] is represented as a two-qubit state and the operators are defined as $Z_a = \sigma^z_a$, $X_a = \sigma^x_a$, $Z_b = \sigma^z_b$, and $X_b = \sigma^x_b$, the purpose of the circuit is to swap the state $|\Psi'\rangle_{ab}$ with the $|00\rangle$ state of registers a and b. By choosing,

$$Z_a = \frac{1}{\sqrt{2}}(A'_0 + A'_1), \quad X_a = \frac{1}{\sqrt{2}}(A'_0 - A'_1), \quad Z_b = B'_0, \quad X_b = B'_1.$$

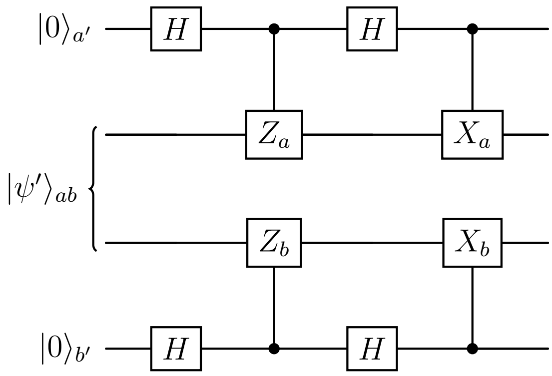

Figure 4.1: Partial Swap gate Isometry, adapted from [7]

From here we can conclude,

$$\{Z_b, X_b\}|\psi'\rangle_{ab} = 0$$

From eq.(4.22),

$$Z_a|\psi'\rangle_{ab} = Z_b|\psi'\rangle_{ab}, \tag{4.28}$$
$$X_a|\psi'\rangle_{ab} = X_b|\psi'\rangle_{ab}. \tag{4.29}$$

Solving the Swap gate Isometry

(i) $|0\rangle_{a'}\,|\psi'\rangle_{ab}\,|0\rangle_{b'}$
(ii) Action of Hadamard on $|0\rangle_{a'}|0\rangle_{b'}$:

$$(H\,|0\rangle_{a'} \otimes H\,|0\rangle_{b'})\,|\psi'\rangle_{ab} = \frac{1}{2}\left(|00\rangle_{a'b'} + |01\rangle_{a'b'} + |10\rangle_{a'b'} + |11\rangle_{a'b'}\right)|\psi'\rangle_{ab} \tag{4.30}$$
$$= \frac{1}{2}\Big(\,|00\rangle_{a'b'}\,|\psi'\rangle_{ab} + |01\rangle_{a'b'}\,|\psi'\rangle_{ab} + |10\rangle_{a'b'}\,|\psi'\rangle_{ab} + |11\rangle_{a'b'}\,|\psi'\rangle_{ab}\Big) \tag{4.31}$$

(iii) Action of Z_a and Z_b

$$= \frac{1}{2}\Big[\,|00\rangle\;(I_a \otimes I_b)\,|\psi'\rangle_{ab} + |01\rangle\;(I_a \otimes Z_b)\,|\psi'\rangle_{ab} + |10\rangle\;(Z_a \otimes I_b)\,|\psi'\rangle_{ab} + |11\rangle\;(Z_a \otimes Z_b)\,|\psi'\rangle_{ab}\Big] \tag{4.32}$$

(iv) Action of Hadamard gate A.3

$$\begin{aligned}
&= \frac{1}{4}\Big[\, |00\rangle\,(I+Z_a)(I+Z_b)\,|\psi'\rangle_{ab} \\
&\quad + |01\rangle\,(I+Z_a)(I-Z_b)\,|\psi'\rangle_{ab} \\
&\quad + |10\rangle\,(I-Z_a)(I+Z_b)\,|\psi'\rangle_{ab} \\
&\quad + |11\rangle\,(I-Z_a)(I-Z_b)\,|\psi'\rangle_{ab}\Big]
\end{aligned} \tag{4.33}$$

(v) Action of X_a and X_b

$$\begin{aligned}
&= \frac{1}{4}\Big[\, |00\rangle\,(I+Z_a)(I+Z_b)\,|\psi'\rangle_{ab} \\
&\quad + |01\rangle\,(I+Z_a)\,X_b\,(I-Z_b)\,|\psi'\rangle_{ab} \\
&\quad + |10\rangle\,(I-Z_a)\,X_a\,(I+Z_b)\,|\psi'\rangle_{ab} \\
&\quad + |11\rangle\ X_a(I-Z_a)\,X_b(I-Z_b)\,|\psi'\rangle_{ab}\Big]
\end{aligned} \tag{4.34}$$

By solving it, we get

$$\Phi[|\psi'\rangle] = \frac{1}{4}\Big[2\,|00\rangle\,(1+Z_a)\,|\psi'\rangle_{ab} + 2\,|01\rangle\,(1+Z_a)X_a\,|\psi'\rangle_{ab}\Big] \tag{4.35}$$

$$= \frac{1}{4}\Big[2\,|00\rangle\,(1+Z_a)\,|\psi'\rangle_{ab} + 2\,|11\rangle\,(1+Z_a)\,|\psi'\rangle_{ab}\Big] \tag{4.36}$$

$$= \frac{1}{4}\cdot 2\Big[\,|00\rangle + |11\rangle\,\Big](1+Z_a)\,|\psi'\rangle_{ab} \tag{4.37}$$

$$= \frac{1}{2}(|00\rangle + |11\rangle)(1+Z_a)\,|\psi'\rangle_{ab} \tag{4.38}$$

Now writing in normalized Bell form:

$$\Phi[|\psi'\rangle] = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{1+Z_a}{\sqrt{2}}\right)|\psi'\rangle_{ab} \tag{4.39}$$

$$\Phi[|\psi'\rangle_{abE}] = |\Phi^+_{ab}\rangle \otimes |\omega\rangle_{abE} \tag{4.40}$$

Similarly for self-testing of measurement,

First term:

$$|00\rangle\,(I+Z_a)(I+Z_b)B_0'\,|\psi'\rangle_{ab} = |00\rangle\,(I+Z_a)(I+Z_b)\,|\psi'\rangle_{ab}\,.$$

Second term:

$$|01\rangle\,(I+Z_a)X_b(I-Z_b)B_0'\,|\psi'\rangle_{ab} = -\,|01\rangle\,(I+Z_a)X_b(I-Z_b)\,|\psi'\rangle_{ab}\,.$$

The remaining terms vanish: 0.

Combining all these terms, we obtain

$$|00\rangle\,(I+Z_a)(I+Z_b)\,|\psi'\rangle_{ab} - |01\rangle\,(I+Z_a)(I-Z_b)\,|\psi'\rangle_{ab} = (I+Z_a)\Big(|00\rangle - |11\rangle\Big)\otimes|\omega\rangle_{abE}\,. \tag{4.41}$$

So, the action of isometry on B_0' gives

$$\Phi(B_0'|\psi'\rangle) = \mathbb{I}\otimes\sigma_z\,|\phi^+\rangle\otimes|\omega\rangle. \tag{4.42}$$

Action of Φ	
$\Phi(\|\psi'\rangle)$	$\|\phi^+\rangle\otimes\|\omega\rangle$
$\Phi(A_0'\,\|\psi'\rangle)$	$\left(\frac{\sigma_x+\sigma_z}{\sqrt{2}}\otimes\mathbb{I}\right)\|\phi^+\rangle\otimes\|\omega\rangle$
$\Phi(A_1'\,\|\psi'\rangle)$	$\left(\frac{-\sigma_x+\sigma_z}{\sqrt{2}}\otimes\mathbb{I}\right)\|\phi^+\rangle\otimes\|\omega\rangle$
$\Phi(B_0'\,\|\psi'\rangle)$	$(\mathbb{I}\otimes\sigma_z)\,\|\phi^+\rangle\otimes\|\omega\rangle$
$\Phi(B_1'\,\|\psi'\rangle)$	$(\mathbb{I}\otimes\sigma_x)\,\|\phi^+\rangle\otimes\|\omega\rangle$

Table 4.1: Action of isometry Φ on state $|\psi'\rangle$ and measurement operators.

Detailed Derivation is shown in Appendix A.3 The robust self-testing:

$$\langle\psi'|(A_0'B_0' + A_0'B_1' + A_1'B_0' - A_1'B_1')|\psi'\rangle \geq 2\sqrt{2}-\omega,$$

4.5 Self-testing of three qubit W state

To prove that the target state is:

$$|W\rangle = \frac{1}{\sqrt{3}}\,(|001\rangle + |010\rangle + |100\rangle)$$

[43]

Step 1: To find the correlations that self-tests the state W

Projectors P^0 and P^1 are:

$$P^0 = |0\rangle\langle 0| \quad \text{and} \quad P^1 = |1\rangle\langle 1|.$$

A state $|\Psi'\rangle$ is shared among the three parties who are named as Alice, Bob and Charlie. For each parties $M_0^i = Z_i$, $M_1^i = X_i$ and $M_2^i = D_i = \frac{1}{\sqrt{2}}(X_i + Z_i)$.

The following correlations can self-test W_3 state:

$$\langle\psi'|P_a^0 P_b^0 P_c^1|\psi'\rangle = \langle\psi'|P_a^1 P_b^0 P_c^0|\psi'\rangle = \frac{1}{3} \tag{4.43}$$

$$\langle\psi'|P_a^0 X_b X_c|\psi'\rangle = \langle\psi'|P_b^0 X_a X_c|\psi'\rangle = \frac{2}{3} \tag{4.44}$$

$$\langle\psi'|P_a^0 Z_b Z_c|\psi'\rangle = \langle\psi'|P_b^0 Z_a Z_c|\psi'\rangle = -\frac{2}{3} \tag{4.45}$$

$$\langle\psi'|P_a^0 X_b D_c|\psi'\rangle = \langle\psi'|P_b^0 X_a D_c|\psi'\rangle = -\frac{1}{\sqrt{2}\cdot 3} \tag{4.46}$$

$$\langle\psi'|P_a^0 Z_b D_c|\psi'\rangle = \langle\psi'|P_b^0 Z_a D_c|\psi'\rangle = -\frac{1}{\sqrt{2}\cdot 3} \tag{4.47}$$

$$\langle\psi'|P_a^0 X_b Z_c|\psi'\rangle = 0 \tag{4.48}$$

$$\langle\Psi'|P_0^a P_0^b P_1^c|\Psi'\rangle + \langle\Psi'|P_0^a P_1^b P_0^c|\Psi'\rangle + \langle\Psi'|P_1^a P_0^b P_0^c|\Psi'\rangle = 1 \tag{4.49}$$

and the rest are zero.

Step 2: Isometry- Swap gate

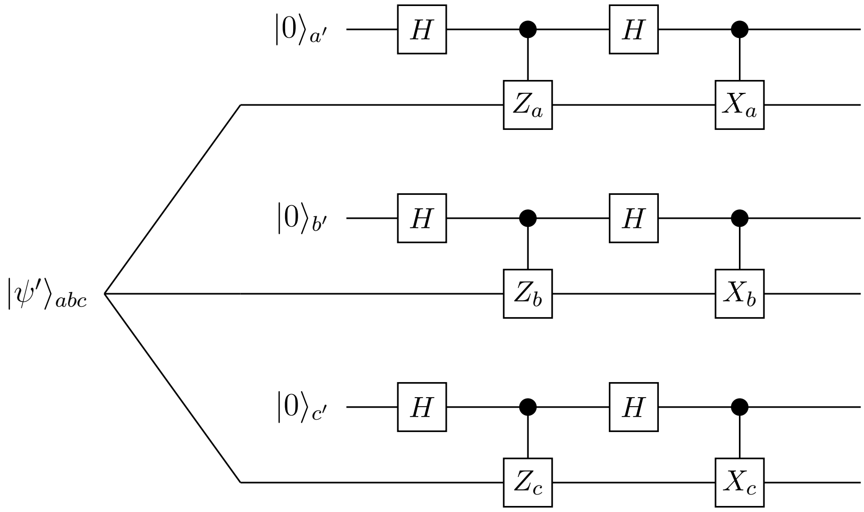

Figure 4.2: Swap gate isometry for W_3 state, adapted from [1]

Step 3: Solving the Isometry

(i) $|0\rangle_{a'} |\psi'\rangle_{abc} |0\rangle_{b'} |0\rangle_{c'}$

(ii) Action of First Hadamard on $|0\rangle_{a'}|0\rangle_{b'}|0\rangle_{c'}$:

$$\begin{aligned}(H\,|0\rangle_{a'} \otimes H\,|0\rangle_{b'} \otimes H\,|0\rangle_{c'})\,|\psi'\rangle = \frac{1}{2\sqrt{2}}\Big(&|000\rangle_{a'b'c'} + |001\rangle_{a'b'c'} + |010\rangle_{a'b'c'} + |011\rangle_{a'b'c'} \\ &+ |100\rangle_{a'b'c'} + |101\rangle_{a'b'c'} + |110\rangle_{a'b'c'} + |111\rangle_{a'b'c'}\Big)\,|\psi'\rangle\end{aligned} \tag{4.50}$$

$$\begin{aligned}= \frac{1}{2\sqrt{2}}\Big(&|000\rangle_{a'b'c'}\,|\psi'\rangle + |001\rangle_{a'b'c'}\,|\psi'\rangle \\ &+ |010\rangle_{a'b'c'}\,|\psi'\rangle + |011\rangle_{a'b'c'}\,|\psi'\rangle \\ &+ |100\rangle_{a'b'c'}\,|\psi'\rangle + |101\rangle_{a'b'c'}\,|\psi'\rangle \\ &+ |110\rangle_{a'b'c'}\,|\psi'\rangle + |111\rangle_{a'b'c'}\,|\psi'\rangle\Big)\end{aligned} \tag{4.51}$$

(iii) Action of control Z

$$\begin{aligned}= \frac{1}{2\sqrt{2}}\Big[&|000\rangle\,(I_a \otimes I_b \otimes I_c)\,|\psi'\rangle + |001\rangle\,(I_a \otimes I_b \otimes Z_c)\,|\psi'\rangle \\ &+ |010\rangle\,(I_a \otimes Z_b \otimes I_c)\,|\psi'\rangle + |011\rangle\,(I_a \otimes Z_b \otimes Z_c)\,|\psi'\rangle \\ &+ |100\rangle\,(Z_a \otimes I_b \otimes I_c)\,|\psi'\rangle + |101\rangle\,(Z_a \otimes I_b \otimes Z_c)\,|\psi'\rangle \\ &+ |110\rangle\,(Z_a \otimes Z_b \otimes I_c)\,|\psi'\rangle + |111\rangle\,(Z_a \otimes Z_b \otimes Z_c)\,|\psi'\rangle\Big]\end{aligned} \tag{4.52}$$

(iv) Action of Second Hadamard A.4

$$
\begin{aligned}
&= \frac{1}{8}\Big[|000\rangle\,(I_a+Z_a)(I_b+Z_b)(I_c+Z_c)\,|\psi'\rangle && (4.53)\\
&\quad +|001\rangle\,(I_a+Z_a)(I_b+Z_b)(I_c-Z_c)\,|\psi'\rangle && (4.54)\\
&\quad +|010\rangle\,(I_a+Z_a)(I_b-Z_b)(I_c+Z_c)\,|\psi'\rangle && (4.55)\\
&\quad +|011\rangle\,(I_a+Z_a)(I_b-Z_b)(I_c-Z_c)\,|\psi'\rangle && (4.56)\\
&\quad +|100\rangle\,(I_a-Z_a)(I_b+Z_b)(I_c+Z_c)\,|\psi'\rangle && (4.57)\\
&\quad +|101\rangle\,(I_a-Z_a)(I_b+Z_b)(I_c-Z_c)\,|\psi'\rangle && (4.58)\\
&\quad +|110\rangle\,(I_a-Z_a)(I_b-Z_b)(I_c+Z_c)\,|\psi'\rangle && (4.59)\\
&\quad +|111\rangle\,(I_a-Z_a)(I_b-Z_b)(I_c-Z_c)\,|\psi'\rangle\Big] && (4.60)
\end{aligned}
$$

Detailed derivation in shown in A.4

(v) Action of Control X A.4

$$
\begin{aligned}
=\;& |000\rangle\;P_a^0P_b^0P_c^0\,|\psi'\rangle + |001\rangle\;P_a^0P_b^0X_cP_c^1\,|\psi'\rangle\\
&+|010\rangle\;P_a^0X_bP_b^1P_c^0\,|\psi'\rangle + |011\rangle\;P_a^0X_bP_b^1X_cP_c^1\,|\psi'\rangle\\
&+|100\rangle\;X_aP_a^1P_b^0P_c^0\,|\psi'\rangle + |101\rangle\;X_aP_a^1P_b^0X_cP_c^1\,|\psi'\rangle\\
&+|110\rangle\;X_aP_a^1X_bP_b^1P_c^0\,|\psi'\rangle + |111\rangle\;X_aP_a^1X_bP_b^1X_cP_c^1\,|\psi'\rangle \qquad (4.61)
\end{aligned}
$$

Solving it further we get, A.4

$$
\begin{aligned}
|\Phi_{\text{out}}\rangle =\;& |001\rangle\;(P_a^0P_b^0P_c^0X_c)\,|\psi'\rangle\\
&+|010\rangle\;(P_a^0P_b^0P_c^0X_b)\,|\psi'\rangle\\
&+|100\rangle\;(P_a^0P_b^0P_c^0X_a)\,|\psi'\rangle \qquad (4.62)
\end{aligned}
$$

$$
\Phi\big(|\psi'\rangle\big) = \left(\frac{|001\rangle+|010\rangle+|100\rangle}{\sqrt{3}}\right)\otimes\Big(\sqrt{3}\,P_a^0P_b^0P_c^0\,X_c\,|\psi'\rangle\Big)
$$

$$
\Phi\,|\psi'\rangle = W_3\otimes|\omega\rangle
$$

However, when there is some presence of noise or some imperfections:

$$
\left|\langle\psi'\mid P_A^0P_B^0P_C^1\mid\psi'\rangle-\frac{1}{3}\right|\le\epsilon_0, \qquad (4.63)
$$

$$
\left|\langle\psi'\mid P_A^0P_B^1P_C^0\mid\psi'\rangle-\frac{1}{3}\right|\le\epsilon_0, \qquad (4.64)
$$

$$
\left|\langle\psi'\mid P_A^1P_B^0P_C^0\mid\psi'\rangle-\frac{1}{3}\right|\le\epsilon_0, \qquad (4.65)
$$

where ϵ_0 is referred as "small deviation".

The robust self-testing of W_3 state is:

$$\| \, |\psi'\rangle - |\omega\rangle_{abc} \otimes |W_3\rangle_{a'b'c'} \| \leq f(\epsilon_0), \tag{4.66}$$

Chapter 5

Conclusion and Future Work

In this thesis, we presented the detailed discussion of self-testing of the two-qubit state and the self-testing of three qubit state using the Partial Swap gate Isometry. We have shown that the self-testing of a pure quantum state is achievable by using the observed correlations. We have shown what are the necessary conditions for self-testing and gave argument for the same. However, in the device-independent scenario the correlations produced by mixed states are equivalent to the correlations produced by pure states, but one can achieve the self-testing for mixed states in a Device-independent Network scenario.

When one trying to do self-testing of single party in Device-Independent scenario, it seems a difficult task because the statistics $P(a|x)$ that is used for self-testing the target state $|\Psi'\rangle$ can be produced by any classical device. To do self-testing of single party, we needs to move from Device-Independent scenario to a Semi-device Independent Scenario where one can make assumption about the dimension. However, it is possible by Self-testing through a Prepare and Measure Scenario [44] which can be achieved by using $2 \rightarrow 1$ RAC or by using Self-testing through contextuality [45].

Bibliography

[1] X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, Physical Review A **90**, 042339 (2014).

[2] X. Li, Y. Miao, W. Zhou, X. Yu, W. Song, Y. Wei, F. Gao, X. Gao, Y.-X. Gong, and S.-N. Zhu, Science China Physics, Mechanics & Astronomy **68**, 290312 (2025).

[3] G. Chen, W.-H. Zhang, P. Yin, C.-F. Li, and G.-C. Guo, Fundamental Research **1**, 27 (2021).

[4] P. Young, An undergraduate course on quantum computing (2024), pHYS 150 / CSE 109 Lecture Notes.

[5] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, IEEE Open Journal of the Communications Society , 1 (2021), survey article.

[6] A. Coladangelo, K. T. Goh, and V. Scarani, Nature Communications **8**, 15485 (2017).

[7] I. Šupić and J. Bowles, Quantum **4**, 337 (2020).

[8] D. D. Georgiev, *Quantum Information and Consciousness: A Gentle Introduction* (CRC Press, Boca Raton, 2017).

[9] F. Neukart, *Reverse Engineering the Mind: Consciously Acting Machines and Accelerated Evolution* (Springer Vieweg, Wiesbaden, 2016).

[10] R. Wolf, *Quantum Key Distribution: An Introduction with Exercises*, Lecture Notes in Physics (Springer, Cham, 2021).

[11] J. Audretsch, *Entangled Systems: New Directions in Quantum Physics* (Wiley-VCH, Weinheim, 2007).

[12] T. Mori, Journal of Physics A: Mathematical and Theoretical **52**, 054001 (2019).

[13] M. G. Knepley, Class notes for cse 410, `https://cse.buffalo.edu/~knepley/classes/cse410/ClassNotes.pdf` (Unknown), accessed: 2026.

[14] A. Name, *Title of the Thesis*, Phd thesis, Freie Universität Berlin (Year).

[15] C. G. Timpson, *Quantum Information Theory and the Foundations of Quantum Mechanics*, Oxford Philosophical Monographs (Oxford University Press, Oxford, 2013).

[16] Unknown, Quantum mechanics, `https://www.slideshare.net/slideshow/linked-in-slides-quantum-mechanics/20743221` (2013), slideShare presentation, accessed 2026.

[17] J. A. Bergou and M. Hillery, *Introduction to the Theory of Quantum Information Processing*, Graduate Texts in Physics (Springer, New York, 2013).

[18] T. J. Kelly, European Journal of Physics **36**, 055041 (2015).

[19] A. Name, Title of the manuscript, `https://www.preprints.org/manuscript/f001d57034a2bcf20d6a6a33fbc42f60` (2024), preprint, not peer-reviewed.

[20] h.r.eskandari.1, Quantum computing explained, `https://fliphtml5.com/zhfid/nwzs` (2022), flipHTML5 online publication.

[21] D. Bruß and G. Leuchs, eds., *Quantum Information: From Foundations to Quantum Technology Applications* (Wiley-VCH, Weinheim, 2016).

[22] Y. Aharonov and D. Rohrlich, *Quantum Paradoxes: Quantum Theory for the Perplexed* (Wiley-VCH, Weinheim, 2008).

[23] R. Paul, S. Sasmal, and A. K. Pan, Physical Review A **110**, 012444 (2024).

[24] A. Name, arXiv preprint arXiv:2006.14883 (2020).

[25] A. Name, in *Book Title*, edited by E. Name (IntechOpen, Year) Chap. 56667.

[26] S. Sharma and A. Sharma, eds., *From Bits to Qubits: The Quantum Transformation of Computing*, Studies in Big Data (Springer, Cham, 2026).

[27] X. Wang, J. Ma, *et al.*, Security and Communication Networks **2017**, 1 (2017).

[28] C. P. Williams, *Explorations in Quantum Computing*, 2nd ed., Texts in Computer Science (Springer, London, 2011).

[29] Symmetry **18**, 153 (2026).

[30] M. McKague, *Quantum Information Processing with Adversarial Devices*, Ph.D. thesis, University of Waterloo (2010).

[31] V. Scarani, The device-independent outlook on quantum physics, in *Quantum Information Processing* (World Scientific, 2006) pp. 1–14.

[32] S. Ghorai, S. Banerjee, and D. Sarddar, e-Prime - Advances in Electrical Engineering, Electronics and Energy **1**, 100004 (2021).

[33] I. Supić, *Device-Independent Certification of Quantum Resources*, Ph.D. thesis, Universitat Politècnica de Catalunya (2018).

[34] J. Kaniewski, Physical Review Research **2**, 033420 (2020).

[35] A. K. Pan, Phys. Rev. A **104**, 10.1103/PhysRevA.104.022212 (2021).

[36] H.-L. Yin and Y. Fu, Scientific Reports **9**, 3045 (2019).

[37] X. Li, Y. Wang, Y. Han, F. Gao, and Q. Wen, arXiv:1907.06397 [quant-ph] (2019).

[38] B. Zygelman, *A First Introduction to Quantum Computing and Information*, 2nd ed. (Springer, Cham, 2024).

[39] M. Plávala, O. Gühne, and M. T. Quintino, arXiv:2403.10564 [quant-ph] (2024).

[40] S. Gupta, A. G. Maity, D. Das, A. Roy, and A. S. Majumdar, Phys. Rev. A **103**, 10.1103/PhysRevA.103.022421 (2021).

[41] D. McMahon, *Quantum Computing Explained* (Wiley, Chichester, UK, 2008).

[42] X. Valcarce, J. Zivy, N. Sangouard, and P. Sekatski, Phys. Rev. Research **4**, 10.1103/PhysRevResearch.4.013049 (2022).

[43] X. Li, Y. Wang, Y. Han, and S.-N. Zhu, Phys. Rev. A **106**, 10.1103/PhysRevA.106.052418 (2022).

[44] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Physical Review A **98**, 062307 (2018).

[45] K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L.-C. Kwek, Physical Review Letters **122**, 250403 (2019).

[46] S. Sarkar, A. C. O. Jr., and R. Augusiak, Nature Physics 10.1038/s41567-026-03181-y (2026).

[47] J. Preskill, Lecture notes for physics 229: Quantum information and computation (1998), available at: `https://www.lorentz.leidenuniv.nl/quantumcomputers/literature/preskill_1_to_6.pdf`.

[48] <Author1>, <Author2>, <Author3>, *et al.*, Physical Review Letters **134**, 200201 (2025).

[49] F. Hirsch, M. T. Quintino, and N. Brunner, Physical Review A **97**, 012129 (2018).

[50] A. Fine, Physical Review Letters **48**, 291 (1982).

[51] C. Jebarathinam, J.-C. Hung, S.-L. Chen, and Y.-C. Liang, Physical Review Research **1**, 033073 (2019).

[52] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. (Cambridge University Press, 2010).

[53] G. L. Oppo, S. M. Barnett, E. Riis, and M. Wilkinson, eds., *Quantum Dynamics of Simple Systems* (CRC Press / Taylor & Francis, 1997).

[54] S. Sharma and A. Sharma, eds., *From Bits to Qubits: The Quantum Transformation of Computing*, Studies in Big Data (Springer Cham, 2026).

[55] I. Šupić, D. Cavalcanti, and J. Bowles, Quantum **5**, 418 (2021), arXiv:1909.12759 [quant-ph] .

[56] D. Mayers and A. Yao, arXiv preprint (2003), quant-ph/0307205 .

[57] A. Preumont, *Twelve Lectures on Structural Dynamics*, Solid Mechanics and Its Applications, Vol. 198 (Springer, 2014).

[58] A. Name, *Title of the Thesis*, Ph.D. thesis, University of California, Berkeley (Year).

[59] J. Audretsch, *Entangled Systems: New Directions in Quantum Physics* (Wiley-VCH, Weinheim, 2007).

[60] A. Name, Physica Scripta 10.1088/1402-4896/ad7ade (2024).

[61] P. Sharma, V. Bhatia, and S. Prakash, IET Quantum Communication **5**, 164 (2024).

[62] D. D. Georgiev, *Quantum Information and Consciousness: A Gentle Introduction* (CRC Press, Taylor & Francis Group, Boca Raton, 2017).

[7]

Appendix A

Additional Derivations

A.1 Detailed derivation for calculating the CHSH value

The known identity for the singlet state:

$$\langle \sigma_i \otimes \sigma_j \rangle = -\delta_{ij}$$

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{A.1}$$

$$A_0 = Z, \quad A_1 = X$$

$$B_0 = \cos(\xi')Z + \sin(\xi')X, \quad B_1 = \cos(\xi')Z - \sin(\xi')X$$

Computing:

1. $\langle A_0 B_0 \rangle$

$$\langle A_0 B_0 \rangle = \langle \psi | A_0 B_0 | \psi \rangle$$

$$\langle A_0 B_0 \rangle = \langle \psi | \left(Z \otimes (\cos \xi' \, Z + \sin \xi' \, X) \right) | \psi \rangle \tag{A.2}$$

$$\langle A_0 B_0 \rangle = \cos \xi' \, \langle \psi | (Z \otimes Z) | \psi \rangle + \sin \xi' \, \langle \psi | (Z \otimes X) | \psi \rangle \tag{A.3}$$

$$(Z \otimes Z) \, |\psi\rangle = \frac{-|01\rangle + |10\rangle}{\sqrt{2}}, \quad (Z \otimes X) \, |\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

we get:

$$\langle A_0B_0\rangle = \left\langle \psi \middle| \left(-\cos\xi' \frac{|01\rangle - |10\rangle}{\sqrt{2}} + \sin\xi' \frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) \right\rangle$$

$$\langle A_0B_0\rangle = -\cos\xi' \tag{A.4}$$

2. $\langle A_0B_1\rangle$

$$\langle A_0B_1\rangle = \langle\psi|A_0B_0|\psi\rangle$$

$$\langle A_0B_1\rangle = \langle\psi|\left(Z\otimes(\cos\xi'\,Z - \sin\xi'\,X)\right)|\psi\rangle \tag{A.5}$$

$$\langle A_0B_1\rangle = \cos\xi'\,\langle\psi|(Z\otimes Z)|\psi\rangle - \sin\xi'\,\langle\psi|(Z\otimes X)|\psi\rangle \tag{A.6}$$

$$(Z\otimes Z)\,|\psi\rangle = \frac{-|01\rangle + |10\rangle}{\sqrt{2}}, \quad (Z\otimes X)\,|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

we get:

$$\langle A_0B_1\rangle = \left\langle \psi \middle| \left(-\cos\xi' \frac{|01\rangle - |10\rangle}{\sqrt{2}} - \sin\xi' \frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) \right\rangle$$

$$\langle A_0B_1\rangle = -\cos\xi' \tag{A.7}$$

3. $\langle A_1B_0\rangle$

$$\langle A_1B_0\rangle = \langle\psi|A_1B_0|\psi\rangle$$

$$\langle A_1B_0\rangle = \langle\psi|\left(X\otimes(\cos\xi'\,Z + \sin\xi'\,X)\right)|\psi\rangle \tag{A.8}$$

$$\langle A_1B_0\rangle = \cos\xi'\,\langle\psi|(X\otimes Z)|\psi\rangle + \sin\xi'\,\langle\psi|(X\otimes X)|\psi\rangle \tag{A.9}$$

we get:

$$\langle A_1B_0\rangle = \left\langle \psi \middle| \left(-\cos\xi' \frac{|11\rangle + |00\rangle}{\sqrt{2}} + \sin\xi' \frac{|10\rangle - |01\rangle}{\sqrt{2}} \right) \right\rangle$$

$$\langle A_1B_0\rangle = -\sin\xi' \tag{A.10}$$

4. $\langle A_1B_1\rangle$

$$\langle A_1 B_1 \rangle = \langle \psi | A_1 B_1 | \psi \rangle$$

$$\langle A_1 B_1 \rangle = \langle \psi | \left(X \otimes \left(\cos \xi' \, Z - \sin \xi' \, X \right) \right) | \psi \rangle \tag{A.11}$$

$$\langle A_1 B_1 \rangle = \cos \xi' \, \langle \psi | (X \otimes Z) | \psi \rangle - \sin \xi' \, \langle \psi | (X \otimes X) | \psi \rangle \tag{A.12}$$

we get:

$$\langle A_1 B_1 \rangle = \left\langle \psi \middle| \left(- \cos \xi' \frac{|11\rangle + |00\rangle}{\sqrt{2}} - \sin \xi' \frac{|10\rangle - |01\rangle}{\sqrt{2}} \right) \right\rangle$$

$$\langle A_1 B_1 \rangle = \sin \xi' \tag{A.13}$$

A.2 Detailed derivation of correlations produced by mixed state and pure state

When Alice and Bob assumes a pure state:

Case I. When Alice and Bob chooses Z+ and X+ basis:

$$p(a_1, a_2 | x_1, x_2) = \left\langle \phi^+ \right| \left(M_{a_1}^{(x_1)} \otimes N_{a_2}^{(x_2)} \right) \left| \phi^+ \right\rangle$$

$$p(+, + | z, x) = \left\langle \phi^+ \right| \left(P_{z+} \otimes P_{x+} \right) \left| \phi^+ \right\rangle$$

$$(P_{z+} \otimes P_{x+}) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$(P_{z+} \otimes P_{x+}) \left| \phi^+ \right\rangle = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$p(+, + | z, x) = \left\langle \phi^+ \right| \left(P_{z+} \otimes P_{x+} \right) \left| \phi^+ \right\rangle = \frac{1}{4}$$

Case II. When Alice and Bob chooses Z+ and X- basis:

$$p(a_1, a_2 | x_1, x_2) = \left\langle \phi^+ \right| \left(M_{a_1}^{(x_1)} \otimes N_{a_2}^{(x_2)} \right) \left| \phi^+ \right\rangle$$

$$p(+, - | z, x) = \left\langle \phi^+ \right| \left(P_{z+} \otimes P_{x-} \right) \left| \phi^+ \right\rangle$$

$$(P_{z+} \otimes P_{x-}) = \frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$(P_{z+} \otimes P_{x-})\left|\phi^+\right\rangle = \frac{1}{2\sqrt{2}}\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

$$p(+,-|z,x) = \left\langle\phi^+\right|(P_{z+} \otimes P_{x-})\left|\phi^+\right\rangle = \frac{1}{4}$$

Case III. When Alice and Bob chooses Z- and X+ basis:

$$p(-,+|z,x) = \left\langle\phi^+\right|(P_{z-} \otimes P_{x+})\left|\phi^+\right\rangle$$

$$(P_{z-} \otimes P_{x+}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$p(-,+|z,x) = \left\langle\phi^+\right|(P_{z-} \otimes P_{x+})\left|\phi^+\right\rangle = \frac{1}{4}$$

Case IV. When Alice and Bob chooses Z- and X- basis:

$$p(-,-|z,x) = \left\langle\phi^+\right|(P_{z-} \otimes P_{x-})\left|\phi^+\right\rangle$$

$$(P_{z-} \otimes P_{x-}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

$$p(-,-|z,x) = \left\langle\phi^+\right|(P_{z-} \otimes P_{x-})\left|\phi^+\right\rangle = \frac{1}{4}$$

Now, Assuming mixed state:

Case I: When Alice and Bob choose $Z+$ and $Z+$ basis

$$(P_{z+} \otimes P_{z-}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\rho_{ab}\left(P_{z+}\otimes P_{z+}\right)=\frac{1}{4}\begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$$

$$\mathrm{tr}(\rho_{ab}\left(P_{z+}\otimes P_{z+}\right))=\frac{1}{4}$$

Case II: When Alice and Bob choose $Z+$ and $Z-$ basis

$$\left(P_{z+}\otimes P_{z-}\right)=\begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$$

$$\rho_{ab}\left(P_{z+}\otimes P_{z-}\right)=\frac{1}{4}\begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$$

$$\mathrm{tr}(\rho_{ab}\left(P_{z+}\otimes P_{z-}\right))=\frac{1}{4}$$

Case III: When Alice and Bob choose $Z-$ and $Z+$ basis

$$\mathrm{tr}(\rho_{ab}\left(P_{z-}\otimes P_{z+}\right))=\frac{1}{4}$$

Case IV: When Alice and Bob choose $Z-$ and $Z-$ basis

$$\mathrm{tr}(\rho_{ab}\left(P_{z-}\otimes P_{z-}\right))=\frac{1}{4}$$

A.3 Detailed Derivations of Self-testing of two-qubit entangled state

Action of second Hadamard gate

$$
\begin{aligned}
= \frac{1}{2}\Big[& \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)(I_a \otimes I_b)\,|\psi'\rangle_{ab} \\
& + \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)(I_a \otimes Z_b)\,|\psi'\rangle_{ab} \\
& + \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)(Z_a \otimes I_b)\,|\psi'\rangle_{ab} \\
& + \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)(Z_a \otimes Z_b)\,|\psi'\rangle_{ab}\Big]
\end{aligned}
\tag{A.14}
$$

$$
\begin{aligned}
= \frac{1}{4}\Big[& |00\rangle\,(I + Z_a)(I + Z_b)\,|\psi'\rangle_{ab} \\
& + |01\rangle\,(I + Z_a)(I - Z_b)\,|\psi'\rangle_{ab} \\
& + |10\rangle\,(I - Z_a)(I + Z_b)\,|\psi'\rangle_{ab} \\
& + |11\rangle\,(I - Z_a)(I - Z_b)\,|\psi'\rangle_{ab}\Big]
\end{aligned}
\tag{A.15}
$$

Action of X_a and X_b

$$
\begin{aligned}
= \frac{1}{4}\Big[& |00\rangle\,(I + Z_a)(I + Z_b)\,|\psi'\rangle_{ab} \\
& + |01\rangle\,(I + Z_a)\,X_b\,(I - Z_b)\,|\psi'\rangle_{ab} \\
& + |10\rangle\,(I - Z_a)\,X_a\,(I + Z_b)\,|\psi'\rangle_{ab} \\
& + |11\rangle\;X_a(I - Z_a)\,X_b(I - Z_b)\,|\psi'\rangle_{ab}\Big]
\end{aligned}
\tag{A.16}
$$

Term 1:

$$|00\rangle\,(I + Z_a)(I + Z_b)\,|\psi'\rangle = |00\rangle\,(I^2 + Z_a^2 + 2Z_a)\,|\psi'\rangle \tag{A.17}$$

$$= |00\rangle\,(1 + 1 + 2Z_a)\,|\psi'\rangle \tag{A.18}$$

$$= |00\rangle\,(2 + 2Z_a)\,|\psi'\rangle \tag{A.19}$$

$$= 2\,|00\rangle\,(1 + Z_a)\,|\psi'\rangle \tag{A.20}$$

Term 2:

$$
\begin{aligned}
|01\rangle\,(I+Z_a)X_b(I-Z_b)\,|\psi'\rangle &= |01\rangle\,(I+Z_a)X_a(1-Z_a)\,|\psi'\rangle && \text{(A.21)}\\
&= |01\rangle\,(I+Z_a)(X_a-X_aZ_a)\,|\psi'\rangle && \text{(A.22)}\\
&= |01\rangle\,(I+Z_a)(X_a+Z_aX_a)\,|\psi'\rangle && \text{(A.23)}\\
&= |01\rangle\,(I+Z_a)X_a(1+Z_a)\,|\psi'\rangle && \text{(A.24)}\\
&= |01\rangle\,(I+Z_a)^2X_a\,|\psi'\rangle && \text{(A.25)}\\
&= |01\rangle\,(1+Z_a^2+2Z_a)X_a\,|\psi'\rangle && \text{(A.26)}\\
&= 2\,|01\rangle\,(1+Z_a)X_a\,|\psi'\rangle && \text{(A.27)}
\end{aligned}
$$

Term 3:

$$
\begin{aligned}
|10\rangle\,X_a(I-Z_a)(I+Z_b)\,|\psi'\rangle &= |10\rangle\,(X_a-X_aZ_a)(I+Z_b)\,|\psi'\rangle && \text{(A.28)}\\
&= |10\rangle\,X_a(I-Z_a)(I+Z_a)\,|\psi'\rangle && \text{(A.29)}\\
&= |10\rangle\,X_a(I-Z_a^2)\,|\psi'\rangle && \text{(A.30)}\\
&= |10\rangle\,X_a(1-1)\,|\psi'\rangle && \text{(A.31)}\\
&= 0 && \text{(A.32)}
\end{aligned}
$$

Term 4:

$$
\begin{aligned}
|11\rangle\,X_a(I-Z_a)X_b(I-Z_b)\,|\psi'\rangle &= |11\rangle\,(X_a-X_aZ_a)X_b(I-Z_b)\,|\psi'\rangle && \text{(A.33)}\\
&= |11\rangle\,X_a^2(I-Z_a)(I-Z_a)\,|\psi'\rangle && \text{(A.34)}\\
&= |11\rangle\,X_a^2(I-Z_a^2)\,|\psi'\rangle && \text{(A.35)}\\
&= |11\rangle\,X_a^2(1-1)\,|\psi'\rangle && \text{(A.36)}\\
&= 0 && \text{(A.37)}
\end{aligned}
$$

$$
\Phi[|\psi'\rangle_{abE}] = |\Phi^+_{ab}\rangle \otimes |\omega\rangle_{abE} \tag{A.38}
$$

A.4 Detailed Derivations of Self-testing of W state

Action of Second Hadamard

$$
\begin{aligned}
&= \frac{1}{2\sqrt{2}} \cdot \frac{1}{2\sqrt{2}} \Big[(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\,(I_a I_b I_c)\,|\psi'\rangle \\
&\quad + (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)\,(I_a I_b Z_c)\,|\psi'\rangle \\
&\quad + (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)\,(I_a Z_b I_c)\,|\psi'\rangle \\
&\quad + (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)\,(I_a Z_b Z_c)\,|\psi'\rangle \\
&\quad + (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\,(Z_a I_b I_c)\,|\psi'\rangle \\
&\quad + (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)\,(Z_a I_b Z_c)\,|\psi'\rangle \\
&\quad + (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)\,(Z_a Z_b I_c)\,|\psi'\rangle \\
&\quad + (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)\,(Z_a Z_b Z_c)\,|\psi'\rangle \Big]
\end{aligned} \tag{A.39}
$$

$$
\begin{aligned}
&\frac{1}{8} \Big[(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\,(I_a \otimes I_b \otimes I_c)\,|\psi'\rangle \\
&\quad + (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)\,(I_a \otimes I_b \otimes Z_c)\,|\psi'\rangle \\
&\quad + (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)\,(I_a \otimes Z_b \otimes I_c)\,|\psi'\rangle \\
&\quad + (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)\,(I_a \otimes Z_b \otimes Z_c)\,|\psi'\rangle \\
&\quad + (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\,(Z_a \otimes I_b \otimes I_c)\,|\psi'\rangle \\
&\quad + (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)\,(Z_a \otimes I_b \otimes Z_c)\,|\psi'\rangle \\
&\quad + (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)\,(Z_a \otimes Z_b \otimes I_c)\,|\psi'\rangle \\
&\quad + (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)\,(Z_a \otimes Z_b \otimes Z_c)\,|\psi'\rangle \Big]
\end{aligned} \tag{A.40}
$$

$$\frac{1}{8}\Big[\ (1+Z_a)(1+Z_b)(1+Z_c)\,|\psi'\rangle\ |000\rangle$$
$$+(1+Z_a)(1+Z_b)X_c(1-Z_c)\,|\psi'\rangle\ |001\rangle$$
$$+(1+Z_a)X_b(1-Z_b)(1+Z_c)\,|\psi'\rangle\ |010\rangle$$
$$+(1+Z_a)X_b(1-Z_b)X_c(1-Z_c)\,|\psi'\rangle\ |011\rangle$$
$$+X_a(1-Z_a)(1+Z_b)(1+Z_c)\,|\psi'\rangle\ |100\rangle$$
$$+X_a(1-Z_a)(1+Z_b)X_c(1-Z_c)\,|\psi'\rangle\ |101\rangle$$
$$+X_a(1-Z_a)X_b(1-Z_b)(1+Z_c)\,|\psi'\rangle\ |110\rangle$$
$$+X_a(1-Z_a)X_b(1-Z_b)X_c(1-Z_c)\,|\psi'\rangle\ |111\rangle\ \Big] \tag{A.41}$$

Action of control X

$$\frac{1}{8}\Big[\ (1+Z_a)(1+Z_b)(1+Z_c)\,|\psi'\rangle\ |000\rangle$$
$$+(1+Z_a)(1+Z_b)X_c(1-Z_c)\,|\psi'\rangle\ |001\rangle$$
$$+(1+Z_a)X_b(1-Z_b)(1+Z_c)\,|\psi'\rangle\ |010\rangle$$
$$+(1+Z_a)X_b(1-Z_b)X_c(1-Z_c)\,|\psi'\rangle\ |011\rangle$$
$$+X_a(1-Z_a)(1+Z_b)(1+Z_c)\,|\psi'\rangle\ |100\rangle$$
$$+X_a(1-Z_a)(1+Z_b)X_c(1-Z_c)\,|\psi'\rangle\ |101\rangle$$
$$+X_a(1-Z_a)X_b(1-Z_b)(1+Z_c)\,|\psi'\rangle\ |110\rangle$$
$$+X_a(1-Z_a)X_b(1-Z_b)X_c(1-Z_c)\,|\psi'\rangle\ |111\rangle\ \Big] \tag{A.42}$$

$$\begin{aligned} =\ & |000\rangle\ P_a^0P_b^0P_c^0\,|\psi'\rangle + |001\rangle\ P_a^0P_b^0X_cP_c^1\,|\psi'\rangle \\ & + |010\rangle\ P_a^0X_bP_b^1P_c^0\,|\psi'\rangle + |011\rangle\ P_a^0X_bP_b^1X_cP_c^1\,|\psi'\rangle \\ & + |100\rangle\ X_aP_a^1P_b^0P_c^0\,|\psi'\rangle + |101\rangle\ X_aP_a^1P_b^0X_cP_c^1\,|\psi'\rangle \\ & + |110\rangle\ X_aP_a^1X_bP_b^1P_c^0\,|\psi'\rangle + |111\rangle\ X_aP_a^1X_bP_b^1X_cP_c^1\,|\psi'\rangle \end{aligned} \tag{A.43}$$

Using the correlations we have,

$$(P_a^0P_b^0P_c^0)\,|\psi'\rangle = (P_a^0P_b^1P_c^1)\,|\psi'\rangle = (P_a^1P_b^0P_c^1)\,|\psi'\rangle = (P_a^1P_b^1P_c^0)\,|\psi'\rangle = (P_a^1P_b^1P_c^1)\,|\psi'\rangle = 0 \tag{A.44}$$

$$|\Phi_{\mathrm{out}}\rangle = |001\rangle\ (P_a^0P_b^0X_cP_c^1)\,|\psi'\rangle + |010\rangle\ (P_a^0X_bP_b^1P_c^0)\,|\psi'\rangle + |100\rangle\ (X_aP_a^1P_b^0P_c^0)\,|\psi'\rangle \tag{A.45}$$

Solving for these terms,

$$P^0 = \frac{I+Z}{2}, \qquad P^1 = \frac{I-Z}{2}$$

X and Z anti-commute:

$$XZ = -ZX$$

Thus it became,

$$\begin{aligned}
XP^1 &= X\left(\frac{I-Z}{2}\right) && \text{(A.46)}\\
&= \frac{1}{2}(X - XZ) && \text{(A.47)}\\
&= \frac{1}{2}(X + ZX) \quad (\text{since } XZ = -ZX) && \text{(A.48)}\\
&= \frac{1}{2}(I+Z)X && \text{(A.49)}\\
&= P^0 X && \text{(A.50)}
\end{aligned}$$

$$\boxed{XP^1 = P^0 X}$$

$$\begin{aligned}
\text{Term 1:} \quad & (P_a^0 P_b^0 X_c P_c^1)\,|\psi'\rangle = (P_a^0 P_b^0 P_c^0 X_c)\,|\psi'\rangle\\
\text{Term 2:} \quad & (P_a^0 X_b P_b^1 P_c^0)\,|\psi'\rangle = (P_a^0 P_b^0 P_c^0 X_b)\,|\psi'\rangle\\
\text{Term 3:} \quad & (X_a P_a^1 P_b^0 P_c^0)\,|\psi'\rangle = (P_a^0 P_b^0 P_c^0 X_a)\,|\psi'\rangle \qquad \text{(A.51)}
\end{aligned}$$

So, it became after some substitution:

$$\begin{aligned}
|\Phi_{\text{out}}\rangle = \; & |001\rangle\ (P_a^0 P_b^0 P_c^0 X_c)\,|\psi'\rangle\\
& + |010\rangle\ (P_a^0 P_b^0 P_c^0 X_b)\,|\psi'\rangle\\
& + |100\rangle\ (P_a^0 P_b^0 P_c^0 X_a)\,|\psi'\rangle \qquad \text{(A.52)}
\end{aligned}$$

$$(P_a^0 P_b^0 P_c^0 X_a)\,|\Psi'\rangle = (P_a^0 P_b^0 P_c^0 X_b)\,|\Psi'\rangle = (P_a^0 P_b^0 P_c^0 X_c)\,|\Psi'\rangle \qquad \text{(A.53)}$$

$$|\Phi_{\text{out}}\rangle = \; (|001\rangle + |010\rangle + |100\rangle)\,\left(P_a^0 P_b^0 P_c^0 X_c\right)|\psi'\rangle$$