UNIVERSITY OF BELGRADE

FACULTY OF PHYSICS

Aleksandra Dimić

# DETECTION OF QUANTUM CORRELATIONS

Doctoral Dissertation


Belgrade, 2019

UNIVERSITY OF BELGRADE
FACULTY OF PHYSICS

Aleksandra Dimić

# DETECTION OF QUANTUM CORRELATIONS

Doctoral Dissertation


Belgrade, 2019

UNIVERZITET U BEOGRADU

FIZIČKI FAKULTET

Aleksandra Dimić

# DETEKCIJA KVANTNIH KORELACIJA

Doktorska disertacija


Beograd, 2019.

**Supervisors:**

- Ass.-Prof. Mag. Dr. Borivoje Dakić, Assistant Professor, Faculty of Physics, University of Vienna
- Prof. Dr. Milan Damnjanović, Full Professor, Faculty of Physics, University of Belgrade

**Advisory Committee:**

- Prof. Dr. Ivanka Milošević, Full Professor, Faculty of Physics, University of Belgrade
- Prof. Dr. Tatjana Vuković, Associate Professor, Faculty of Physics, University of Belgrade
- Dr. Antun Balaž, Research Professor, Institute of Physics Belgrade, University of Belgrade

**Defense date:**

# Acknowledgments

My sincere appreciations go to Prof. Dr. Borivoje Dakić for his leadership, engagement, and supervision throughout the years. Discussions of quantum foundations and quantum technologies in WUK were a unique experience that made me more open-minded and laid the groundwork for my further research. I would like to thank Prof. Dr. Časlav Brukner for his support during my time as a visiting student in his group. His passion for fundamental research led to many stimulating discussions, and his positivity made me feel welcomed during every visit to Vienna. I am therefore emotionally attached to people without whom I would never take the scientific path: Prof. Dr. Đorđe Spasojević and Prof. Dr. Milorad Kuraica, who were supervisors of my master thesis in Belgrade. I extend gratitude to my internship supervisor Prof. Dr. Morgan Mitchell, who gave me the rare opportunity to do research in my pre PhD year. I deeply appreciate the encouragement and support he provided. I will never forget five wonderful, life-changing months in Barcelona and all the amazing people I met at ICFO.

A special place in my research work has Prof. Dr. Milan Damnjanović. Milan's probing chasing questions were of great importance for the deep understanding of the quantum world and made me more self-confident and assertive when speaking about my work. He also supported my stay in Belgrade as a research and teaching assistant and suggested a collaboration with Prof. Dr. Borivoje Dakic. I was lucky to meet Marko Milivojević and Dragoljub Gočanin, fellow PhD students. Many thanks to both of you for the fantastic time spent working, discussing and traveling together.

From the many people with whom I enjoyed important discussions during the last few years I would like to thank especially Valeria Saggio, Ivan Šupić and Flavio Del Santo. Thank you for being great partners in crime and reading all long e-mails explaining crazy ideas that I had time from time. I will always cherish my collaboration with Valeria, who had the patience to explain to me every experimental detail and handle my rashness. I owe special thanks to Prof. Dr. Philip Walther for a fruitful collaboration. He accepted a theoretical proposal made by Borivoje and I, and gave Valeria a "hot potato" that had to be confirmed.

Many thanks go to Brukner's and Walther's group for coming to Belgrade for an amazing group retreat. It is easy to be a good host when you have cheerful guests.

I should not miss the opportunity to thank all colleagues from my group – Group for Quantum, Mathematical, and Nano-Physics led by Prof. Milan Damnjanović and all colleagues from Center for Quantum Theoretical Physics, in particular for great

seminars and discussions we had.
Many thanks to Thesis Advisory Committee, Prof. Dr. Ivanka Milošević, Prof. Dr. Tatjana Vuković and Dr. Antun Balaž.

I acknowledge support from the project no. ON171035 of Serbian Ministry of Education and Science and from the scholarship awarded from The Austrian Agency for International Cooperation in Education and Research (OeAD-GmbH).

I would especially like to thank Nataša Dragović, Ajil Jalal and Joshua Morris for helpful suggestions while preparing the dissertation. Finally, I thank my mother Mirjana for her unconditional support and continuing inspiration. And for the real end, the most important place in this acknowledgement is taken by Dragoljub Gočanin for being there for me and with me at all time and sharing all victories in science and life.

In Belgrade, September 2019

*Aleksandra Dimić*

**Abstract**

One of the main foci of modern applied quantum information theory is the production of large-scale quantum entanglement involving many particles, to achieve the next-generation quantum technologies. Although a full-scale quantum computer is still far away in time, in the next few years we can expect to have quantum devices composed of up to a hundred controllable qubits. The primary challenge in moving towards such devices lies in the development of reliable and resource-efficient detection techniques to prove genuine quantum advantage. The main objective of this thesis is to investigate novel methods to detect the presence of quantum correlations in such systems, in particular, quantum entanglement and quantum nonlocality.

The first part of this thesis is dedicated to entanglement detection in large-scale quantum systems. Our main goal is to develop a novel probabilistic method in which entanglement is seen as an ability of a quantum system to accomplish certain information-processing tasks. We show that for certain classes of large (e.g. few tens of qubits) quantum states, even a single copy of a quantum state suffices to detect entanglement with a high confidence. Compared to the standard detection methods, this makes our method exceptionally resource-efficient. The developed probabilistic scheme applies to multiple classes of states, vital for quantum computation, such as cluster states or ground states of local Hamiltonians.

In the second part of this thesis, we develop a generic framework for translating any entanglement witness into a resource-efficient probabilistic scheme. We show that the confidence level of entanglement detection grows exponentially fast with the number of detection events, which makes this ansatz very efficient and reliable. Furthermore, we present the first experimental performance of our method by verifying the presence of entanglement in a photonic six-qubit cluster state.

The third part of this thesis describes the extension of our entanglement verification method to quantum nonlocality. Concrete examples are presented where we convert Bell's inequalities into the probabilistic procedure and incorporate our method into self-testing schemes. We show that the performance of our method significantly exceeds the ability of the existing methods for detection of quantum nonlocality and self-testing.

The last part of this thesis is a study of the weak-convergence properties of random variables generated by quantum measurements. Be-

ginning with a sequence of random variables generated by repeated unsharp quantum measurements, we study the limit distribution of measured relative frequency. We provide the de Finetti-type of representation theorem for all separable states, showing that the measured distribution can be well approximated by a mixture of normal distributions. Additionally, we investigate the convergence rates and show that the relative frequency converges to some constant at the rate of order $1/\sqrt{N}$ for all separable inputs. Finally, we provide an example of a strictly unsharp quantum measurement where we obtain better scaling by using entangled inputs. We find such behaviour of entangled states relevant for quantum information processing.

**Key words:** quantum correlations, entanglement, probabilistic method, detection, quantum nonlocality, convergence, random variables
**Scientific field**: Physics
**Research area**: Quantum Information Theory
**UDC number:** 530.145

**Rezime**

Glavni cilj istraživanja u oblasti moderne primenjene kvantne informacije je generisanje višečestičnih sistema u kojima su prisutne kvantne korelacije (na prvom mestu kvantna spletenost), a koji se mogu primeniti za razvoj kvantnih tehnologija. Postojanje takve vrsta korelacija jeste jedan od osnovnih preduslova za rad kvantnih računara. Sam kvantni računar zahteva spletenost više (desetina) hiljada kvantnih bitova u potpuno kontrolisanim eksperimentalnim uslovima, što je još dalek cilj (sa praktičnog stanovišta). U ovom trenutku, nalazimo se u početnoj fazi razvoja kvantnih tehnologija i u narednih nekoliko godina možemo očekivati realizaciju kvantnih sistema koji se sastoje od nekoliko stotina kvantnih bitova, u relativno kontrolisanim uslovima. Jedan od osnovnih zadataka i budućih izazova jeste razvoj novih metoda detekcije kvantne spletenosti u višečesticnim sistemima. To je ujedno i osnovni cilj ove doktorske disertacije.

Prvi deo ove teze posvećen je detekciji kvantne spletenosti u velikim kvantnim sistemima. Predstavljen je novi probabilistički metod detekcije kvantne spletenosti baziran na kvantno-informatičkim protokolima. Uveden je novi pristup čitavom problemu detekcije, u kome se sama kvantna spletenost posmatra kao potencijal kvantnog sistema da uspešno ostvari neki vid obrade informacije. Pokazali smo da u slučaju određenih klasa velikih kvantnih stanja (desetak kvantnih bitova), možemo detektovati kvantnu spletenost iz samo jedne kopije kvantnog stanja sa visokim nivoom poverenja. Stoga je razvijeni metod detekcije višestruko efikasniji u poređenju sa standardnim metodama. Ovaj metod se može primeniti na klase stanja posebno značajne za kvantno računarstvo, kao što su klaster stanja ili osnovna stanja lokalnih hamiltonijana.

Drugi deo ove teze fokusiran je na razvoj generalnog metoda za prevođenje bilo koje detekcione procedure bazirane na operatorima provere *entanglement witnesses* u efikasnu probabilističku shemu. Pokazano je da nivo poverenja detekcije kvantne spletenosti raste eksponencijalno sa brojem kopija posmatranog kvantnog sistema, što potvrđuje efikasnost metoda. Urađena je prva eksperimentalna potvrda razvijenog metoda, verifikacijom kvantne spletenosti u fotonskom klaster stanju koje se sastoji od šest kvantnih bitova.

U trećem delu ove teze, razvijeni metod primenjen je na detekciju nelokalnosti. Kroz različite primere, pokazali smo kako se vrši prevođenje Belovih nejednakosti u probabilističku proceduru i kako se

ovaj metod može iskoristiti kao alternativa za metod samoprovere (*self-testing*). Pokazano je da je učinak razvijenog metoda znatno bolji od dosadašnjih metoda detekcije kvantne nelokalnosti.

Poslednji deo ove teze predstavlja ispitivanje konvergencije distribucije slučajnih varijabli dobijenih pomoću generalnih kvantnih merenja. Izvedena je teorema de Finetijevog tipa za sva separabilna kvantna stanja, u kojoj smo pokazali da se sve distribucije generisane pomoću ovih stanja mogu dobro aproksimirati kao konveksna kombinacija normalnih raspodela. Ispitivana je i brzina konvergencije raspodele i dobijeno je da se u slučaju separabilnih stanja relativna frekvencija stabilizuje brzinom reda $1/\sqrt{N}$, gde je $N$ broj ponavljanja. Sa druge strane, kvantno spletena stanja daju bolje (veće) brzine konvergencije. Takvo ponašanje kvantno spletenih stanja kroz odgovarajuće protokole, tj. "kvantne igre" može biti upotrebljeno za detekciju kvantnih korelacija.

**Ključne reči:** kvantne korelacije, kvantna spletenost, probabilistički metod, detekcija, kvantna nelokalnost, konvergencija, slučajne varijable
**Naučna oblast:** Fizika
**Uža naučna oblast:** Kvantna informacija
**UDK broj:** 530.145

**List of Publications**

Publications which content constitutes part of this dissertation are coloured dark green and the chapter where the publication is referred to is indicated in the parentheses.

**Articles in refereed journals**

**1.** Dimić, A. and Dakić, B., Single-copy entanglement detection. *NPJ Quantum Information*, **4(1)**, 11 (2018). *(Chapter 4, section 1; in part Chapter 1, 2 and 3)*

**2.** V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, and B. Dakić, Experimental few-copy multipartite entanglement detection. *Nature Physics*, **15**, 935-940 (2019). *(Chapter 4, section 2)*[1]

**3.** Dimić, A. and Dakić, B. On the central limit theorem for unsharp quantum random variables. *New J. Phys.* **20**, 063051 (2018). *(Chapter 6)*

**4.** Lucivero, V. G., Dimić, A., Kong, J., Jiménez-Martínez, R., and Mitchell, M. W. Sensitivity, quantum limits, and quantum enhancement of noise spectroscopies. *Physical Review A*, **95**(4), 041803 (2017).

[1]The theoretical work is provided by Dakić, B. and Dimić, A., while the experimental work is done by Saggio, V. and co-workers.

**Contents**

## List of Figures

# 1 Introduction

Quantum computers promise to outperform their classical counterparts by employing genuine quantum features such as superposition and entanglement. The milestone of practical quantum information research is to develop controllable quantum systems composed of thousands of qubits to achieve the so-called quantum computational supremacy [1]. One particular example of quantum computational advantage is the celebrated Shor's algorithm [2] which factors integer numbers in polynomial time.

While the practical realization of a universal quantum computer is still far in the future, the present quantum experiments are at the level of generating and manipulating tens of quantum bits with high precision [3, 4], which brings us into a new era of the so-called noisy, intermediate-scale quantum devices (NISQD) [5]. Such devices involve a large number of quantum particles, and have been already experimentally designed, for example in optical lattice simulations involving $10^3 - 10^4$ atoms [6, 7, 8, 9], experiments with hundreds of trapped ions [10], tens of qubits for commercial use in IBM Q Experience[2] or thousands of qubits in D-Wave systems[3]. These devices show high potential for real applications, as for modeling complex processes such as protein folding or nuclear reaction by using quantum simulators [11].

Nevertheless, in order to achieve the real applications of quantum technologies, we have to benchmark those quantum devices, i.e. to verify their correct functionality. This is the main task of the so-called *verification problem*, which involves entanglement verification [12], certification of quantum states [13], reliable quantum state tomography [14], verification of quantum computing [15], nonlocality detection [16] and self-testing [17]. While the techniques for verification of small-scale quantum systems have been extensively studied, developed and successfully implemented in practice, the verification and detection methods for large-scale quantum systems are yet to be designed and developed. This is the main research direction of this PhD thesis.

The objective of this doctoral research is to address the verification of quantum correlations in large-scale quantum systems from an information-theoretic perspective. There are two main goals:

- To develop resource-efficient method for detection of quantum correlations in

[2]See: https://www.research.ibm.com/ibm-q/
[3]See: https://www.dwavesys.com/

large-scale quantum systems with a central focus on quantum entanglement and quantum nonlocality.

- To show practical aspects of the designed method, i.e. to apply the theoretical results to concrete experimental situations, primarily focusing on photonic quantum devices.

Chapter 2 reviews the basic notion of quantum correlations and explains the different types of quantum correlations such as quantum entanglement and quantum nonlocality. In Chapter 3, we present the standard methods for detection of quantum correlations and explain their limitations. To overcome the difficulties of the standard techniques, we present a novel probabilistic framework for entanglement detection in Chapter 4. We apply these findings to the various classes of quantum states for which the method reveals reliable and resource-efficient entanglement detection even in a *single-copy* regime. We explicitly construct the detection procedure for $k$-producible states, cluster states and ground states of local Hamiltonians. Moreover, we discuss the robustness of the method in the presence of noise, which makes an essential step towards its practical applications. Furthermore, Chapter 4 introduces the general method for translating any entanglement witness to the probabilistic verification procedure. We show the practical aspect of our method by providing a proof-of-principle demonstration of our protocol with the six-qubit H-shaped cluster state. The generalization of our method to nonlocality detection and self-testing is presented in Chapter 5. We focus our research on detection of nonlocality in cluster states. Finally, in Chapter 6, we present our work on the weak convergence of quantum random variables under general quantum measurements. We study the properties of the measured distribution and deliver our result in the form of a theorem of the de Finetti-type. We examine different behaviour of separable and entangled states under general measurements from the quantum-information perspective. More precisely, we formulate the distinction between separable (classical) and entangled states by means of a "quantum game". We show that entangled states have better convergence rates in comparison with separable ones. Apart from the applications in quantum information, we find these results relevant for quantum metrology as well. Chapter 7 gives a summary of the thesis and possible impact it could have on practical applications of quantum technologies.

# 2 Quantum Correlations

In this chapter, we will introduce basic notions of quantum correlations, in particular, quantum entanglement and quantum nonlocality. We will start with fundamental concepts, such as qubits, their transformations and general quantum measurements. Then, we continue with defining the difference between entangled and separable quantum states and local and nonlocal quantum correlations. Finally, we explain the idea of self-testing, i.e. we introduce the device-independent framework for quantum nonlocality.

## 2.1 Basic ingredients of quantum information: states, transformations and measurements

The mathematical foundations of quantum mechanics have been formulated by Von Neumann [18] involving the notion of Hilbert space, unitary operators and completely positive maps. Let $\mathcal{H}$ be a complex Hilbert space associated to a quantum system. In this thesis we will consider quantum systems having a finite-dimensional (dimension is denoted as $d$) Hilbert space only, i.e. $\mathcal{H} = \mathbb{C}^d$. The most relevant case is $d = 2$, which represents a quantum bit (qubit). There are many physical realisations of the qubit, such as the spin of an electron, or a photon in a superposition of two orthogonal polarisations. A pure state[4] of a qubit $|\psi\rangle$ is defined by normalised linear combination of basis states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1. \tag{2.1}$$

The states $|0\rangle$ and $|1\rangle$ constitute the so-called computational basis. For a general $d$-level system (usually called qudit), the equation (2.1) extends to

$$|\psi\rangle = \sum_{k=0}^{d-1} \alpha_k |k\rangle, \quad \alpha_k \in \mathbb{C}, \quad \sum_{k=0}^{d-1} |\alpha_k|^2 = 1. \tag{2.2}$$

For simplicity, we provide complete analysis for qubits, and all the results derived here can be easily generalized to the case of qudits.

For a composite system of $N$ qubits, the total Hilbert space is a tensor product of single-qubit spaces, i.e.: $\mathcal{H} = \otimes_{k=1}^{N} \mathcal{H}^{(k)}$. The computational basis states of this system are of the form $|i_1 i_2 ... i_N\rangle$, where $i_k = 0, 1$. A state of such a system is

[4] Throughout this thesis, we will use Dirac *bra* - *ket* notation.

specified by $2^N$ probability amplitudes. Thus, the most general pure state of $N$ qubits is given by

$$|\psi_N\rangle = \sum_{i_1...i_N=0,1} \alpha_{i_1...i_N}|i_1...i_N\rangle \qquad \sum_{i_1...i_N=0,1} |\alpha_{i_1...i_N}|^2 = 1. \tag{2.3}$$

Before we introduce the concept of transformation and quantum measurement, let us consider the notion of a mixed quantum state.

**Definition 2.1.** Let us suppose that a quantum system can be prepared in one of the pure states $|\psi_i\rangle$, $(i = 1, 2...)$, with respective probabilities $p_i$. An ensemble of pure states is set of pairs $\{p_i, |\psi_i\rangle\}$. The density operator, i.e. *mixed state* for such a system, is defined by

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|, \qquad \sum_i p_i = 1. \tag{2.4}$$

The basic properties of the density matrix are contained in the following theorem [19].

**Theorem 2.1.** An operator $\rho$ is the density operator associated to some ensemble $\{p_i, |\psi_i\rangle\}$ if and only if it satisfies the conditions:

- (Hermiticity) $\rho$ is hermitian operator.
- (Positivity condition) $\rho$ is a positive-semidefinite operator, i.e. $\langle\varphi|\rho|\varphi\rangle \geq 0$ for any $|\varphi\rangle$.
- (Normalisation condition) $\mathrm{Tr}\rho = 1$.

It is easy to show that $\mathrm{Tr}\rho^2 = 1$ if and only if $\rho$ is a pure state, i.e. $|\psi\rangle\langle\psi|$. One can also prove the following interesting property of $N$-qubit density matrix. Namely, for $N$-qubit mixed state $\rho_N$ we have $\frac{1}{2^N} \leq \mathrm{Tr}\rho_N^2 \leq 1$. The lower and upper bounds of the last inequality are achieved by maximally mixed and pure states, respectively [19].

Time-evolution of a *isolated* quantum system is described by a unitary operator $U(t - t_0)$ that transforms the quantum state $\rho$ of the system. That is, the state $\rho$ of the system at time $t_0$ is uniquely related to the state $\rho'$ of the system at some later time $t > t_0$ by

$$\rho' = U\rho U^\dagger. \tag{2.5}$$

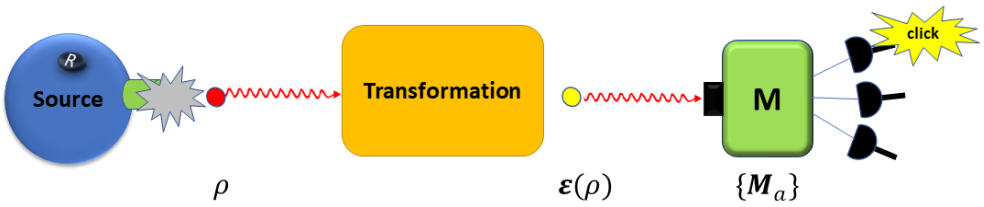


**Figure 2.1:** The basic elements of quantum information processing: preparation, transformation and measurement of a quantum system.

Unitary operators are information-preserving, in the sense that they do not change the scalar product (the degree of overlap) between quantum states. In particular, under unitary evolution orthogonal states stay orthogonal. To deal with a more realistic non-isolated systems, such as the systems that undergo interaction with the environment and decoherence, one has to generalize the notion of a quantum transformation to completely positive (CP) maps.

**Definition 2.2.** Let us introduce the set of operators $\{M_a\}$ such that they satisfy completeness relation:

$$\sum_a M_a^\dagger M_a = \mathbb{1}. \tag{2.6}$$

They are called *Kraus operators*. Linear map $\epsilon$ that maps the quantum state $\rho$ into

$$\epsilon(\rho) = \sum_a M_a \rho M_a^\dagger \tag{2.7}$$

is completely positive trace preserving map (CPTP) or simply, a quantum channel.

CP maps do not only represent the most general transformations of a quantum state, but also they are closely related to general quantum measurements. Before introducing them, let us define the notion of a standard, i.e. projective quantum measurement.

**Definition 2.3.** A *projective measurement* is described by an observable $M$, a Hermitian operator on the state space of the system being observed. The observable has a spectral form

$$M = \sum_m m P_m, \tag{2.8}$$

where $P_m$ is the projector onto the eigenspace of $M$ with eigenvalue $m$. The eigenvalues $m$ are the possible measurement outcomes. Upon measuring the state $\rho$, the

probability of getting result $m$ is given by

$$p(m) = \mathrm{Tr}(P_m \rho). \tag{2.9}$$

Given that outcome $m$ occurred, the state of the quantum system immediately after the measurement is updated to

$$\frac{P_m \rho P_m}{\mathrm{Tr}(P_m \rho)}. \tag{2.10}$$

By definition, the expectation value of the projective measurement is

$$\mathbb{E}[M] = \langle M \rangle = \sum_m m p(m) = \sum_m m \mathrm{Tr}(P_m \rho) = \mathrm{Tr}(M\rho). \tag{2.11}$$

Similarly, the variance associated to the measurement of $M$ is given by

$$\mathrm{Var}[M] = \langle (M - \langle M \rangle)^2 \rangle = \langle M^2 \rangle - \langle M \rangle^2. \tag{2.12}$$

The square root of the variance is the standard deviation which is the measure of the typical spread of the observed values upon measurement of $M$. Projective measurements are the special class of the general quantum measurements or positive operator value measures (POVMs) which capture the most general situation of measuring the system that interacts with an enviroment. The mathematical formalism for defining POVMs is given by the Naimark theorem [20]. The Naimark theorem says that if we focus attention on a portion of a composite system where a standard projective measurement takes place, then the statistics of the outcomes and the post-measurement states of the target system may be obtained with the tools of CP maps and Kraus operators. They define the formalism for POVMs.

**Definition 2.4.** A *general quantum measurement* is described by the set of Kraus operators $M_m$ that satisfy the completeness relation $\sum_m M_m^\dagger M_m = \mathbb{1}$. Each of the Kraus operators is associated to the measurement outcome and they appear with the probability $p(m) = \mathrm{Tr}(M_m^\dagger M_m \rho)$. We define

$$E_m = M_m^\dagger M_m. \tag{2.13}$$

Then $E_m$ is a positive operator such that

$$\sum_m E_m = \mathbb{1} \quad \text{and} \quad p(m) = \mathrm{Tr} E_m \rho. \tag{2.14}$$

Therefore, the set of operators $\{E_m\}$ is sufficient to determine the probabilities of the different measurement outcomes. The operators $E_m$ are known as the POVM

elements associated with the measurement. The complete set $\{E_m\}$ is known as the POVM.

Now, we have all the ingredients to illustrate a typical quantum experiment from the operational point of view (see Figure 2.1). The quantum experiment consists of preparation of the quantum system, its transformation through CP map and finally, a general quantum measurement.

## 2.2 Distance measures in quantum information

One of the main goals of the presented work is to find a reliable and resource-efficient method for verification of quantum correlations, more specifically of quantum entanglement. As figures of merit, we will extensively use various information-theoretic measures such as the probability of success or fidelity of quantum state. For the sake of completeness, we want to present two standard measures of "the closeness" of two quantum states, the trace distance and fidelity of quantum states [19].

**Definition 2.5.** The *trace distance* between quantum states $\rho$ and $\sigma$ is defined as

$$D(\rho, \sigma) = \frac{1}{2}\mathrm{Tr}|\rho - \sigma|, \tag{2.15}$$

where $|A| = \sqrt{A^\dagger A}$.

If $\rho$ and $\sigma$ commute, then the trace distance between $\rho$ and $\sigma$ is equal to the classical trace distance between probability distributions defined by the sets of eigenvalues of $\rho$ and $\sigma$ [19]. More explicitly, if $\rho$ and $\sigma$ commute they have a common orthonormal eigenbasis $\{|i\rangle\}$:

$$\rho = \sum_i r_i |i\rangle\langle i| \quad \text{and} \quad \sigma = \sum_i s_i |i\rangle\langle i|. \tag{2.16}$$

Therefore,

$$D(\rho, \sigma) = \frac{1}{2}\mathrm{Tr}\left|\sum_i (r_i - s_i)|i\rangle\langle i|\right| = \frac{1}{2}\sum_i |r_i - s_i|. \tag{2.17}$$

In the classical probability theory, this measure is known as distinguishability of probability distributions or Kolmogorov distance.
The second important measure of closeness of two quantum states is quantum fidelity [19].

**Definition 2.6.** If $\rho$ and $\sigma$ are two quantum states then the *fidelity* between them is defined as

$$F(\rho, \sigma) = (\mathrm{Tr}[(\sqrt{\rho}\sigma\sqrt{\rho})^{1/2}])^2. \tag{2.18}$$

If $\rho = \sigma$ then $F(\sigma, \rho) = 1$. In the case of fidelity of a pure state $|\psi\rangle$ and a mixed state $\rho$ we have

$$F(\rho, |\psi\rangle) = \langle\psi|\rho|\psi\rangle, \tag{2.19}$$

which represents the overlap (probability of confusing) between states $|\psi\rangle$ and $\rho$.

## 2.3 Quantum entanglement

In order to define entanglement, we first need to define its opposite: separability.

**Definition 2.7.** A pure quantum state $|\psi_{AB}\rangle$ of a composite system $\mathcal{H}_A \otimes \mathcal{H}_B$ is *separable* if and only if:

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle. \tag{2.20}$$

**Definition 2.8.** A general mixed quantum state $\rho_{AB}$ is called *separable* if it can be written as a probabilistic mixture of separable pure states:

$$\rho_{AB} = \sum_i p_i |\psi_A^{(i)}\rangle\langle\psi_A^{(i)}| \otimes |\psi_B^{(i)}\rangle\langle\psi_B^{(i)}|, \text{ such that } p_i \in [0,1] \text{ and } \sum_i p_i = 1. \tag{2.21}$$

**Definition 2.9.** A quantum state that is not separable is called *entangled quantum state*.

Each separable density matrix can be prepared by following specific instruction, via mixing the states $|\psi_A^{(i)}\rangle$ and $|\psi_B^{(i)}\rangle$ drawn from a classical probability distribution $\{p_i\}$. Such preparation procedure is known as *LOCC*, i.e. a separable state can be produced by local operations supported by classical communication (LOCC) [21, 22]. On the contrary, any state that is not separable (entangled state) cannot be produced by LOCC. If we want to examine subsystems of a composite quantum system, we need to introduce the reduced density operator which describes the state of the subsystem.

**Definition 2.10.** A quantum system composed of two subsystems A and B is described by a density operator $\rho_{AB}$. The state of the subsystem A is described by the reduced density operator

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}), \tag{2.22}$$

where $\mathrm{Tr}_B$ is the *partial trace* over system B.

One can pose a question on how to use a partial trace to describe a subsystem of a composite quantum system. It can be proven [19] that the partial trace is the unique operation which gives the accurate description of observable quantities for subsystems of a composite system. And to confirm it, we will introduce the notion of a local observable.

**Definition 2.11.** Local observables acting on a system AB are of the form $A \otimes B$ and they correspond to properties that can be measured locally.

Having this in mind, let us assume that $M_A$ is observable of the system A. If we ignore the properties of the system B, than the corresponding observable on a joint system $\tilde{M}_{AB}$ is given by

$$\tilde{M}_{AB} = M_A \otimes \mathbb{1}. \tag{2.23}$$

Now, we should show that the partial trace procedure gives the correct measurement statistics for observations on the part of the system. We can use the fact that measurement averages must be the same in both cases, when using only $\rho_A$ or using $\rho_{AB}$. By direct inspection, we get that

$$\mathrm{Tr}(M_A \rho_A) = \mathrm{Tr}(\tilde{M}_{AB} \rho_{AB}) = \mathrm{Tr}((M_A \otimes \mathbb{1}_B)\rho_{AB}) \tag{2.24}$$

is certainly satisfied if we choose $\rho_A \equiv \mathrm{Tr}_B(\rho_{AB})$. Moreover, the partial trace turns out to be a unique function having this property [19].

A very convenient way to analyze the entanglement properties of bipartite pure states is through the Schmidt decomposition.

**Theorem 2.2.** *Schmidt decomposition.* Suppose $|\psi\rangle$ is a pure state of a composite system AB. There exist orthonormal states $|i_A\rangle$ and $|i_B\rangle$ for subsystems A and B respectively such that

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle. \tag{2.25}$$

Here $\lambda_i$ are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$ and they are called Schmidt coefficients.

This is a classical theorem, proof of which can be found in many textbooks (see for example [19]). We will focus on the consequences of the Schmidt decomposition theorem. As the first example, let us consider a pure state $|\psi\rangle$ of a composite system AB. Then, by the Schmidt decomposition, we obtain $\rho_A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$

and $\rho_B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$, so the eigenvalues of $\rho_A$ and $\rho_B$ are identical. Therefore, all the properties captured by the eigenvalues will be the same for both subsystems. The second important feature that follows from the Schmidt decomposition is the quantity called the Schmidt number. Namely, for the state $|\psi\rangle$ with the Schmidt decomposition $\sum_i \lambda_i |i_A\rangle|i_B\rangle$, the number of non-zero values $\lambda_i$ is called Schmidt number. In some sense, this number quantifies the entanglement between systems A and B. First, the set of eigenvalues of $\lambda_i$ is invariant under local transformations of $\rho_A$ and $\rho_B$, i.e. $U_A \rho U_A^\dagger$ and $U_B \rho U_B^\dagger$ respectively. All algebraic-invariant quantities of this type (such as the Schmidt number) are a handy tool to analyze entanglement properties. For example, it is easy to prove that the state $|\psi\rangle$ is a product state if and only if it has Schmidt number 1. Consequently, if there are at least two non-zero $\lambda_i$ (Schmidt number = 2), the state is necessarily entangled. Furthermore, the bipartite measures of quantum entanglement (for pure states) can be expressed in terms of Schmidt coefficients, such as the entanglement of formation [23]

$$E_F = S[\rho_A] = S[\rho_B] = -\sum_i \lambda_i^2 \log_2 \lambda_i^2, \tag{2.26}$$

where $S[\rho] = -\operatorname{Tr} \rho \ln \rho$ is Von Neumann entropy.

### 2.3.1 Classification of entanglement

Classification of entanglement will be discussed in terms of experimental work in the next chapters. Here, for the sake of completeness, we want to provide some general definitions of the classes of entanglement both for pure and mixed states.

**Definition 2.12.** Let us assume that $|\psi\rangle$ is a $N$-partite pure quantum state , i.e. $|\psi\rangle \in \otimes_{k=1}^N H^{(k)}$. The state $|\psi\rangle$ is *fully separable* if it can be written in the product form

$$|\psi\rangle = \otimes_{i=1}^N |\phi_i\rangle. \tag{2.27}$$

Further, let us assume that $\rho$ is $N$-partite mixed quantum state. The state $\rho$ is called *fully separable* if it can be written as a convex combination of pure fully separable states:

$$\rho = \sum_k \omega_k |\phi_1^{(k)}\rangle\langle\phi_1^{(k)}| \otimes |\phi_2^{(k)}\rangle\langle\phi_2^{(k)}| ... \otimes |\phi_N^{(k)}\rangle\langle\phi_N^{(k)}|. \tag{2.28}$$

If a quantum state is not fully separable, then it contains some entanglement. The question is: what structure of entanglement does it contain? There are different ways of answering this question, and here we will use basic way of classification provided in [24].

**Definition 2.13.** We call a pure $N$-partite state *$m$-separable*, with $1 < m < N$, if there exist a splitting of the $N$ systems into $m$ parts $P_1, ..., P_m$ such that

$$|\psi\rangle = \otimes_{i=1}^{m} |\phi_i\rangle_{P_i} \tag{2.29}$$

holds. Here $|\phi_i\rangle_{P_i}$ is the state of part $P_i$. Using elementary combinatorics, we can derive that there are $\frac{m^N}{m!}$ possible partitions of the $N$ systems into $m$ parts.

In accordance with definition 2.13, we call a mixed state $m$-separable, if it can be written as a convex combination of pure $m$-separable states (which can belong to different partitions).

Note that an $m$-separable state contains some entanglement in at least one partition. Using definition 2.13 we can only say that $m$ partitions are separable. On the other side, one could ask an alternative question: how many particles are entangled? According to that, we provide the following definition.

**Definition 2.14.** An $N$-partite pure state $|\psi\rangle$ is said to contain only *$m$-party entanglement*, if it can be written as

$$|\psi\rangle = \otimes_{i=1}^{K} |\phi_i\rangle, \tag{2.30}$$

where $K \geq N/m$ and the $|\phi_i\rangle$ are states of maximally $m$ qubits. If $|\psi\rangle$ is not of this form, it contains at least $(m+1)$-party entanglement.

The last definition can be expanded to mixed states using convex combinations. Similarly, we can introduce the notion of $k$-producibility.

**Definition 2.15.** A mixed state is *$k$-producible* if it requires only the generation of $k$-party pure entangled states and mixing for its production.

Consequently, a mixed state contains k-party entanglement, if and only if the density matrix cannot be obtained by mixing pure states that are $(k-1)$-producible. The definitions provided give elementary classes of entanglement. The general classification is far more complex. However, in most experimental situations, we aim to verify genuine multipartite entanglement (i.e. the state of $N$ particles that contains $N$-party entanglement); thus, we put the focus on the whole system, instead of one particular partition.

## 2.4 Quantum nonlocality

In 1964, Bell found that the predictions of quantum theory are incompatible with those of any physical theory satisfying a natural notion of locality [25]. Bell's theorem has profoundly influenced our perception and understanding of physics and arguably stands among the most important scientific discoveries ever made. With the development of quantum information, many scientists put their interest in Bell's theorem. They took part in developing both fundamental concepts and technical tools for describing and studying nonlocality of quantum theory. Here, we omit many significant contributions before and after Bell's ground-breaking discovery, the most notable one being the famous Einstein-Podolsky-Rosen paper [26], and we establish operational formulation of locality. The complete review of the field can be found in [27] and references therein.

### 2.4.1 Operational framework for quantum nonlocality

The typical scenario for any Bell-like experiment is a game between two players, usually called Alice and Bob. Alice and Bob sit in their distant, spacelike separated laboratories and use a shared resource in the game. Commonly, a resource is a collection of pairs of systems which may have previously interacted. For example, two particles provided by a common source, which are now spatially separated and each of them is measured by one of two observers, either Alice or Bob. Both Alice and Bob have freedom of choice to pick up measurement that she or he will perform on the corresponding particle. We will denote Alice's measurement choice with $x$ and Bob's with $y$. For instance, $x/y$ may indicate the position of a knob on *her*/*his* measurement apparatus.

Once the measurements on the particles are performed, they yield some outcomes which we will denote as $a$ for Alice and $b$ for Bob. In each run of the game, players can obtain diverse outcomes, even if the same pair $(x, y)$ measurement choices are made. Therefore, the main quantity for describing the whole game is the probability distribution $p(a, b|x, y)$. By repeating the procedure a certain number of times and collecting the observed data, one gets a reasonable estimate of such probabilities. If this type of experiment is really performed, it will be observed that in the general case

$$p(a, b|x, y) \neq p(a|x)p(b|y), \tag{2.31}$$

i.e. measurement outcomes are not statistically independent. Obtained correlations do not imply extraordinary behaviour of two observed systems, for example,

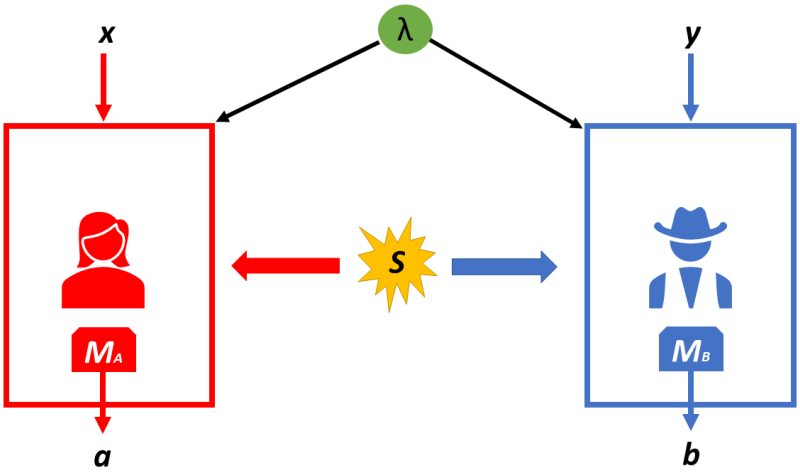


**Figure 2.2:** Can we have two parties, Alice and Bob residing in their spacelike separated laboratories and explain all the results of their experiments just by using classical probabilistic strategy defined by parameter $\lambda$?

instantaneous influence between spacelike separated particles, but some dependence between them, which was established during their interaction in the past.

Let us establish a more formal statement of local theory. Locality assumption says that we can identify the complete set of past factors, that will be denoted with $\lambda$, and that had a joint causal influence on both system which determined getting results $a$ and $b$. If we find all these factors, then all the rest indeterminacies about the outcomes do not exist, formally meaning factorisation of probabilities:

$$p(a, b|x, y, \lambda) = p(a|x, \lambda)p(b|y, \lambda). \tag{2.32}$$

Taking factorisation into account, we conclude that there must exist a description of the observed systems that depend only on the joint past variables $\lambda$ and local measurements. Furthermore, the variable $\lambda$ can have probabilistic behaviour, involving some physical process that is not completely controllable. Thus, we can describe it with the probability distribution of $q(\lambda)$. If we combine probabilistic behaviour with factorization given in (2.32), then locality condition in the context of Bell experiments is as follows:

$$p(a, b|x, y) = \int_\Lambda \mathrm{d}\lambda q(\lambda)p(a|x, \lambda)p(b|y, \lambda). \tag{2.33}$$

Here we also assume that Alice and Bob freely chose settings $x$ and $y$ independently of $\lambda$, i.e. $q(\lambda|x, y) = q(\lambda)$. We should emphasize that equation (2.33) is not derived under assumptions of determinism or "classical behaviour". We only assume that

Alice's result $a$ is probabilistically obtained by the measurement choice $x$ and the variable $\lambda$, without limitations on physical laws dictating causal relations. Illustration of a typical Bell experiment is given in Figure 2.2. The fundamental assumption behind (2.33) is that *events in one region of space-time should not influence events in spacelike separated regions* [27](no-signaling constraint). Now, it is a straightforward mathematical theorem that the predictions of quantum theory for certain experiments involving entangled particles do not admit a decomposition of the form (2.33).

When we think about Bell's games, as a starting example, we typically consider Alice and Bob sharing pairs of spin $\frac{1}{2}$ particles and measuring their spins in different directions. Locality condition then becomes famous *Clauser - Horne - Shimony - Holt* inequality [28], which is violated when parties share entangled inputs. It brings us to the statement of the famous Bell's theorem:

*No physical theory of local hidden variables can ever reproduce all of the predictions of quantum mechanics.*

More operationally said, violation of Bell's inequalities establishes a gap between what non-communicating parties have in their possession, classically or quantumly correlated resource.

### 2.4.2 Self-testing

Self-testing is a method to deduce the underlying physics of a quantum experiment in a black box scenario. As such, it represents the most reliable form of certification for quantum systems [17]. As one of the goals of the presented research is to merge a novel probabilistic framework for verification of quantum correlations and self-testing, the idea behind self-testing will be briefly predicted.
Let us imagine our two characters, Alice and Bob, entering two separated laboratories equipped with many instruments and devices which they do not know how to use. They only can realize that the experiment in each of the laboratories consists of a choice of settings $(x/y)$ and result shown on the screen $(a/b)$. Both of them have some knob in their respective laboratories that Alice can put in a set of positions $x$ and Bob in a set of positions $y$. Furthermore, there is a source emitting physical systems positioned straight between the laboratories. In each run of the experiment, the source sends two physical systems, one to Alice and another to Bob. Alice and

Bob have a task to find out what is the state $\rho$ which the source is emitting. In principle, they could do quantum state tomography, but they do not know how things work in their laboratories, nor the general characteristics of the produced physical systems. The only thing they can do is acquire the statistics and estimate probabilities of seeing results $a$ and $b$ when knobs are set to the positions $x$ and $y$:

$$p(a, b|x, y). \tag{2.34}$$

The situation presented is a sketch of the device-independent scenario. It turns out that Alice and Bob can accomplish the task using the Bell nonlocality [25] and maximal violations of corresponding Bell's inequality. A Bell's inequality is a function $\mathcal{F}$ of the probabilities $\{p(a, b|x, y)\}$ such that, for a source producing separable states one gets

$$\mathcal{F}(\{p(a, b|x, y)\}) \leq \mathcal{B}. \tag{2.35}$$

Bound $\mathcal{B}$ does not depend on the physical nature of the tested systems, as long as they are separable. Therefore, Alice and Bob can compare their set of probabilities against as many Bell's inequalities as they know. Maximal violation of Bell's inequality is possible only for a unique particular state that is prepared up to local transformations [17]. Thus, if the maximal violation is found in practice, we are sure that a very particular state $\rho$ (up to local transformations) is being prepared. The procedure described is called a device-independent self-test or simply a self-test of the quantum state.

# 3 Entanglement detection

There exists a plethora of entanglement quantifiers and classifiers, corresponding to different operational paradigms and mathematical techniques [24, 29]. However, for most quantum systems, correctly quantifying the amount of entanglement is exceedingly demanding, if at all possible.

For example, full quantum state tomography [30] is the method from which one can recover the entire density matrix and have complete information about the quantum state preparation. However, when dealing with moderate or large size quantum systems, the full tomography becomes an unworkable task as the number of measurement settings grows exponentially fast with the size of the system [29]. Fortunately, in many cases, we do not require complete knowledge of the quantum state. In such cases, one can find alternative ways to detect entanglement by measuring the mean values or the higher moments of a moderate number of physical quantities. Examples of such detection procedures are witness operator method [31, 32, 33, 34, 35, 36], non-linear entanglement witnesses [37, 38, 39], Bell's inequalities [40, 41], quantum Fisher information [42, 43, 44, 45] and random correlations [46, 47, 48]. These procedures are beneficial for many practical applications, and they have been broadly developed for different classes of quantum states and used in various scenarios (see review articles [49, 50, 24, 29]).

## 3.1 Standard methods of entanglement detection: Entanglement witness

In this section, we focus on one of the most common methods for entanglement verification, which is entanglement witness method [24].

**Definition 3.1.** An observable $W$ is called an entanglement witness if $\mathrm{Tr}(W\rho_s) \geq 0$ for all separable states $\rho_s$ and $\mathrm{Tr}(W\rho_e) < 0$ for at least one entangled state $\rho_e$.

From the definition of separability (2.21) we know that the set of separable states (that we will denote with $\mathcal{S}$) is a convex subset of all quantum states. The Hahn-Banach theorem [51] ensures that there is a hyperplane that distinguishes every entangled state from the set of separable states. These hyperplanes correspond to observables $W$, such that $\mathrm{Tr}(W\sigma) \geq 0$ for all $\sigma \in \mathcal{S}$ and $\mathrm{Tr}(W\rho) < 0$ for at least one entangled state [29]. Thus, if we measure $\mathrm{Tr}(W\rho) < 0$, we know for sure that the state $\rho$ is entangled. Furthermore, it is vital to note that entanglement witnesses

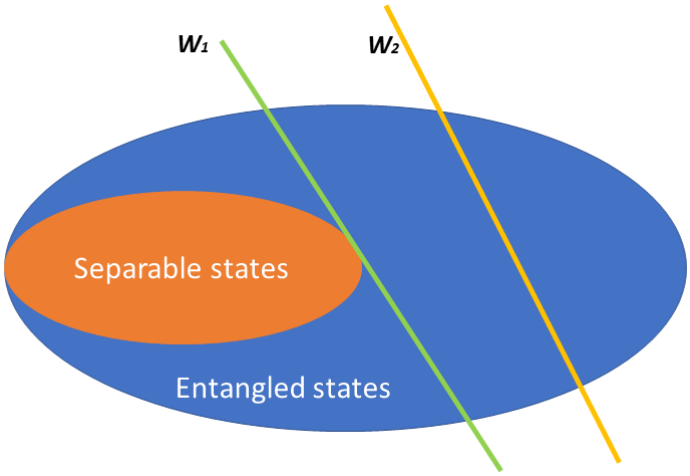


**Figure 3.1:** Figure taken from [24]. The green line represents the hyperplane where $\mathrm{Tr}W_1\rho = 0$. The witness $W_1$ is sharper than $W_2$.

have a clear geometrical meaning, see Figure 3.1. The expectation value of an observable depends linearly on the state. Hence, the set of states where $\mathrm{Tr}(W\rho) = 0$ holds is a hyperplane in the set of all states, cutting this set into two parts. In the first part with $\mathrm{Tr}(W\rho) > 0$ lies the set of all separable states, and in the other part with $\mathrm{Tr}(W\rho) < 0$, we have the set of entangled states detected by $W$ [24]. However, it is essential to note that finding $\mathrm{Tr}(W\rho) > 0$ does not indicate that $\rho$ is separable. Actually, chosen $W$ may not be a suitable witness for the state we want to verify. For example, in Figure 3.1 we have that one witness is obviously better than the other one. Formally speaking, witness $W_1$ is finer (sharper) than witness $W_2$ as it detects all the states detected by $W_2$ and also some states in addition. That means that $W_2$ can be written as $W_2 = W_1 + P$, where $P$ is a positive operator. Consequently, for any quantum state $\rho$ we obtain $\mathrm{Tr}(\rho W_1) \leq \mathrm{Tr}(\rho W_2)$. Therefore, the main goal is to construct sharp entanglement witnesses, which is an immense challenge without information about particular state generated in an experiment. Nevertheless, if we know the target state $|\psi_T\rangle$ (i.e. the state that the experimentalist aims to prepare), then we can use a canonical witness construction [24, 29]:

$$W = \lambda_{\max}^2 \mathbb{1} - |\psi_T\rangle\langle\psi_T|. \tag{3.1}$$

Here, $\lambda_{\max}$ denotes the largest Schmidt coefficient of $|\psi_T\rangle$. It represents the maximal overlap of the target state $|\psi_T\rangle$ with any separable state $\rho_s \in \mathcal{S}$, that is

$$\lambda_{\max} = \max_{\rho_s} \sqrt{\langle\psi_T|\rho_s|\psi_T\rangle}. \tag{3.2}$$

The separability condition $\mathrm{Tr}\rho_s W > 0$ is automatically satisfied. Even with this con-

struction, measurement of entanglement witness is highly nontrivial task in practice. Namely, it is clear that $W$ is not of the product form, i.e. $A_1 \otimes A_2 ... \otimes A_N$, therefore it cannot be measured locally [24, 29]. In other words, $W$ is global observable and its measurement is very demanding in practice (it requires the measurement of a joint system in entangled basis). In order to extract the mean value of $W$ by local measurements, one has to decompose the witness into local components,

$$W = \sum_i A_1^{(i)} \otimes \cdots \otimes A_N^{(i)}. \tag{3.3}$$

Each of the local observables $A_k^{(i)}$ has to be measured in a separate experiment. Therefore, one has to conduct different experiments (using different measurement settings for each), each of which requires a large number of identically prepared copies of the quantum system in order to extract the corresponding mean value with high accuracy. Such a procedure becomes intractable already for a moderate size of quantum systems.

## 3.2 Limitations of standard verification schemes

In this section, we review the main problems of standard methods for the detection of quantum correlations when dealing with large quantum systems. Consequently, we clarify the motivation for the research conducted in this thesis.

The first standard requirement which is hard to achieve in practice is to perform the verification method by repeating measurements on a large ensemble of identically prepared copies of a quantum resource. This is the so-called *i.i.d. (independent and identically distributed) assumption*, which means that a specific physical process, such as the use of quantum channel or preparation of the quantum state is done arbitrarily many times identically and independently of other processes. The i.i.d. assumption is justified for the case of small quantum systems, where a high level of control is present. On the other hand, if we increase the size of the quantum system, the level of control notably decreases and the i.i.d. requirement becomes infeasible. Based on the current status of experimental quantum information, tens of qubits of quantum systems are already difficult to handle as there is no guarantee given that the experiment can be repeated many times under the same conditions. The conventional techniques, such as the witness method heavily rely on i.i.d. assumption, therefore, their applicability is questionable, inaccurate and can even lead to unjustified observations [52].

The second standard requirement one has to fulfill in practice is collecting comprehensive and in the ideal case, infinite statistics in order to extract the mean values of desired quantities (e.g. mean value of the witness operator $W$). Ideally, we should have an infinite number of repeated experimental runs, but in real experiments, we perform a finite number of measurements, thus generating a finite amount of data. Practically, our aim becomes to collect "sufficiently large" statistics in order to compute standard deviations and estimate the errors. This method works if the number of available data is significantly large. Nonetheless, in real experiments, we are very far from this scenario. One may take the example of a recent experiment with single photons where the ten qubit entangled state was registered every five minutes on average [53]. In such case, the collection of a sufficient experimental data takes weeks of measurement. Furthermore, with the same technology, that is by using the parametric down-conversion and postselection techniques, every additional photon pair would reduce the count rate by at least one order of magnitude. Consequently, the duration of the experiment will become months or even years longer, provided that one can keep the system stable for such a long period of time. Therefore, we can expect that the next generation of quantum experiments dealing with 20-30 controllable qubits will significantly reduce the number of available instances of given quantum resources, making future experiments unreliable and unrealistic in justifiable time.

Finally, providing a reliable statistical analysis is the major challenge in dealing with a finite amount of data. The conventional method of calculating the sample variances and standard errors is known to be unreliable from the conceptual [54], and practical point of view [55]. It can even produce counter-intuitive results. Advanced statistical inference techniques such as maximum likelihood [56] or Bayesian estimation [57] are needed to obtain meaningful conclusions. While the theory of statistical analysis for the quantum scenario [58, 59] has been widely developed and established, the fundamental barrier for practical applications is the post-processing of experimental data. For instance, a quantum experiment involving a medium amount of quantum particles, like eight trapped ions, requires enormous computational resources for reliable statistical analysis, and the post-processing time can take several weeks [60]. The reason is simple: as the number of constituents of the quantum system increases, the number of parameters needed to model it explodes rapidly. For example, an $N$ qubit density matrix specification requires $3^N$ real parameters, making numerical calculations very difficult. On the other hand, we may "overfit" a system, since the gap between the number of observations and model parameters overgrows with the size of the system. In other words, the proposed theoretical models are intractable for practical applications due to a large number

of parameters.

Therefore, as the size of the systems grows, we will reach the limitations of the standard verification methods and novel models are needed to handle large-scale quantum systems. These models have to encompass into a sustainable framework a very limited statistics collected in practice, on one hand side, and significant number of parameters needed for modeling, on the other side.

# 4 Probabilistic entanglement detection

In recent years numerous works go beyond i.i.d. scenario, in the context of quantum state tomography [14] and reliable entanglement verification [12, 39]. Despite the techniques and methods developed there are quite generic, they still require many copies of the target quantum resource to provide high confidence of verification. In real experiments, where only a low number of instances of a given quantum resource are available, it seems natural to employ *random sampling techniques* [61] for reliable detection. The benefit of such techniques stems from a simple way to work out data analysis, since, in these cases, one does not need to have prior knowledge of the global population. In the quantum scenario, random sampling is demonstrated to be very useful for quantum communication complexity [62, 27], tomography via compressed sensing [63], fidelity estimation [64], self-testing methods [65, 66, 67, 68, 69, 70], quantum state certification [71, 72], quantum secret sharing [73] and verification of quantum computing [15]. One can use some of them for probabilistic verification of entanglement as demonstrated in [74, 75].

## 4.1 Single-copy entanglement detection

Here, our aim is to combine random sampling methods with techniques of quantum communication complexity [62, 27] in order to introduce entanglement verification scheme in the form of *a quantum information task*. Unlike standard verification procedures that focus on the repeated measurements and extraction of mean values, we are focusing on a single experimental run. The central quantity for entanglement detection is *the probability of success* to perform a particular binary task, given that the state was entangled/separable. Thus, our detection scheme is designed to detect entanglement probabilistically [76]. As compared to conventional detection schemes, our framework has two main advantages.
First, it promises a dramatic reduction of the resources needed for reliable verification in large quantum systems and second, it provides a simple tool for reliable statistical analysis.

Most importantly, we argue that in many situations the probability of accomplishing a certain binary task decreases exponentially fast with the system size for all separable inputs, whereas, it approaches certainty if a particular entangled state was prepared. Thus, even a *single experimental run* can reveal the presence of entanglement with high accuracy.

We explicitly construct the detection procedure for $k$-producible states [77] and cluster states [78]. The method developed for $k$-producible states can be used to naturally embed conventional entanglement witnesses methods into our framework, making the statistical analysis of confidence intervals and errors straightforward.

Finally, we design a general method for entanglement detection in ground states of local Hamiltonians that exhibit the so-called entanglement gap [35]. Among them are many vital classes of quantum states, such as the matrix product states [79] and projected-entangled pair states [80] as they can be seen as unique ground states of the so-called parent Hamiltonians [79, 81]. In the end, we analyze the noise effect, and we show that our probabilistic detection is very robust against the noise modeled by an arbitrary separable state.

### 4.1.1 Description of detection framework

Now, we will explain how our probabilistic scheme works. Let us consider a quantum system consisting of $N$ subsystems, each carrying a finite-dimensional Hilbert space of dimension $d$. In the case of $N$ qubits $d = 2$. In our analysis, we assume $N$ is large, although all derived formulas hold for general $N$. Then we associate a certain set of possible local measurements to each subsystem. For example, these may be measurements in complementary bases ($X$ and $Z$ measurement) in the case of qubits. In order to build the general case, we include the most general quantum measurements (POVMs). Therefore, to each subsystem we associate a set of $M$ different measurement settings defined by the set of positive semidefinite operators $E_{mi}^{(n)}$, where $\sum_i E_{mi}^{(n)} = \mathbb{1}$ and $m = 1 \dots M$. Here $n$ labels the subsystem, $m$ the measurement setting and $i$ labels the measurement outcome.

For a single copy of a $N$-partite quantum system, the detection procedure consists of the following four steps (see Figure 4.1):

1. A sequence of measurement settings $\{m_1, m_2, \dots, m_N\}$ is randomly generated from the probability distribution of settings $\Pi(m_1, \dots, m_M)$.

2. The measurements are locally performed on each subsystem and the set of outcomes $\{i_1, \dots, i_N\}$ is obtained.

3. A certain binary cost function of settings and outcomes $F_{[N]} = F_{m_1 \dots m_N}^{i_1 \dots i_N}$ is calculated.

4. If $F_{[N]} = 0/1$ we associate "success/failure" to the experimental run.

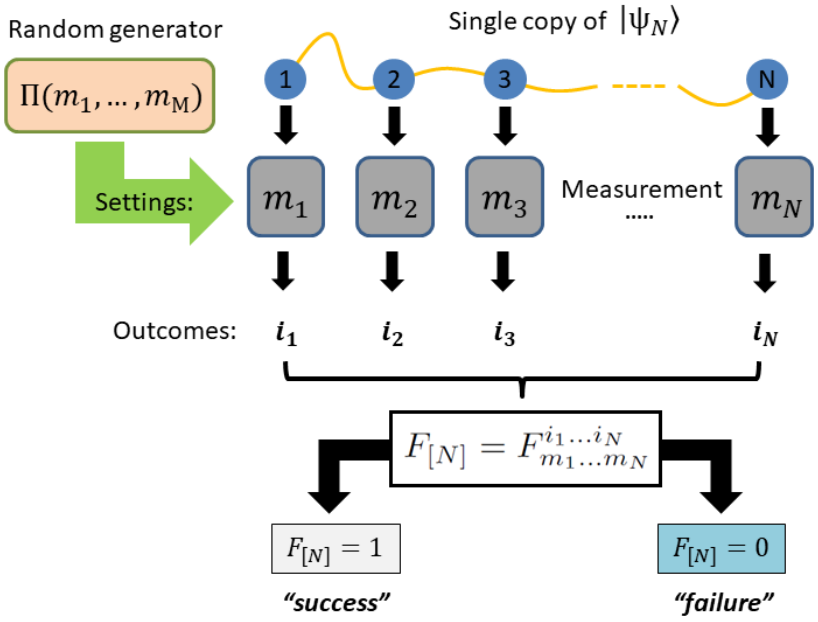


**Figure 4.1:** A single-copy of $N$-partite quantum state is prepared. The sequence of measurement settings $\{m_1, \ldots, m_N\}$ is randomly drawn from distribution $\Pi(m_1, \ldots, m_M)$. Each $m_k$ is locally executed on $k^{\text{th}}$ subsystem and the set of outcomes $\{i_1, \ldots, i_N\}$ is obtained. The value of binary cost function $F_{[N]} = F^{i_1 \ldots i_N}_{m_1 \ldots m_N}$ prescribes either "success" ($F_{[N]} = 1$) or "failure" ($F_{[N]} = 0$) to the experimental run.

The main goal here is to choose the cost function properly. It is created such that the probability of success vanishes exponentially fast in $N$ for all separable states $\rho_{sep}$

$$P_{\rho_{sep}}[F_{[N]} = 1] \leq \exp[-Nc], \tag{4.1}$$

where $c > 0$ is constant depending of the particular class of the quantum system. On the other hand, the $F_{[N]}$ is constructed such that there is an entangled state for which $P_{\rho_{ent}}[F_{[N]} = 1] \approx 1$, meaning that whenever the target state $\rho_{ent}$ has been prepared, the detection scheme works even in a one-shot scenario. In the next sections, we will provide explicit bounds on the probability of success for concrete examples.

### 4.1.2 Example of $k$-producible quantum state

The first example that we are going to present is that of the $k$-producible entangled state [77], i.e.

$$|\phi_1\rangle|\phi_2\rangle\ldots|\phi_m\rangle, \tag{4.2}$$

where the products $|\phi_s\rangle$ involve at most $k$ parties. To give even more concrete example, we take the target state to be the product of quantum singlets

$$|\psi_0\rangle = |\psi^-\rangle^{\otimes N}, \tag{4.3}$$

where

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{4.4}$$

We want to emphasize that provided example is inspired by "non-local" quantum games (see [62, 27]). Still, it is an appropriate starting point for introducing a more delicate examples. For each qubit, we have the set of $\{X, Y, Z\}$ measurement settings. Therefore, every measurement is performed in the eigenbasis of Pauli operators and gives binary outcome $i = 0$ or $i = 1$. The quantum singlet is the only state that satisfies $X \otimes X = Y \otimes Y = Z \otimes Z = -1$, which means that the measurement of $X \otimes X$, $Y \otimes Y$, and $Z \otimes Z$ will reveal perfect anticorrelations. Now we introduce the projectors on the outcome $-1$ for the correlation measurements

$$A = \frac{\mathbb{1} - X \otimes X}{2}, \tag{4.5}$$

$$B = \frac{\mathbb{1} - Y \otimes Y}{2}, \tag{4.6}$$

$$C = \frac{\mathbb{1} - Z \otimes Z}{2}. \tag{4.7}$$

Each of these projectors is associated with one of the three measurement settings $S = \{XX, YY, ZZ\}$. It can be easily checked that the projectors are commutative. Nevertheless, no separable state can reveal $A = B = C = 1$ simultaneously; the unique state with this property is the singlet state. The best chance to obtain the outcome 1 for all separable inputs is at most $2/3$. More precisely, the probability of success is bounded by

$$P_{\rho_{sep}} = \langle\frac{1}{3}(A + B + C)\rangle \leq \frac{2}{3}, \tag{4.8}$$

for all separable two-qubit states $\rho_{sep}$. Here $\langle\cdot\rangle = \mathrm{Tr}(\cdot)\rho$ denotes the mean value. This suggests that the detection procedure goes as follows. First, we divide the set of $2N$ qubits into consecutive pairs. Then, for every single pair, we randomly pick

one of the settings from $S$ (with probability 1/3). We perform the corresponding correlation measurement and collect $N$ results. For each pair, the result is given with

$$F_k = \frac{1}{2}\left(1 - (-1)^{i_k + j_k}\right). \tag{4.9}$$

Here $i_k, j_k = 0, 1$ denote the single-qubit measurement outcomes for the $k^{\text{th}}$ pair. Assuming that $N$ is large, from the bound (4.8) we can conclude that the relative frequency of the outcome 1 cannot exceed the value of 2/3 for all separable states. Formally, we define a quantity

$$R_{[N]} = \sum_{k=1}^{N} F_k, \tag{4.10}$$

where $F_k$ is the outcome of the $k^{\text{th}}$ pair correlation measurement.
The cost function is defined as

$$F_{[N]} = \begin{cases} 1, & R_{[N]} \geq (\frac{2}{3} + \delta)N; \\ 0, & R_{[N]} < (\frac{2}{3} + \delta)N, \end{cases} \tag{4.11}$$

where $\delta > 0$ is some constant that we keep at the moment as a free parameter. In other words, we associate "success" to the run if the number of local successes $F_k$ exceeds certain threshold of $(\frac{2}{3} + \delta)N$. The overall probability of success reads

$$P_\rho[F_{[N]} = 1] = P_\rho\left[F_1 + \cdots + F_N \geq \left(\frac{2}{3} + \delta\right) N\right]. \tag{4.12}$$

From (4.12), we see that our target quantity is the probability that the sum of random variables $F_1 + \cdots + F_N$ exceeds the value of $(\frac{2}{3} + \delta)N$. In the case of a product state

$$\rho_{prod} = \rho_1 \otimes \cdots \otimes \rho_{2N}, \tag{4.13}$$

$F_k$'s become independent random variables with

$$\langle F_k \rangle \leq \frac{2}{3}. \tag{4.14}$$

For such a case the bound on (4.12) is well studied in classical probability theory and the results are known as the Chernoff bounds [82]. We will show in the Appendix A that

$$P_{\rho_{prod}}[F_{[N]} = 1] \leq e^{-D(\frac{2}{3}+\delta||\frac{2}{3})N}, \tag{4.15}$$

where

$$D(x||y) = x \log \frac{x}{y} + (1-x) \log \frac{1-x}{1-y} \geq 0 \tag{4.16}$$

is the Kullback–Leibler divergence. Moreover, the bound (4.15) holds for all separable states, as they are just mixtures of product states. For all $\delta > 0$, the probability of success vanishes exponentially fast in $N$. The procedure becomes even more convenient as we don't have to set $\delta$ in advance. This enables us to calculate $\delta$ directly from the experimental data as deviation of sum of obtained results $F_1, F_2, \ldots F_N$ from $2N/3$:

$$\delta = (F_1 + \cdots + F_N)/N - 2/3, \tag{4.17}$$

which implies bound on probability of success for all separable states (4.15).

Contrarily, in the case of $N$ singlets $|\psi_0\rangle = |\psi^-\rangle^{\otimes N}$, we obtain $F_k = 1$ deterministically, therefore we get $\delta = 1/3$. The bound (4.15) becomes

$$P_{\rho_{sep}}[F_{[N]} = 1] \leq \left(\frac{2}{3}\right)^N. \tag{4.18}$$

If $N$ is large enough, a single copy of $|\psi_0\rangle$ is sufficient to certify entanglement with high probability. Some numeric examples should illustrate these probabilities. If we want to certify entanglement in a single-shot experiment with a probability of at least 95%, we need the minimal number of pairs $N_{min} = 8$, which is exceptionally low. Namely, certification of entanglement with minimal probability of 95% is equivalent to the fact that no separable state can achieve a probability of success higher than 5%.

In our example, we demonstrate the implementation of the standard detection of entanglement based on the witness operator using our framework. Conventionally, we are dealing with witness operator $W = \frac{1}{3}(A + B + C)$, where measurements $A$, $B$ and $C$ are performed in three separate experiments. For each experiment, we have to use an i.i.d. ensemble consisting of $N$ qubit pairs $\rho_{12}^{\otimes N}$ to estimate the mean values $\langle A\rangle$, $\langle B\rangle$ and $\langle C\rangle$ properly. However, it is almost impossible to work with the i.i.d. assumption (experimental preparation of an enormous number of identical copies of quantum state) from the practical point of view. Moreover, as the number of experimental runs increases, the statistical analysis becomes highly non-trivial, rendering the verification procedure operationally challenging.
Furthermore, in the case of having a small number of singlet pairs, it is not clear how to conduct the detection scheme. Let us take a situation where only $N = 8$ pairs of qubits are available. The main issue is how to group these pairs and perform the corresponding measurements. We may use the first two pairs to measure $A$, the

second three to measure $B$, and the last three for the measurement of $C$. However, product state $(|x+\rangle|x-\rangle)^{\otimes 2}(|y+\rangle|y-\rangle)^{\otimes 3}(|z+\rangle|z-\rangle)^{\otimes 3}$ gives exactly the same result as the state $|\psi^-\rangle^{\otimes 8}$ if the order of measurements is known and fixed in advance. Therefore, we can not conclude the presence of entanglement or we may even claim its presence falsely. Certainly, a correct statement requires appropriate statistical analysis. On the other side, one of the main ingredients of our framework is the random sampling of measurement settings, which equips us with a simple tool to analyze the errors and confidence intervals through the probability of success. Thus, there is a clear distinction between the state $|\psi^-\rangle^{\otimes 8}$ and the product state mentioned above, since the latter only has the chance of $(2/3)^8 \approx 0.039$ to reveal the result $F_1 + \cdots + F_8 = 8$.

Finally, we would like to indicate that the scheme examined here can be seen as a method for translating entanglement witnesses into the "single-copy" scenario, in order to achieve more resource-efficient entanglement detection (as compared to the witness method) without assuming the i.i.d. assumption (*a priori*). In this respect, one may object that our method still requires many copies for reliable detection (i.e. $N$ copies of $k$-partite state $|\psi\rangle$ folded into a single multipartite copy $|\psi\rangle^{\otimes N}$ ). Nevertheless, in the next examples, we will unambiguously show that, indeed, one can certify entanglement with a high confidence by measuring only a single copy of the provided quantum state.

### 4.1.3 Example of cluster states

Another example we present in this thesis is that of cluster states [78]. In contrast to the previous example of $k$-producible states, cluster states contain genuine multipartite entanglement [83] and they are known to be a universal resource for measurement-based quantum computation [78]. Here, we will clarify how the single-copy detection scheme operates for the linear cluster states (LCS). In the end we will just briefly discuss the straightforward generalization to higher dimensions. The $N$-qubit LCS is uniquely defined by the set of $2^N$ stabilizers, i.e.

$$G_{q_1 \ldots q_N}|LCS\rangle = G_1^{q_1} \ldots G_N^{q_N}|LCS\rangle = +1|LCS\rangle, \tag{4.19}$$

where $G_k = Z_{k-1}X_kZ_{k+1}$ and $q_k = 0, 1$. Here $\{X_k, Y_k, Z_k\}$ is the set of standard Pauli matrices acting on $k^{\text{th}}$ qubit and, for simplicity, we have chosen the cluster state with periodic boundaries, i.e. $Z_{N+1} \stackrel{\text{def}}{=} Z_1$ and $X_{N+1} \stackrel{\text{def}}{=} X_1$. We are dealing with the set of $\{X, Y, Z\}$ measurement settings for each qubit, having the measurements performed in the eigenbasis of Pauli operators, with the set of binary outcomes

$i = 0, 1$. For simplicity, we analyze a small cluster of four qubits, let say $\{1, 2, 3, 4\}$ with the corresponding stabilizers

$$G_2 = Z_1 X_2 Z_3, \;\; G_3 = Z_2 X_3 Z_4 \;\text{ and }\; G_2 G_3 = Z_1 Y_2 Y_3 Z_4 \tag{4.20}$$

acting exclusively on it. Even though these three stabilizers are commutative, they are not locally compatible; meaning that all three of them can not be measured simultaneously with local measurement. Therefore, for no product (separable) state, all three observables can take the same value, $G_2 = G_3 = G_2 G_3 = +1$, simultaneously. As a consequence, if we randomly chose to measure one of the stabilizers, with probability $1/3$, there is only a chance of $2/3$ to get the result $+1$, for all separable inputs. This is the crucial observation that empowers our detection method to work. Our main goal is to show that if we pick a random partition of the set of $N$ qubits into 4-qubit clusters and then measure one of the corresponding stabilizers randomly on each of them, the relative frequency of the outcome $+1$ can not substantially surpass the value of $2/3$. Formally speaking, we start by introducing partitions of $N$ qubits into 4-qubit clusters $\{c_{t_1}, c_{t_2}, \dots c_{t_L}\}$, where $c_{t_s}$ is the cluster consisting of the sequence of four qubits

$$c_{t_s} = \{t_s, t_s + 1, t_s + 2, t_s + 3\}. \tag{4.21}$$

Moreover, border qubits in each cluster are always measured in the $Z$ basis when measuring the corresponding stabilizer. Thus, we shall take into account possible overlap between neighbouring clusters on border qubits. More specifically, we say that the partition is regular if the neighbouring clusters overlap on at most one (border) qubit, i.e. $t_{s+1} - t_s \geq 3$.
For example, the partition $\{\dots, \{7, 8, 9, 10\}, \{10, 11, 12, 13\}, \dots\}$ is considered regular, whereas $\{\dots, \{7, 8, 9, 10\}, \{9, 10, 11, 12\}, \dots\}$ is irregular, as the two clusters in partition overlap on qubits 9 and 10. The general method for partitioning and a few simple examples are presented in the Appendix A. The set of all regular partitions of size $L$ is denoted by $\mathcal{C}_L$. We consider $L$ being large, as well as the number of qubits and, at the same time, we take $L$ such that the set $\mathcal{C}_L$ is large. We establish the cost function $F_{[N]}$ using the clusters in the given partition. Namely, for every cluster $c_{t_s}$ in the partition we associate three stabilizers:

$$G_{t_s+1} = Z_{t_s} X_{t_s+1} Z_{t_s+2}, \tag{4.22}$$

$$G_{t_s+2} = Z_{t_s+1} X_{t_s+2} Z_{t_s+3} \tag{4.23}$$

$$G_{t_s+1, t_s+2} = G_{t_s+1} G_{t_s+2} = Z_{t_s} Y_{t_s+1} Y_{t_s+2} Z_{t_s+3}. \tag{4.24}$$

To each of them we associate three projectors

$$A_{t_s} = \frac{\mathbb{1} + G_{t_s+1}}{2}, \tag{4.25}$$

$$B_{t_s} = \frac{\mathbb{1} + G_{t_s+2}}{2}, \tag{4.26}$$

$$C_{t_s} = \frac{\mathbb{1} + G_{t_s+1}G_{t_s+2}}{2}, \tag{4.27}$$

that project on the $+1$ outcome. We identify the following measurement settings with each projector

$$\{ZXZZ, ZZXZ, ZYYZ\}, \tag{4.28}$$

and we assign "success" to the cluster measurement only if the outcome $+1$ is obtained. We define the following local cost function for each cluster

$$F_s = F_m^{i_1 i_2 i_3 i_4} = \frac{1}{2} + \frac{1}{2} \begin{cases} (-1)^{i_1+i_2+i_3}, & m = ZXZZ; \\ (-1)^{i_2+i_3+i_4}, & m = ZZXZ; \\ (-1)^{i_1+i_2+i_3+i_4}, & m = ZYYZ, \end{cases} \tag{4.29}$$

where $s = 1 \dots L$. Finally, for a given partition $\{c_{t_1}, c_{t_2}, \dots, c_{t_L}\}$ the overall cost function is represented in the following way

$$F_{[N]} = \begin{cases} 1, & F_1 + \dots + F_L \geq (\frac{2}{3} + \delta)L; \\ 0, & F_1 + \dots + F_L < (\frac{2}{3} + \delta)L, \end{cases} \tag{4.30}$$

where $\delta > 0$ is some constant that we keep at the moment as a free parameter. In other words, we associate the "success" to the run if the number of local successes exceeds a certain threshold of $(\frac{2}{3} + \delta)L$.

Having defined all we need, our detection procedure goes as follows. First of all, a particular partition $\{c_{t_1}, c_{t_2}, \dots, c_{t_L}\}$ is randomly generated from the set $\mathcal{C}_L$ (with probability $1/|\mathcal{C}_L|$). Then, for each cluster in the partition we pick with probability $1/3$ one setting from the set (4.28) and perform the corresponding measurement. The experimental run gives the sequence of results $F_1, F_2, \dots, F_L$ from which we evaluate $F_{[N]}$ by using (4.30). The next step is to prove that as the number of qubits grows, the probability of success goes to zero exponentially fast for all separable states. Firstly, for a fixed partition $\{c_{t_1}, c_{t_2}, \dots, c_{t_L}\}$ it is clear that product states do not meet $F_s = 1$ for all three settings $\{ZXZZ, ZZXZ, ZYYZ\}$, since $XZ, ZX, YY$ are locally incompatible on a second and third qubit. Therefore, if the settings are uniformly distributed, with probability of $1/3$, one can straightforwardly derrive the

probability of success for individual clusters

$$P_{\rho_{prod}}[F_s = 1] \;\; = \;\; \langle F_s \rangle = \frac{1}{3}\langle A_{t_s} + B_{t_s} + C_{t_s} \rangle \leq \frac{2}{3}, \tag{4.31}$$

for all product states $\rho_{prod} = \rho_1 \otimes \cdots \otimes \rho_N$. Additionally, if the input state is a product state, the local cost functions $F_s$ can be treated as independent binary ("0/1") random variables with $\langle F_s \rangle \leq 2/3$ for all $s = 1 \ldots L$. The overall probability of success reads

$$P_{\rho_{prod}}[F_{[N]} = 1] = P_{\rho_{prod}}\left[F_1 + \cdots + F_L \geq \left(\frac{2}{3} + \delta\right) L\right], \tag{4.32}$$

which is the probability that the sum of independent random variables $F_1 + \cdots + F_L$ exceeds the value of $(\frac{2}{3} + \delta)L$. As $\langle F_s \rangle \leq 2/3$ we expect that the sum $F_1 + \cdots + F_L$ cannot exceed $2/3L$ significantly. Similar to the previous example (of singlet state), the Chernoff bound holds (see Appendix A for the proof), i.e.

$$P_{\rho_{prod}}[F_{[N]} = 1] \leq e^{-D(\frac{2}{3}+\delta||\frac{2}{3})L}, \tag{4.33}$$

where $D(x||y)$ is the Kullback-Leibler divergence. Furthermore, if the bound holds for all product states, it also holds for their mixtures, i.e. it holds for all separable states. Thus, as long as $L$ grows with $N$, for example, we can set $L = [N/5]$, where $[.]$ denotes the integer part, the probability of success vanishes exponentially fast, for all $\delta > 0$. As before, we do not have to fix $\delta$ in advance. Once the experiment has been performed, we can calculate directly from the experimental data $F_1, F_2, \ldots$ how much the sum of results deviates from $2L/3$, i.e. we set

$$\delta = (F_1 + \cdots + F_L)/L - 2/3, \tag{4.34}$$

and consequently calculate the bound on probability of success for separable states by using (4.33). For the case of cluster state preparation $|LCS\rangle$, each local cost function $F_s = 1$ deterministically, thus we get $\delta = 1/3$. The bound (4.33) reduces to

$$P_{\rho_{sep}}[F_{[N]} = 1] \leq \left(\frac{2}{3}\right)^L. \tag{4.35}$$

If the number of qubits is sufficiently large, even a single-copy of LCS suffices to certify the presence of entanglement with high probability. For example, if we want to have a detection probability of at least 95%, i.e. we want to be sure that no separable state has a probability of success more than 5%, in a single-shot experiment, we get the minimal number of clusters $L_{min} = 8$. The lowest number of qubits with

such support is $N = 24$. Nevertheless, in such a case the set of all partitions $\mathcal{C}_L$ reduces to three only, and for a reason explained below, the method rather certifies the presence of the entanglement blocks with high confidence. For that reason, one may want to have $|\mathcal{C}_L|$ significantly larger. For example, already $N = 25$ has $|\mathcal{C}_L| = 25$, for $N = 26$ we get $|\mathcal{C}_L| = 117$ etc. Thus $N \approx 30$ shall already suffice to certify the large-scale entanglement with 95% within the single-copy scenario.

This scheme can be used not only to detect entanglement, it can be also used to certify the presence of LCS, which will be used for nonlocality detection. To see this, note that $P_\rho[F_{[N]} = 1] = \mathrm{Tr}\,\rho\Pi$, where

$$\Pi = \frac{1}{|\mathcal{C}_L|} \sum_{\{c_{t_1},\ldots,c_{t_L}\}\in\mathcal{C}_L} \prod_{s=1}^{L} \frac{1}{3}(A_{t_s} + B_{t_s} + C_{t_s}). \tag{4.36}$$

Clearly LCS is the eigenstate $\Pi|LCS\rangle = 1|LCS\rangle$ for the maximal eigenvalue. Now, the operator $\Pi$ can be expanded in terms of stabilizers $G_{q_1\ldots q_N}$ defined by the equation (4.19). If the set $\mathcal{C}_L$ is sufficiently large, the expansion will include all $2^N$ stabilizers. As the LCS is the only state with $G_{q_1\ldots q_N}|LCS\rangle = +1|LCS\rangle$ for all stabilizers, we conclude that LCS is a unique eigenstate of $\Pi$ for eigenvalue 1. Therefore, the LCS state is the only state that achieves maximal probability of success, $P[F_{[N]} = 1] = 1$.

We shall comment briefly on the type of entanglement that the single-copy detection scheme certifies. Firstly, if we want to detect multipartite entanglement, it is essential to set $\mathcal{C}_L$ being large in size. Recall, that the bound (4.33) holds for arbitrary partition from the set $\mathcal{C}_L$ for all separable states. Therefore, if the partition $\{c_{t_1}, \ldots, c_{t_L}\}$ is fixed and known in advance, the bound (4.33) still holds. Nevertheless, for such a case, the following 4-producible state $|\phi\rangle = |\psi\rangle_1|\psi\rangle_2 \ldots |\psi\rangle_L$, where $|\psi\rangle_s$ is the common eigenstate for all three projectors $A_{t_s}$, $B_{t_s}$ and $C_{t_s}$ for eigenvalue 1, reveals $F_s = 1$ deterministically for every cluster. As a consequence, we have $P[F_{[N]} = 1] = 1$ for $|\phi\rangle$ being the input state. Quantum state $|\phi\rangle$ contains localized entanglement on individual clusters (blocks of entanglement). To prevent $|\phi\rangle$ maximizing the probability of success, a random choice of partition from a large set $\mathcal{C}_L$ is necessary. For example, already including additional partition $\{c_{t_1+1}, \ldots, c_{t_L+1}\}$ obtained by shifting one qubit to the right, prevents $|\phi\rangle$ to be the common eigenstate of $A_{t_s}$, $B_{t_s}$, $C_{t_s}$ and $A_{t_s+1}$, $B_{t_s+1}$, $C_{t_s+1}$. Contrarily, if we want $F_{[N]} = 1$ deterministically for both partitions, we need to have entanglement between neighbouring clusters. To conclude, if we take all partitions of large $\mathcal{C}_L$, the only way to have non-trivial probability of success is to input delocalized entanglement.

Finally, let us briefly explain the generalization to the higher dimensional case. Take an example of a 2D cluster state, known to be universal for quantum computation [78]. Here, one can introduce partitions into $4 \times 4$ qubit clusters with the corresponding stabilizer projectors (in analogy to $A_{t_s}$, $B_{t_s}$ and $C_{t_s}$ for LCS) and define the local cost functions. In complete analogy to the 1D case, the 2D detection scheme consists of drawing a random partition followed by a random measurement of local projectors on individual clusters. The separable bound similar to (4.33) can be derived. On the other hand, if the 2D cluster state has been prepared, the probability of success is 1.

### 4.1.4 Example of ground states of local Hamiltonians

One of the reasons why single-copy entanglement detection works for cluster states is the robustness of entanglement to local perturbations. For instance, if we measure one or even a group of localized qubits in the cluster state, there is still entanglement between the remaining qubits. This is a different situation in comparison with "fragile" entangled states, such as GHZ (Greenberger-Horne-Zeilinger)-like states where entanglement is very sensitive, e.g. measurement of a single qubit will destroy entanglement completely. Therefore, we expect that "robust states" are amendable to single-copy verification. It is presumed that ground states of local Hamiltonians share this property (robustness of entanglement) [84]; therefore, we can expect that it is feasible to apply the single-copy verification.

Consider a $L$-local Hamiltonian on some graph of $N$ particles

$$H = \sum_{k=1}^{N} H^{(k)}, \tag{4.37}$$

where $H^{(k)}$ acts on at most $L$ subsystems. Here $L$ is fixed and independent of $N$. For simplicity, we take the number of local terms $H^{(k)}$ being equal to the number of particles $N$ [63], as in the most physical situations. In general, we could extend our analysis to the case where the number of local terms grows as a polynomial function of $N$. Nevertheless, the detection scheme will work the same way. Let $|\psi_0\rangle$ is the ground state $H|\psi_0\rangle = N\epsilon_0|\psi_0\rangle$, where $E_0 = N\epsilon_0$ is the ground-state energy. We are working with Hamiltonians that exhibit the so-called entanglement gap [35]:

$$g_E = \epsilon_s - \epsilon_0 > 0, \tag{4.38}$$

where

$$\epsilon_s = \frac{1}{N} \min_{\rho_{sep}} \mathrm{Tr}\, H\rho_{sep} \tag{4.39}$$

is the minimal obtainable energy per particle by a separable state. Moreover, we assume $g_E$ to be finite and non-zero in the thermodynamical limit, i.e.

$$0 < \lim_{N\to\infty} g_E < +\infty. \tag{4.40}$$

To summarize, our target objects are Hamiltonians for which the expected value of energy $\langle H\rangle$ can serve as the entanglement witness. For all separable states, we have $\langle H\rangle \geq N\epsilon_s$, whereas at least the ground state violates this bound. Our goal is to establish a general scheme convenient for arbitrary local Hamiltonian. Therefore, we work with a set of tomographically complete measurements for each particle. In the case of qubits, a logical choice is the three complementary measurements defined by $X$, $Y$ and $Z$ Pauli operators. Thus, the set of measurement operators $E^{(k)}_{mi}$ forms a complete basis in the space of observables, that is, any observable $A^{(k)}$ acting on $k^{\text{th}}$ subsystem can be decomposed as

$$A^{(k)} = \sum_{mi} a_{mi} E^{(k)}_{mi}. \tag{4.41}$$

Here $m = 1 \ldots M$ and $i = 1 \ldots D$, where $M$ represents the number of settings and $D$ represents the number of outcomes. To make the notation shorter, we introduce a new variable $x_k = (m_k, i_k)$ which identifies a pair of measurement setting and outcome, hence $E^{(k)}_{x_k}$ refers to $E^{(k)}_{m_k i_k}$. Note that $\sum_{x_k} E^{(k)}_{x_k} = M\mathbb{1}^{(k)}$.

As we assumed before, for a given local Hamiltonian $H = \sum_{k=1}^{N} H^{(k)}$, operator $H^{(k)}$ acts on at most $L$ neighbouring subsystems (neighbours of $k$ including $k$ itself). It is convenient to introduce the $N\times L$ "neighbouring" matrix $n_{k,l}$, where $n_{k,1}, \ldots n_{k,L}$ is a sequence of integers labeling all the neighbours of $k$th subsystem (including $k$th subsystem itself) on which the local operator $H^{(k)}$ acts. The "neighbouring" matrix can be seen as the list of neighbourhoods $(\mathcal{N}(1), \ldots, \mathcal{N}(N))$, where $\mathcal{N}(k)$ denotes the set of all neighbours of $k$. For example, the notation $\{n_{3,1}, n_{3,2}, n_{3,3}\} = \{2, 3, 4\}$ suggests that $H^{(3)}$ acts on subsystems $2, 3$ and $4$. Using the fact that the set of measurement operators is tomographically complete, we decompose each $H^{(k)}$ into the sum of products of local measurement operators

$$H^{(k)} = \sum_{x_1 \ldots x_L} h^{(k)}_{x_1 \ldots x_L} E^{(n_{k,1})}_{x_1} \ldots E^{(n_{k,L})}_{x_L}. \tag{4.42}$$

The operator $H^{(k)}$ can be completely described with the tensor $h^{(k)} = h^{(k)}_{x_1 \ldots x_L}$. Si-

milarly, the full Hamiltonian $H$ reads

$$H = \sum_{x_1 \ldots x_N} H_{x_1 \ldots x_N} E^{(1)}_{x_1} \ldots E^{(N)}_{x_N}, \tag{4.43}$$

where we set

$$M^{N-L} H_{x_1 \ldots x_N} = \sum_{k=1}^{N} h^{(k)}_{x_{n_{k,1}} \ldots x_{n_{k,L}}}. \tag{4.44}$$

The factor $M^{N-L}$ comes because of the normalization $\sum_x E_x = M\mathbb{1}$.

We can now build up the detection procedure. First of all, we randomly select measurement settings for individual subsystems, each with probability $1/M$, and generate the sequence $\{m_1, \ldots, m_N\}$. Then, the measurements are performed on local subsystems and the set of outcomes $\{i_1, \ldots, i_N\}$ is obtained. Equivalently, we say that we generate the sequence of random variables $\{x_1, \ldots, x_N\}$, where $x_k = (m_k, i_k)$. Now, we want to characterize the adequate cost function $F_{[N]}$, so we define

$$H_{[N]} = M^N H_{x_1 \ldots x_N} = M^L \sum_{k=1}^{N} h^{(k)}. \tag{4.45}$$

A straightforward inspection shows $\langle H_{[N]} \rangle = \mathrm{Tr}\, \rho H = \langle H \rangle$, thus using the classical random variable $H_{[N]}$ we can extract the mean value of Hamiltonian $\langle H \rangle$. Since $\langle H \rangle \geq N\epsilon_s$ holds for all separable states, it is natural to chose the following cost function

$$F_{[N]} = \begin{cases} 1, & H_{[N]} \leq N(\epsilon_s - \delta); \\ 0, & H_{[N]} > N(\epsilon_s - \delta), \end{cases} \tag{4.46}$$

where $0 < \delta < \epsilon_s - \epsilon_0 = g_E$ is constant. At the moment we keep $\delta$ as a free parameter. Since the random variable $H_{[N]}$ fully captures Hamiltonian properties, we expect that $H[N]$ will not significantly precede the separable bound $N\epsilon_s$ in a single-shot experiment, assuming that $N$ is large. In the Appendix A we provide detailed proof that for all separable states $\rho_{sep}$ the following bound holds

$$P_{\rho_{sep}}[F_{[N]} = 1] \;\; \leq \;\; \exp\left[-N\kappa^2\delta^2\right], \tag{4.47}$$

where $\kappa > 0$ is constant. Thus, for all separable inputs, the probability of success vanishes exponentially fast with $N$. On the other side, if the ground state $|\psi_0\rangle$ is prepared, then in the thermodynamical limit, the probability of success reaches 1

$$P_{\psi_0}[F_{[N]} = 1] \geq 1 - \frac{\beta^2}{N(g_E - \delta)^2}, \tag{4.48}$$

where $\beta > 0$ is constant. The complete derivation of (4.48) is given in the Appendix A as well. Particularly, if $N$ is sufficiently large, the probability of success reaches 1.

Here, we should point out several things. Firstly, we could incorporate the previous example of cluster states in the present scheme, as cluster states can be represented as unique ground-states of local Hamiltonians [85]. Nevertheless, previously explained detection scheme for cluster states is more efficient for the two following reasons. Firstly, the bound (4.33) is tighter than (4.47), and secondly, the probability of success takes value 1 for the cluster-state input, in contrast to (4.48) which reaches 1 asymptotically. This also means, that the detection scheme for ground states of local Hamiltonians can be optimized, in a sense that for a particular Hamiltonian one can find a more resource-efficient method and get better bounds than (4.33) and (4.47). The ground-state detection technique, on the other hand, has some practical benefits. In particular, one of the key elements for detection is the use of a tomographically complete set of measurements. In principle, a single informationally complete POVM (ICPOVM) [86] can be used to replace them. More precisely, rather than using a set of tomographically complete measurements, it is possible to use a single POVM with $E_i$ measurement operators forming a complete basis in the observable space. Thus, an $N$-partite Hamiltonian can be expressed as

$$H = \sum_{i_1 \dots i_N = 1}^{D} h_{i_1 \dots i_N} E_{i_1}^{(1)} \dots E_{i_N}^{(N)}, \tag{4.49}$$

where $i_k = 1 \dots D$ stands for the measurement outcome. The properties of Hamiltonian are completely captured by the classical random variable $H_{[N]} = h_{i_1 \dots i_N}$, which is the function of the measurement outcomes $i_1, \dots, i_N$. Here, we do not apply random sampling of measurement settings; there is only one measurement (ICPOVM) for each particle. The variable $H_{[N]}$ is calculated from the set of measurement outcomes $\{i_1, \dots, i_N\}$. The cost function is defined as (4.46), and derivation of bounds (4.33) and (4.47) is essentially the same as before. Formally, both methods are equivalent. Nevertheless, the practical advantage of using ICPOVM compared to a random sampling of measurement settings can be significant in some instances, depending on the physical implementation of POVM. For example, if ICPOVM is implemented through the use of additional degrees of freedom, the same single measurement setting applies to each local subsystem. One such example is the case of single-photons by combining the path and polarization degree of freedom [87]. This is very useful when dealing with large-scale quantum systems for which it is necessary to accomplish complete manipulation and addressability of individual particles.

### 4.1.5 Tolerance to noise

Now, we will analyze the effects of noise on probabilistic entanglement detection. Consider a $N$-partite target state $\rho_0$ with the probability of success $p_0 > 0$, i.e. there is a chance of $p_0$ to get success (detect entanglement) in a single experimental run if the state $\rho_0$ has been prepared. In practice, one needs in average $1/p_0$ copies of $\rho_0$ in order to get "success", i.e. to detect entanglement. In addition, let the separable bound (4.1) hold, i.e. the probability of success for all separable inputs is exponentially small in $N$. We consider a mixture

$$\rho = \lambda\rho_{sep} + (1-\lambda)\rho_0, \tag{4.50}$$

where $\rho_{sep}$ is an arbitrary separable state and parameter $0 < \lambda < 1$ quantifies the amount of noise. Operationally, the state $\rho$ can be prepared by using a probabilistic source that emits either $\rho_{sep}$ with probability $\lambda$ or $\rho_0$ with probability $1-\lambda$ every individual experimental run. Of course, this does not have to be the actual experimental situation; for example, $\rho$ can be the marginal state of a larger (entangled) state. Nevertheless, even if so, the probabilities for the measurement outcomes are precisely the same in both scenarios.

In that case, the overall probability of success is a mixture of probabilities, i.e.

$$P_\rho = \lambda P_{\rho_{sep}} + (1-\lambda)P_{\rho_0} \approx (1-\lambda)p_0, \tag{4.51}$$

as long as $(1-\lambda)p_0$ is significantly larger than $P_{\rho_{sep}} = O(\exp[-Nc])$. This implies that noise impacts detection by suppressing the probability of success by the factor $1-\lambda$, for any kind of separable noise (i.e., represented by a separable state). Therefore, one requires in average $\frac{1}{(1-\lambda)p_0}$ experimental runs in order to confirm the presence of entanglement. This represents a strong resistance to noise if $(1-\lambda)p_0$ is not exponentially small in $N$. For example, if we consider $(1-\lambda)p_0 > 0$ constant and independent of $N$, then entanglement can be verified with the fixed cost, in terms of the number of resources.

On the other side, the situation with standard detection methods is very different. Generally, a witness method tolerates noise bellow a certain critical point, i.e. $\lambda < \lambda_c$. Thus, if noise passes the threshold, even if an infinite number of resources are accessible, the scheme does not work.

In this respect, let us examine the example of a linear cluster state mixed with the white noise $\rho_{LCS} = \lambda\mathbb{1}/2^N + (1-\lambda)|LCS\rangle\langle LCS|$, where $|LCS\rangle$ is the linear

cluster state defined by the equation (5.4). The following set of witness operators can detect the existence of entanglement [88]:

$$W_k = \mathbb{1} - G_k - G_{k+1}, \tag{4.52}$$

with $\langle W_k \rangle_{sep} \geq 0$ for all separable states. We have $\langle W_k \rangle_{LCS} = -1$, for the linear cluster state, so the witness detects entanglement for $\lambda \leq 1/2$. On the other hand (see subsection **Example of cluster states**), if our detection framework is implemented, the separable bound is provided by the equation (4.33), where $\delta > 0$ is a free parameter. As before, we set $\delta = 1/3$ and we get $P_{sep} \leq (\frac{2}{3})^L$ (see equation (4.35)), where $L$ is the size of partitions. For $N$ (and consequently $L$) being large enough, $P_{sep} \approx 0$ is negligible. On the contrary, if the state $\rho_{LCS}$ is prepared, the probability of success is lower bounded by

$$P_\rho = \lambda P_{\mathbb{1}/2^N} + (1-\lambda) P_{|LCS\rangle} \geq 1 - \lambda, \tag{4.53}$$

where we used $P_{|LCS\rangle} = 1$. This means that one needs $1/(1-\lambda)$ copies on average in order to get success. For example, if we set $\lambda = 1/3$, we need three copies on average to certify entanglement, while in such a case, the witness (4.52) will not detect entanglement even an infinite number of copies is supplied.

## 4.2 Translation of entanglement witnesses to probabilistic procedure

As we have already emphasized, verifying quantum entanglement is an essential task to scale up quantum technologies. Although progressively more efficient methods have been developed, most of these focus solely on minimizing the number of measurement settings. However, in each measurement setting these techniques still require many measurements to be made on the same quantum state (i.e. many detection events). Moreover, typical approaches require each experimental run to be identical and independent, meaning that source drift can lead to unreliable results.

Our main goal is to extend previously presented "single-shot" entanglement verification technique [76] for practical applications. In our work, we show that any entanglement witness can be translated into a probabilistic verification protocol that only requires a few detection events, and does not require the assumption of identical experimental runs. Moreover, we demonstrate the applicability of our new protocol by verifying entanglement in a photonic six-qubit cluster state [89]. The proof-of-

principle experimental demonstration has been performed in the group of Prof. Dr. Philip Walther at University of Vienna. The state was generated with three state-of-the-art photon-pair sources operating at telecommunication wavelengths. We found that only 20 copies of the quantum state are needed to certify some entanglement with at least 99.74 % confidence, and we can even show that the state possesses genuine six-qubit entanglement using a mere 112 copies of the quantum state.

By combining our novel theoretical protocol, which will be explained in details throughout this chapter, with an advanced experimental demonstration, we achieve a dramatic reduction of resources. Our technique works for all physical platforms, and thus, we believe that it will become a widely-used standard method to certify the presence of entanglement.

### 4.2.1 Description of the framework

Let us assume we own a quantum state previously prepared in the laboratory, and we want to check whether entanglement is present in it. One possible way to certify the presence of entanglement is by using the standard witness-based approach. That means one should measure the mean value of the witness operator $W$ and inspect if it is smaller or larger than zero. As we said before, $\langle W \rangle \geq 0$ for any separable state $\rho_{sep}$, where $\langle W \rangle = \mathrm{Tr}(W\rho_{sep})$. Thus, any state leading to the mean value less than zero necessarily contains entanglement. However, measuring the mean value of the witness operator requires many copies of a quantum state. As a consequence, these techniques are not reliable when a few copies are available. Furthermore, operator $W$ is not locally accessible in general; one has to decompose it into the sum of local observables $W_k$'s as $W = \sum_{k=1}^{L} W_k$, where each $W_k$ needs to be measured in a separate experimental run, requiring one to estimate several mean values and therefore demanding even more copies. Having a limited number of copies $N$, it is necessary to use $L$ independent measurement settings and ensure that the source provides precisely the same copy of the quantum state for each individual detection event. Furthermore, as we will see in what follows, the number $L$ of experimental runs can exceed the number of available copies $N$, which makes the procedure logically impossible. On a top of that, the *i.i.d.* assumption is hard to fulfil in practice due to various imperfections and lack of control, such as the source drift. By using a probabilistic framework for detecting entanglement, we overcome both of these challenges. More precisely, our protocol is based on a set $\mathcal{M} = \{M_1, M_2, ..., M_L\}$ of binary local multi-qubit observables, which can be derived for any entanglement witness. Each $M_k$ (with $k = 1, ..., L$) returns a binary

outcome $m_k = 1, 0$, which is associated with the success or failure, respectively. The procedure consists in randomly drawing $N$ times from the set $\mathcal{M}$ the measurements $M_k$'s, each with some probability $\pi_k$, and applying them to the quantum state, thus obtaining the outcomes $m_k$'s. The set $\mathcal{M}$ is tailored such that the probability of obtaining success, i.e. to get $m_k = 1$ for a randomly chosen $M_k$, for any separable state is upper bounded by a certain value $p_s < 1$, that we call *separable bound*. On the other hand, if a certain entangled state, target state has been prepared, then the probability of success is maximized to $p_e$. Quantity $p_e$ is called *entanglement value*. The entanglement value $p_e$ is strictly greater than the separable bound $p_s$, i.e. the difference $\delta_0 = p_e - p_s > 0$. We now randomly sample $N$ times from the set $\mathcal{M}$ and apply the drawn measurements $M_k$'s to obtain the sequence of corresponding outcomes $m_k$'s. For any separable input, we expect to get at best around $Np_s$ successes, whereas the target state preparation would reveal around $Np_e$ successful runs. Therefore, for preparations close to the target state, we expect to clearly observe the difference $\approx N(p_e - p_s) > 0$ as the number of runs grows. We have been shown both in [76] and in the previous chapter, that the probability $P(\delta_0)$ to observe $\delta_0 > 0$ for any separable state is upper-bounded with

$$P(\delta_0) \leq e^{-D(p_s+\delta_0||p_s)N}, \tag{4.54}$$

which vanishes exponentially fast with the number of copies $N$. Here

$$D(p_s + \delta_0||p_s) = (p_s + \delta_0) \log \frac{p_s + \delta_0}{p_s} + (1 - (p_s + \delta_0)) \log \frac{1 - (p_s + \delta_0)}{1 - p_s} \tag{4.55}$$

is the Kullback-Leibler divergence. Therefore, the confidence $C(\delta_0)$ of detecting quantum entanglement is lower bounded by $C_{\min}(\delta_0)$:

$$C(\delta_0) = 1 - P(\delta_0) \geq 1 - e^{-D(p_s+\delta_0||p_s)N} = C_{\min}(\delta_0), \tag{4.56}$$

and reaches 1 exponentially fast with number of runs $N$. From expression (4.56) we can estimate the average number of copies $N_{av}$ needed to achieve a certain confidence $C_0$, meaning that for a target state preparation we find

$$N_{av} \leq -K \log(1 - C_0) = N_{\max}, \tag{4.57}$$

which grows logarithmically as $C_0$ approaches unity at the rate of $K = D(p_s + \delta_0||p_s)^{-1}$. In a realistic framework, we can experimentally prepare a certain state $\rho_{exp}$ and assume that the experiment reveals $S$ successful outcomes. The observed

deviation from the separable bound $\delta$ therefore reads

$$\delta = \frac{S}{N} - p_s. \tag{4.58}$$

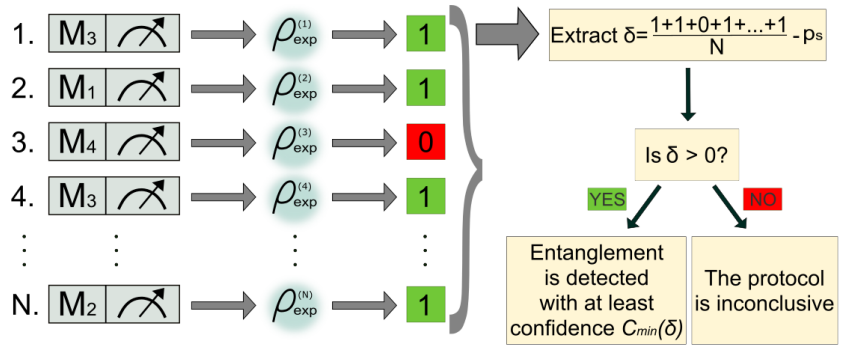


**Figure 4.2:** The measurements $M_k$'s are randomly sampled from the set $\mathcal{M}$ and applied to the experimental state $\rho_{exp}$, which returns binary outcomes 1 or 0 (success or failure, respectively). The superscripts in $\rho_{exp}$ account for possible variations of the state due to experimental imperfections. After $N$ runs, the protocol reveals $S$ successful outcomes. If the deviation $\delta = S/N - p_s > 0$, entanglement is verified in the system with at least confidence $C_{\min}(\delta)$. Otherwise, the protocol is inconclusive.

If $\delta$ holds always positive after using a sufficient number of copies, we can calculate $C_{min}(\delta)$ from expression (4.56). We summarize the presented entanglement detection framework in Figure 4.2.

Additionally, due to a random sampling of the measurement settings, our protocol does not require the *i.i.d.* assumption. This is an essential aspect of our framework as the experimental state is necessarily subjected to fluctuations over time due to experimental conditions such as the source drift. In such cases, other protocols can lead to unsatisfactory results [55, 90], while in our case, we never obtain false positives.

### 4.2.2 Witness translation method

Here, we want to explain the procedure that translates any entanglement witness into our probabilistic scheme. Generally, a witness operator $W$ is normalized such that

$$\langle W \rangle = \mathrm{Tr}(W\rho_s) \geq 0 \tag{4.59}$$

for any separable state $\rho_s$. An equivalent form can be obtained from the equivalence transformation given by

$$W = g_s \mathbb{1} - O, \tag{4.60}$$

where $O$ is an Hermitian operator for which $\langle O \rangle \leq g_s$ holds for any separable state [34]. Now, we make the local decomposition of

$$O = \sum_{k=1}^{q} W_k \tag{4.61}$$

into $q$ settings neccesary to measure $\langle O \rangle$. In the next step we can add a constant term to each local setting $W_k^{'} = W_k + a\mathbb{1}$ such that they become non-negative observables. This transformation leads to the new witness

$$O' = \sum_{k=1}^{q} W_k^{'} = O + aq\mathbb{1}. \tag{4.62}$$

We choose $a \geq 0$ to take the minimal possible value. Having everything considered, we can rewrite the separability condition as

$$\langle O' \rangle = \mathrm{Tr}(O'\rho_s) \leq g_s + aq. \tag{4.63}$$

Our main goal is to test this inequality in practice using our probabilistic framework. Note that this inequality is violated for certain entangled (target) state $\rho_e$, i.e.

$$\mathrm{Tr}(O'\rho_e) = g_e + aq, \tag{4.64}$$

with $g_e - g_s > 0$. We write spectral decomposition of operator $W_k^{'}$ as

$$W_k^{'} = \sum_{s=1}^{\mu_k} \lambda_{ks} M_{ks}, \tag{4.65}$$

where $M_{ks}$ are eigen-projectors, binary observables, with $\lambda_{ks} > 0$ since $W_k$'s are non-negative operators. The number $\mu_k$ counts the non-zero eigenvalues of $W_k^{'}$. Furthermore, we define the constant

$$\tau = \sum_{k=1}^{q} \sum_{s=1}^{\mu_k} \lambda_{ks}. \tag{4.66}$$

Now, we can set-up our verification procedure. As $W_k$'s are local observables, the binary operators $M_{ks}$ are local as well. They constitute the set $\mathcal{M}$ introduced in the previous section, which contains in total $L = \sum_{k=1}^{q} \mu_k$ elements. The probability weights for $M_{ks}$'s are set to $\Pi_{ks} = \lambda_{ks}/\tau$. If the input state is separable state $\rho_s$, the probability to obtain success for a randomly drawn measurement $M_{ks}$ from the set

$\mathcal{M}$ is given by

$$p = \sum_{k=1}^{q} \sum_{s=1}^{\mu_k} \Pi_{ks} \mathrm{Tr}(M_{ks}\rho_s) = \frac{1}{\tau} \sum_{k=1}^{q} \langle W'_k \rangle \leq \frac{1}{\tau}(g_s + aq). \tag{4.67}$$

Therefore, the separable bound is given by

$$p_s = \frac{1}{\tau}(g_s + aq). \tag{4.68}$$

Apparently, if the target state is prepared, we get

$$p_e = \frac{1}{\tau}(g_e + aq) \tag{4.69}$$

with the strict separation $\delta_0 = p_e - p_s = (g_e - g_s)/\tau > 0$. Once we have defined the set $\mathcal{M}$ and found $p_s$, we can apply the protocol illustrated in Fig. 4.2 and obtain the minimum confidence for entanglement detection.

### 4.2.3 Application of the translation framework to graph states

In order to make an illustration of our translation procedure, we will consider the entanglement detection in an $n$-qubit graph state $|G\rangle$ using the witness

$$W = \frac{1}{2}\mathbb{1} - |G\rangle\langle G|, \tag{4.70}$$

for which we have $\langle W \rangle \geq 0$ for any separable state. This witness can be easily transformed to the equivalent one

$$W' = \frac{1}{2}\mathbb{1} + \frac{1}{2}|G\rangle\langle G|, \tag{4.71}$$

for which we obtain

$$\langle W' \rangle \leq 3/4 = p_s \tag{4.72}$$

for any separable state. The graph state can be written in terms of its stabilizers $S_k$'s as

$$|G\rangle\langle G| = \frac{1}{2^n} \sum_{k=1}^{2^n} S_k, \tag{4.73}$$

where the $S_k$'s are certain products of local Pauli observables. Therefore, the new witness reads

$$W' = \frac{1}{2^n} \sum_{k=1}^{2^n} M_k, \tag{4.74}$$

where $M_k = (\mathbb{1} + S_k)/2$ is one of the binary observables needed in our probabilistic protocol. The sampling is uniform, i.e. the probabilities equal $\pi_k = 1/2^n$, over the set of $2^n$ settings defined by stabilizers of the state. As the $S_k$'s stabilize the state, $p_e = 1$ for an ideal graph state and we recall that $p_s = 3/4$ for any separable state. We show that this procedure also leads to an estimate of the fidelity

$$F = \langle G|\rho_{exp}|G\rangle \tag{4.75}$$

between the experimentally generated state $\rho_{exp}$ and the ideal one $\rho_{ideal} = |G\rangle\langle G|$. This is related to the direct fidelity estimation protocol [64].

Given $p_e = p_s + \delta_0$ and $p_s$, we can calculate the average number of copies needed to achieve certain confidence $C_0$ from expression (4.56):

$$N_{av} \leq D(1||3/4)^{-1} \log(1 - C_0) \approx 3.47 \log(1 - C_0). \tag{4.76}$$

Therefore, to achieve the confidence of $C_0 = 0.99$ we need at most $N_{\max} \approx 16$ copies of $|G\rangle$, which is a remarkably low number. Furthermore, this number is independent on the size of the system, i.e. the number of qubits $n$. In this case, the corresponding entanglement witness-based approach would require $2^n$ measurement settings, each of which would demand a large number of copies, whereas our procedure provides reliable detection with the constant overhead. Thus, our method applies even if the number of measurement settings exceeds the number of available copies, which is impossible to achieve when using the standard techniques.

### 4.2.4 Practical application of the framework to six-qubit H shaped cluster state

In this section, we present our first practical application of the developed framework. All experimental details are provided in [89]. Here we will explain the main theoretical points of our work, while experimental results will be briefly commented in the next section.
First of all, we will translate two different six-qubit cluster state witnesses, tailored for target state, into our probabilistic framework. The ideal experimental six-qubit cluster state is

$$\begin{aligned} |Cl_6\rangle =& \frac{1}{2}(|H_1H_2H_3H_4H_5H_6\rangle + |H_1H_2H_3V_4V_5V_6\rangle + \\ & |V_1V_2V_3H_4H_5H_6\rangle - |V_1V_2V_3V_4V_5V_6\rangle), \end{aligned} \tag{4.77}$$

which is equivalent to the quantum state presented in Fig. 4.3 up to local unitary transformations.

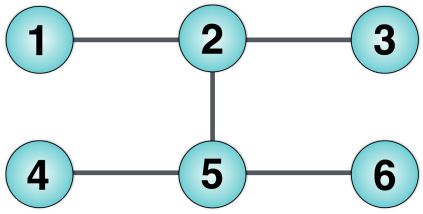


**Figure 4.3:** Each sphere is a qubit prepared in the eigenstate $|+\rangle$ of the Pauli operator $X$, and the solid lines connecting the qubits represent entanglement between them. The entanglement is generated from the application of controlled phase gates between the connected qubits.

It is uniquely defined by the following six generators [91]:

$$\begin{aligned} G_1 &= Z_1Z_2, \quad G_2 = X_1X_2X_3Z_5, \quad G_3 = Z_2Z_3 \\ G_4 &= Z_4Z_5, \quad G_5 = Z_2X_4X_5X_6, \quad G_6 = Z_5Z_6, \end{aligned} \tag{4.78}$$

where $X$, $Y$, $Z$ are labels for standard Pauli operators. From these set, we can construct all products of generators $G_k$'s, and there are in total 64 independent operators, i.e. stabilizers, $G_k|Cl_6\rangle = +1|Cl_6\rangle$ for $k = 1, ..., 64$.

We consider the two following witnesses, designed to detect genuine six-qubit entanglement. First of them is the witness presented in [92] which combines three cluster state generators into one measurement setting, consequently reducing the number of measurement setting from six to two. It is the case of minimal possible number of settings and it is defined as:

$$W_1 = 3\mathbb{1} - 2\left(\prod_{k=1,3,5}\frac{\mathbb{1}+G_k}{2} + \prod_{k=2,4,6}\frac{\mathbb{1}+G_k}{2}\right), \tag{4.79}$$

where the $G_k$'s ($k = 1, ..., 6$) are the experimental generators of the cluster state. The second is the standard witness tailored for our cluster state [83], requiring $2^6 = 64$ measurement settings, is:

$$W_2 = \frac{1}{2}\mathbb{1} - |Cl_6\rangle\langle Cl_6|. \tag{4.80}$$

where $|Cl_6\rangle\langle Cl_6| = \frac{1}{2^6}\sum_{k=1}^{2^6} S_k$, analogous to the previous graph state example.

For both witnesses, we obtain $\langle W_1\rangle$, $\langle W_2\rangle \geq 0$ for any biseparable state. For clarity, we emphasize that biseparable states are the one that does not contain genuine six-qubit entanglement. Therefore, both can be used to distinguish fully

separable and entangled states, and the corresponding separable bounds can be evaluated numerically [93]. We will distinguish two types of separable bound: one is the so-called *biseparable bound* $p_{bs}$, that is directly extractable from our translation protocol and used for detection of genuine six-qubit entanglement; the other one is the *full separability bound* $p_{fs}$, evaluated numerically and used for the detection of some entanglement.

To translate the witness $W_1$ into our procedure, we start with

$$O = 2\left(\prod_{k=1,3,5}\frac{\mathbb{1}+G_k}{2}+\prod_{k=2,4,6}\frac{\mathbb{1}+G_k}{2}\right) \tag{4.81}$$

and $g_s = 3$. The witness $O$ has already the spectral form with

$$M_1 = \prod_{k=1,3,5}\frac{\mathbb{1}+G_k}{2} \tag{4.82}$$

and

$$M_2 = \prod_{k=2,4,6}\frac{\mathbb{1}+G_k}{2} \tag{4.83}$$

with eigenvalues $+1$, therefore $a = 0$. We get $\tau = 4$ and the sampling is uniform from the set $\{M_1, M_2\}$. For the biseparable bound we clearly get $p_{bsW_1} = 3/4$.

For witness $W_2$, the binary observables constituting the set $\mathcal{M}_{W_2}$ are

$$\frac{\mathbb{1}+S_k}{2}, \tag{4.84}$$

where $k = 1, ..., 64$, and the biseparable bound is $p_{bsW_2} = 3/4$ analogous to the example of the graph state discussed in the previous section. The full separability bounds are derived numerically [93] and read $p_{fsW_1} = 9/16$ and $p_{fsW_2} = 5/8$. The entanglement values are $p_{eW_1} = p_{eW_2} = 1$, as the $G_k$'s stabilize the state.

### 4.2.5 Experimental results

The experimental setup used for the cluster state generation and its description are shown in Fig. 4.4.[5] From the experimental point of view, it is relevant to emphasize that the six-qubit cluster state is generated using three photon-pair sources operating at telecommunication wavelength and measurements are perfor-

[5] All figure credits in this Chapter go to Valeria Saggio. They are presented in our recent work [89].

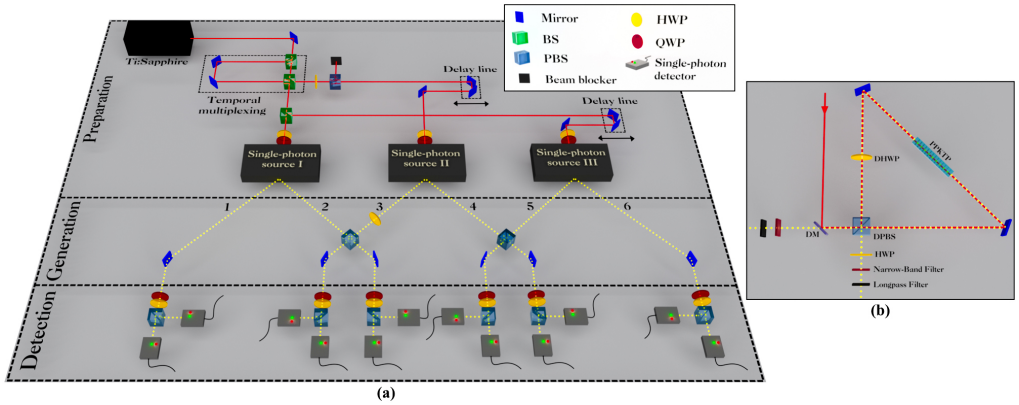


**Figure 4.4:** **(a)** A picosecond Ti:Sapphire laser outputs a beam which is temporally multiplexed to double the repetition rate and reduce contributions from single parametric down-conversion (SPDC) high-order emissions. Two beams equally split at the third beam splitter (BS) pump the first and third single-photon source, while the beam exiting the right output of the second BS passes through a half-wave plate (HWP) and a polarizing beam splitter (PBS) before pumping the second source. In this way, the power of the second source can be tuned. Movable translation stages are used as delay lines for temporal synchronization. An HWP and a QWP are placed along each beam's path to set the needed polarization. Each beam pumps a single-photon source, which emits a polarization-entangled photon pair via type-II SPDC. Two photons from different sources interfere at two PBSs and are then sent to a tomographic system composed of a QWP, an HWP and a PBS. Eventually, photons exiting both outputs of the PBSs reach the single-photon detectors. **(b)** Schematic of a single-photon source. A PPKTP crystal placed into a Sagnac interferometer is used to generate single photons. DM, Dichroic Mirror; DPBS, Dual PBS; DHWP, Dual HWP. Narrow-Band and Longpass filters are respectively used to increase the photon purity and cut the residual pump.

med with detection apparatus, which consists of twelve pseudo-number resolving multi-element superconducting detectors [94, 95].

Now, we will give brief explanation of the results obtained.

*Witness 1.* A set of $N = 150$ measurement operators $M_k$'s randomly picked from the set $\mathcal{M}_1$ has been implemented with our tomographic elements at the *Detection stage*. Measurement results that did not register any six-fold coincidence event have not been taken into account. When more than one coincidence was detected during the same measurement, we processed the outcomes to extract only the first coincidence click that the detectors registered, to ensure that we used only one copy of the state for every measurement. We use each copy to evaluate the outcome $m_k$ of each $M_k$ operator. Besides the separable bound $p_{s1}$, which holds for any separable state, we also apply an algorithm presented in [93] and show that for any fully separable state we have at best $p_{s1} = 9/16$. Formula (4.56) has been used to plot the

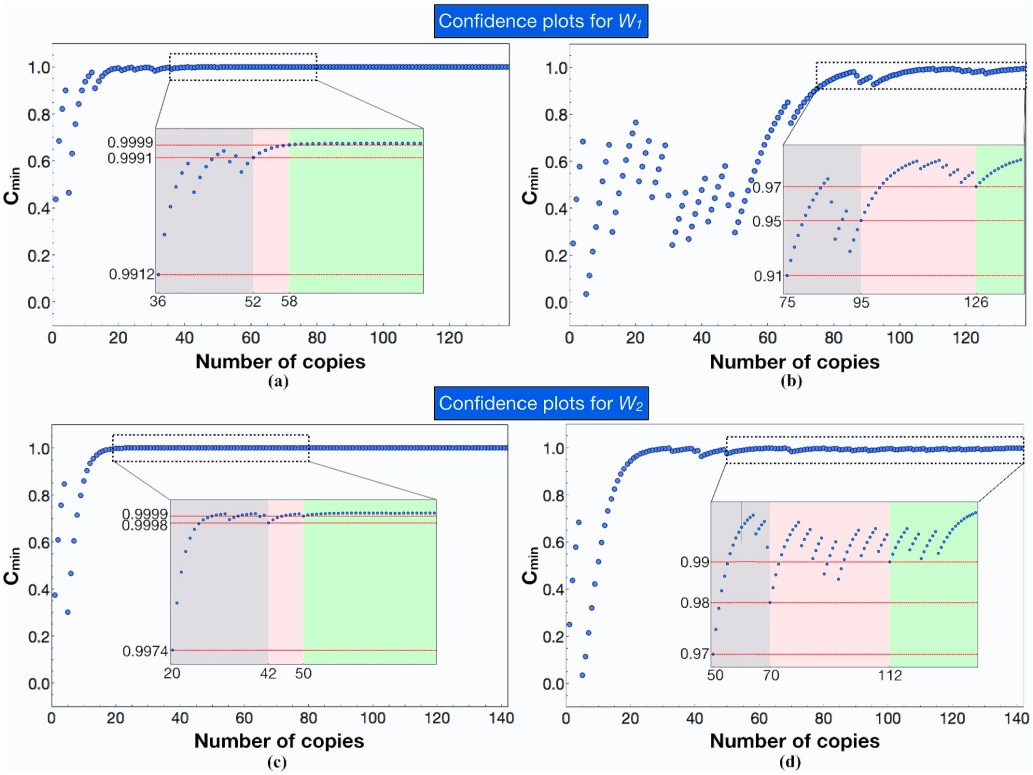


**Figure 4.5:** Blue dots represent $C_{\min}$ extracted from expression (4.56). **(a)**, **(b)** show the results for the witness $W_1$, **(c)**, **(d)** for the witness $W_2$. **(a)** and **(c)** show the minimum confidence when the full separability bound is used (meaning $C\min(S_1/N_1 - 9/16)$ and $C\min(S_2/N_2 - 5/8)$ for **(a)** and **(c)**, respectively) and **(b)**, **(d)** are extracted by using the biseparable bound (meaning $C\min(S_1/N_1 - 3/4)$ and $C\min(S_2/N_2 - 3/4)$, respectively). The reach for the confidence stability is highlighted and shown in the insets, where areas marked with different colors indicate different thresholds for the confidence level. Red dotted lines emphasize the different levels.

confidence of entanglement detection versus the number of copies for biseparability and full separability classes. The plots are provided in Fig. 4.5, where blue dots represent the confidence. Fig. 4.5a and 4.5b show the plots realized using the same experimental data for the two different separability classes. Plugging in formula (4.56) the separable bound $p_{s1} = 3/4$ — which holds for the biseparability case — we obtain the data shown in Fig. 4.5a, while when using $p_{s1} = 9/16$ — valid for the full separability case — we extract the plot in Fig. 4.5b. Both plots show an overall growth of the confidence and eventually a region of stability. Insets show how the confidence stabilizes to a particular value. Oscillations in confidence clearly show the presence of noise in the system. Whenever an outcome evaluates to 0, that is the failure case, the confidence behaviour shows a drop and rises again when the right outcomes, i.e. 1, are obtained. These oscillations become, of course, less dominant when a higher number of copies is used. In the biseparability case (Fig. 4.5a) we find

at best that 75 copies suffice to detect quantum entanglement with more than 91% confidence. After 95 copies, the confidence exceeds 95% and more than 97% is reached with 126 copies. The plot can be understood in a way according to which above 75 copies we are able to exclude biseparability in the state with more than 91% confidence, hence certifying genuine multipartite entanglement. In the full separability case (Fig. 4.5b), we show that only 36 copies suffice to detect entanglement with more than 99.12% confidence. Stability at the confidence's third digit is reached above 52 copies, and 58 copies always give more than 99.99% confidence. Here, as we can exclude full separability in the system — already for example after 36 copies with more than 99.12% confidence — we are obviously not able to certify genuine multipartite entanglement, but nonetheless, we show that the number of copies to detect entanglement is reduced with respect to the biseparability case. The different areas are marked with different colours in both plots, and red dotted lines are there to help to visualize the different confidence levels.

*Witness 2.* Here, a set of $N = 160$ measurement settings randomly picked from the set $\mathcal{M}_2$ has been applied to the state. Analogously, measurement results that didn't register any six-fold coincidence event have been removed. Also in this case we can compute the separable bound $p_{s2}$ for the full separability class, finding $p_{s2} = 5/8$. The plots of the confidence versus the number of copies for the biseparability and full separability class are provided in Fig. 4.5c,d, respectively. In Fig. 4.5c, we can observe that only 50 copies suffice to reveal entanglement with more than 97% confidence. This fact clearly shows the power of our approach: entanglement can be detected with high confidence even with a number of copies smaller than the number of measurement settings. Above 112 copies, the confidence never drops below 99%. Fig. 4.5d can be read in the same way. The confidence reaches third digit stability after only 50 copies. As in this case we are spanning the whole space of generators, the fidelity can be estimated to be $F = \langle Cl_6|\rho_{exp}|Cl_6\rangle = 0.75 \pm 0.06$.

The experimental plots confirm the efficiency of our entanglement verification method by showing an evident exponential growth of confidence. The insets show that the confidence stabilizes towards a certain value with the number of runs. Since usual technical limitations lead to experimentally generated multi-qubit states with imperfect fidelities, one can expect that the confidence would not grow monotonically. Naturally, there will be occasional failure events with the binary outcome 0, which will decrease the confidence. The fluctuations in the confidence values are connected to the number of measured copies, such that a higher number of copies suppresses these fluctuations.

# 5 Nonlocality detection

Nonlocality is one of the most important properties of quantum mechanics, where two or more spatially separated observers sharing entangled quantum bits can create correlations that cannot be explained by any local realistic theory. This work aims to apply methods developed in [76] for nonlocality verification. In order to do so, we study nonlocal properties of cluster states and translate the procedure for entanglement verification for linear cluster states into the procedure for nonlocality verification. Our final goal is to apply techniques from quantum state verification to the self-testing scenario [96, 76, 89] and to develop device independent scheme for quantum state verification [97].

## 5.1 Framework for testing nonlocality

The simplest way to test nonlocality is by observing violation of Bell's inequalities, that is by using nonlocal games. In a nonlocal game, we imagine that $(n)$ players play against a referee. The referee hands them questions, and the players reply with appropriate answers with the aim to win the game, but depending on the type of the game they might not be able to win always, even if they use quantum strategies. The players' goal is to collaborate and maximize their chances of winning. Before the game, the players meet and may agree upon a joint strategy – but then they move far apart from each other and cannot communicate with each other while the game is being played. Our task (as a referee) is to check whether players use classical (local) strategy or they share a quantum resource (e.g. GHZ state, linear cluster state,...) that provides certain advantage.

Let us assume to own a set of binary local observables, here representing challenges, $\mathcal{M} = \{M_1, M_2, ..., M_Q\}$ where the mean value of each $M_k$ (with $k = 1, ..., Q$) returns the binary outcome $m_k = 1, 0$. To be precise, every challenge $M_k$ is decomposable into local questions for each player. Each player answers its question, and final result $m_k = 1$ (0) is associated with the success (failure) in the challenge, having all answers collected. The procedure consists in randomly drawing $N$ times from the set $\mathcal{M}$ the challenges $M_k$'s (each with some probability $\Pi_k$) and sending them to players, obtaining the outcomes $m_k$'s. Some games are such that any classical local strategy is upper bounded by a certain value $p_{local} < 1$, that we call *locality bound*. On the other hand, the probability of success is maximized to $p_{nonlocal}$ (called *nonlocality value*) if a certain quantum resource (nonlocality winning resource ) has been used. Value of $p_{nonlocal}$ is strictly greater than $p_{local}$, i.e. the difference

$\delta_0 = p_{nonlocal} - p_{local} > 0$. Usually, the set $\mathcal{M}$ is tailored such that $p_{nonlocal}$ equals 1 only for target quantum resource, making the procedure even more efficient. It has been shown in [76, 89] that the probability $P(\delta_0)$ to observe $\delta_0 > 0$ for any classical strategy is upper-bounded as $P(\delta_0) \leq e^{-D(p_{local}+\delta_0||p_{local})N}$, which goes exponentially fast to zero with the number of runs $N$. Here $D(x||y) = x \log \frac{x}{y} + (1-x) \log \frac{1-x}{1-y}$ is the Kullback-Leibler divergence, as we had before. Therefore, the confidence $C(\delta_0)$ of detecting nonlocality is lower-bounded by $C_{\min}(\delta_0)$:

$$C(\delta_0) = 1 - P(\delta_0) \geq 1 - e^{-D(p_{local}+\delta_0||p_{local})N} = C_{\min}(\delta_0), \tag{5.1}$$

and converges exponentially fast to unity in $N$. From expression (5.1) we can estimate the average number of runs $N_{av}$ needed to achieve a certain confidence $C_0$, meaning that for a target resource sharing we find

$$N_{av} \leq -K \log(1 - C_0) = N_{\max}, \tag{5.2}$$

which grows logarithmically as $C_0$ approaches certainty at the rate of $K = D(p_e||p_s)^{-1}$. In a realistic framework, we can say that players share a certain quantum state $\rho_{exp}$ and assume that the experiment reveals $S$ successful outcomes. The observed deviation from the locality bound $\delta$ therefore reads

$$\delta = \frac{S}{N} - p_{local}. \tag{5.3}$$

If $\delta$ evaluates to a positive number, we can use the expression above to calculate $C_{min}(\delta)$ from expression (5.1).

## 5.2 Linear cluster state and nonlocality

As explained in the previous chapter, the $n$-qubit LCS is uniquely defined by the set of $2^n$ stabilizers, i.e.

$$G_{q_1 \ldots q_N}|LCS\rangle = G_1^{q_1} \ldots G_n^{q_n}|LCS\rangle = +1|LCS\rangle, \tag{5.4}$$

where $G_k = Z_{k-1}X_kZ_{k+1}$ and $q_k = 0, 1$. Here $\{X_k, Y_k, Z_k\}$ is the set of standard Pauli operators acting on $k^{\text{th}}$ qubit, having binary outcomes $i_k = 0, 1$ and we consider the one-dimensional lattice as an open segment. It turns out by later inspection that the nonlocality properties described in this paper do not change if the lattice would be a closed-loop (that is if qubits $n$ and 1 were taken to be neighbours). Switching to the general case of $n$-qubit linear cluster state can be done straightforwardly via

regular partitioning. As an illustration, we will explain how our method works on the example of four qubit linear cluster state.

The 4-qubit cluster state

$$|LCS_4\rangle = \frac{1}{2}(|+\rangle|0\rangle|+\rangle|0\rangle + |+\rangle|0\rangle|-\rangle|1\rangle + |-\rangle|1\rangle|-\rangle|0\rangle + |-\rangle|1\rangle|+\rangle|1\rangle) \tag{5.5}$$

is defined with four generators

$$\begin{aligned} G_1 &= XZ\mathbb{1}\mathbb{1} \\ G_2 &= ZXZ\mathbb{1} \\ G_3 &= \mathbb{1}ZXZ \\ G_4 &= \mathbb{1}\mathbb{1}ZX. \end{aligned} \tag{5.6}$$

And for each of them $G_i|LCS_4\rangle = |LCS_4\rangle$, $i \in \{1,2,3,4\}$, for which we will use shortcut $G_i = +1$. Eleven other stabilizers can be obtained by multiplication using the algebra of Pauli matrices. Following the work presented in [98] we introduce Bell expression given by:

$$A_1C_1D_2 + 2A_2B_1C_2D_2 + A_1C_2D_1 - 2A_2B_1C_1D_1 + B_2C_1D_2 + B_2C_2D_1 \leq 4 \tag{5.7}$$

This expression can attain the algebraic maximum of 8 with a cluster state. The respective settings $(A_i, B_j, C_k)$ are $Z$ and $X$ up to local rotations. This means that we can translate this Bell's type inequality into probability of success operator ($\langle LCS_4|P_s|LCS_4\rangle = 1$) using local measurements. In this case our probability of success operator is:

$$P_s = \frac{1}{8}(Q_1 + 2Q_2 + Q_3 + 2Q_4 + Q_5 + Q_6), \tag{5.8}$$

where $Q_1 = \frac{\mathbb{1}+A_1C_1D_2}{2}$, $Q_2 = \frac{\mathbb{1}+A_2B_1C_2D_2}{2}$, $Q_3 = \frac{\mathbb{1}+A_1C_2D_1}{2}$, $Q_4 = \frac{\mathbb{1}-A_2B_1C_1D_1}{2}$, $Q_5 = \frac{\mathbb{1}+B_2C_1D_2}{2}$ and $Q_6 = \frac{\mathbb{1}+B_2C_2D_1}{2}$. Here "questions" (challenges) $Q_2$ and $Q_4$ are sampled with probability 1/4 and the remaining four questions with probability 1/8. Local bound is 3/4 [99], so after performing our random sampling protocol, the confidence level of nonlocality detection can be calculated using (5.1).

## 5.3 Bell's inequality for self-testing cluster states

Currently, there exist several methods for self-testing graph states. For our purposes, we need a Bell's inequality maximally violated by the given graph state and such that the maximal violation achieves the algebraic bound of the inequality. Such is the inequality given in (5.7). The inequality has already been used for numerical self-testing of the four-qubit linear cluster state [96]. Here we show the analytical self-testing proof. The maximal violation of inequality (5.7) implies the following relations:

$$\langle\psi|A_1C_1D_2|\psi\rangle = 1 \tag{5.9a}$$
$$\langle\psi|A_1C_2D_1|\psi\rangle = 1 \tag{5.9b}$$
$$\langle\psi|A_2B_1C_2D_2|\psi\rangle = 1 \tag{5.9c}$$
$$\langle\psi|A_2B_1C_1D_1|\psi\rangle = -1 \tag{5.9d}$$
$$\langle\psi|B_2C_1D_2|\psi\rangle = 1 \tag{5.9e}$$
$$\langle\psi|B_2C_2D_1|\psi\rangle = 1 \tag{5.9f}$$

Since we work in the device-independent scenario we can assume that the state is pure (i.e. we operate with the purification of the state shared between the four parties) and we can exploit the Naimark extension and assume that the measurements are projective, i.e. $A_i^2 = B_i^2 = C_i^2 = D_i^2 = \mathbb{1}$. Hence, eqs. (5.9a) and (5.9b) imply

$$A_1|\psi\rangle = C_1D_2|\psi\rangle = C_2D_1|\psi\rangle. \tag{5.10}$$

Equivalently eqs. (5.9c) and (5.9d) imply

$$A_2B_1|\psi\rangle = C_2D_2|\psi\rangle = -C_1D_1|\psi\rangle. \tag{5.11}$$

By isolating the second equalities from (5.10) and (5.11) and multiply with $C_1D_1$ and $C_2D_1$, respectively, we get:

$$\begin{aligned} C_1D_1C_1D_2|\psi\rangle = C_1D_1C_2D_1|\psi\rangle \quad &\Rightarrow \quad D_1D_2|\psi\rangle = C_1C_2|\psi\rangle \\ C_2D_1C_2D_2|\psi\rangle = -C_2D_1C_1D_1|\psi\rangle \quad &\Rightarrow \quad D_1D_2|\psi\rangle = -C_2C_1|\psi\rangle. \end{aligned}$$

By combining the obtained equations we get:

$$\{C_1, C_2\}|\psi\rangle = 0. \tag{5.12}$$

In a similar manner, by multiplying equalities from (5.10) and (5.11) with $C_1D_1$ and $C_1D_2$, we obtain

$$\{D_1, D_2\}|\psi\rangle = 0. \tag{5.13}$$

From eqs. (5.10) and (5.11) we also obtain

$$\begin{aligned}
\{A_1, A_2\}|\psi\rangle &= A_1A_2|\psi\rangle + A_2A_1|\psi\rangle \\
&= -A_1B_1C_1D_1|\psi\rangle + A_2C_1D_2|\psi\rangle \\
&= -B_1C_1D_1C_2D_1|\psi\rangle + C_1D_2B_1C_2D_2|\psi\rangle \\
&= -B_1C_1C_2|\psi\rangle + B_1C_1C_2|\psi\rangle \\
&= 0.
\end{aligned} \tag{5.14}$$

Equivalently by using eqs. (5.9c),(5.9d), (5.9e),(5.9f) we are able to prove that

$$\{B_1, B_2\}|\psi\rangle = 0. \tag{5.15}$$

Let us focus on the pair of observables $A_1$ and $A_2$. The following equality holds for any two binary projective observables [100]:

$$|\{A_1, A_2\}|^2 + |[A_1, A_2]|^2 = 4\mathbb{1}, \tag{5.16}$$

where $|A| = (AA^\dagger)^{1/2}$. It further follows that for state $\rho = |\psi\rangle\langle\psi|$ satisfies

$$\mathrm{Tr}\left(|\{A_1, A_2\}|^2\rho\right) + \mathrm{Tr}\left(|[A_1, A_2]|^2\rho\right) = 4, \tag{5.17}$$

and due to (5.14)

$$\mathrm{Tr}\left(|[A_1, A_2]|^2\rho\right) = 4, \tag{5.18}$$

On the other hand, due to the Höler inequality we have

$$\mathrm{Tr}\left(|[A_1, A_2]|^2\rho\right) \leq \||[A_1, A_2]|^2\|_\infty \,\mathrm{Tr}\,\rho. \tag{5.19}$$

By the triangle inequality one can prove that $\||[A_1, A_2]|^2\|_\infty \leq 4$, hence from (5.18) it must be that the inequality (5.19) is saturated. The saturation of the inequality happens when $|[A_1, A_2]|^2 = \||[A_1, A_2]|^2\|_\infty\mathbb{1} = 4\mathbb{1}$. Furthermore

$$|[A_1, A_2]|^2 \leq (|A_1A_2| + |A_2A_1|)^2 = 4\mathbb{1}. \tag{5.20}$$

Since the inequality is saturated it must hold $A_1A_2 = -A_2A_1$, or equivalently

$$\{A_1, A_2\} = 0. \tag{5.21}$$

Note that from anticommutation relation on the support of the state given in (5.14) we obtained the full anticommutation relation in (5.21). By repeating the procedure one can obtain

$$\{B_1, B_2\} = 0, \tag{5.22}$$
$$\{C_1, C_2\} = 0, \tag{5.23}$$
$$\{D_1, D_2\} = 0. \tag{5.24}$$

Let us now state and prove an important lemma

**Lemma 5.1.** Take two local hermitian operators $A$,$B$ acting on an arbitrary Hilbert space and satistying the idempotency property $A^2 = B^2 = \mathbb{1}$ and the anticommutation relation $\{A, B\} = 0$. There exist a local unitary operator $U$ such that

$$UAU^\dagger = X \otimes \mathbb{1}_d\,,$$
$$UBU^\dagger = Z \otimes \mathbb{1}_d\,,$$

where $X, Z$ are the qubit Pauli matrices and the dimesion $d$ is such that $2d$ is the total dimension of the Hilbert space where $X$,$Z$ act on.

*Proof.* First of all, recall that the idempotency implies that the two operators have only $\pm 1$ eigenvalues. We can then make use of the idempotency property to rewrite the anticommutation relation as $ABA = -B$. Such a condition implies that the number of $+1$ and $-1$ eigenvectors of $B$ has to be the same and the unitary $A$ acts on the eigenspace of $B$ by simply rearranging them. Let us name the positive eigenvectors of $B$ as $|e_i^+\rangle$ with $i = 1, \dots, d$, where $2d$ is the dimension of the Hilbert space on which the two operators are acting. We then associate to each of these eigenvector the corresponding negative eigenvector obtained by the rearranging action of $A$, namely

$$|e_i^-\rangle = A|e_i^+\rangle\,.$$

One can check that the vectors defined above are indeed negative eigenvectors of $B$. Indeed, by means of the anticommutation relation, we get

$$B|e_i^-\rangle = BA|e_i^+\rangle = -AB|e_i^+\rangle = -|e_i^-\rangle\,.$$

By writing the $A, B$ operators in the $\{|e_i^\pm\rangle\}_{i=1}^d$, one obtains

$$B = \sum_{i=1}^{d} |e_i^+\rangle\langle e_i^+| - \sum_{i=1}^{d} |e_i^-\rangle\langle e_i^-|$$

$$A = \sum_{i=1}^{d} |e_i^-\rangle\langle e_i^+| + \sum_{i=1}^{d} |e_i^+\rangle\langle e_i^-|\,,$$

If we define $U$ as the unitary mapping the $|e_i^{\pm}\rangle$ vectors in $\mathbb{C}^{2d}$ to a basis in $\mathbb{C}^2 \otimes \mathbb{C}^d$ as follows

$$U|e_i^+\rangle = |0\rangle|g_i\rangle\,,$$
$$U|e_i^-\rangle = |1\rangle|g_i\rangle\,,$$

where the $|g_i\rangle$ can be an arbitrary orthogonal basis of $\mathbb{C}^d$, then

$$UBU^\dagger = Z \otimes \mathbb{1}_d\,, \quad UXU^\dagger = X \otimes \mathbb{1}_d\,,$$

as desired. □

Lemma implies that there exist unitaries $U_A$, $U_B$, $U_C$ and $U_D$ such that

$$U_A A_1 U_A^\dagger = X \otimes \mathbb{1}_d\,, \quad U_A A_2 U_A^\dagger = Y \otimes \mathbb{1}_d\,, \tag{5.25a}$$
$$U_B B_1 U_B^\dagger = X \otimes \mathbb{1}_d\,, \quad U_B B_2 U_B^\dagger = Z \otimes \mathbb{1}_d\,, \tag{5.25b}$$
$$U_C C_1 U_C^\dagger = Y \otimes \mathbb{1}_d\,, \quad U_C C_2 U_C^\dagger = X \otimes \mathbb{1}_d\,, \tag{5.25c}$$
$$U_D D_1 U_D^\dagger = Z \otimes \mathbb{1}_d\,, \quad U_D D_2 U_D^\dagger = Y \otimes \mathbb{1}_d\,. \tag{5.25d}$$

Now given eqs. (5.25a)-(5.25b) it can be shown that the state $\rho$ satisfying all the equations (5.9a)-(5.9f) must be

$$U\rho U^\dagger = |\phi_4\rangle\langle\phi_4| \otimes |\xi\rangle, \tag{5.26}$$

where $U = U_A \otimes U_B \otimes U_C \otimes U_D$, $|\phi_4\rangle$ is the 4-qubit linear cluster state and $|\xi\rangle$ is some unknown quantum state.

## 5.4 Device independent quantum state verification

Our goal here is to apply techniques from quantum state verification to the self-testing scenario. First, let us describe the scenario for device-independent verification of multipartite entangled states. The state is shared between $n$ parties, who treat their measurement devices as black boxes. The measurement-base choices for each box are encoded in classical inputs, on which each box answers with a classical output - the measurement result. Crucially, there is no communication between different boxes. The process is repeated $N$ times, i.e. there are $N$ rounds, and $N$ copies of the target state are necessary for the success of the protocol. We do not make the i.i.d. assumptions, but in the same spirit as in quantum state verification [96]

we make the assumption that the source is either always sending the state $\Phi_i(\psi)$, where $\psi$ is our target state and $\Phi_i$ is some local isometry (which can be different in each round) or always sends a state from the set $\{\sigma_1, \sigma_2, \cdots, \sigma_N\}$ such that for all $i = 1, \cdots N$ fidelity between $\Phi(\sigma_i)$ and $\psi$, optimized across all local isometries $\Phi$ is lower than $1 - \epsilon$. The test is based on the robust self-testing procedure for the target state $\psi$. Let us imagine the state is self-tested by maximal violation of a Bell inequality $\sum_{abxy} b_{xy}^{ab} p(ab|xy) \leq \beta_{loc}$, such that its maximal quantum violation $\beta_q$ is equal to its algebraic maximum, i.e. all the probabilities are equal to either 1 or 0. Any state $\Phi_i(\psi)$ achieves the maximal violation $\beta_q$. Robustness of the self-testing procedure ensures that any state $\sigma$ achieving violation of $\beta_q - \delta$ is such that the fidelity between $\Phi(\sigma)$ and $\psi$ where $\Phi$ is a convenient local isometry is higher or equal than $1 - f(\delta)$.

Let us look at the particular example of the GHZ state $\psi_{GHZ} = (|000\rangle + |111\rangle)/\sqrt{2}$ and its self-test, the maximal violation of the Mermin inequality:

$$\langle A_0 B_0 C_1 \rangle + \langle A_0 B_1 C_0 \rangle + \langle A_1 B_0 C_1 \rangle - \langle A_1 B_1 C_0 \rangle \leq 2 \tag{5.27}$$

The maximal violation is achieved by the GHZ state, and it is equal to 4. It is shown in [101] that any state $\sigma$ achieving violation $4-\delta$ implies there is an isometry $\Phi$ such that the fidelity between $\psi_{GHZ}$ and $\Phi(\sigma)$ is higher than $1-\delta/c$, where $c = 4(2-\sqrt{2})$. This bound is proven to be tight, meaning that for any state $\sigma$ achieving violation $4-\delta$ there is no isometry $\Phi$ such that the fidelity between $\Phi(\sigma)$ and $\psi_{GHZ}$ is higher than $1-\delta/c$. Now, let us see what this implies for the device-independent verification procedure as described above. In each round, the boxes receive inputs comprising one of the four global inputs (001, 010, 100 or 111). Any state locally isometric to GHZ on one of the first three global questions provides one of the following answers (111, 100, 010, 001), while on the last global input the 'correct' answers are (000, 011, 101, 110). If in a round we ask one of the global questions and get the correct answer the achieved score in the round is $p_i = 1$, otherwise $p_i = 0$. The final score is $P = \sum_{i=1}^{N} p_i/N$. From the tight bound on robust self-testing for every state such that there is no local isometry bringing it closer to $\psi_{GHZ}$ then $1 - \epsilon$ we know that it cannot violate GHZ more than $4 - c\epsilon$. It means that, given random sampling of global inputs, on average it has probability $p_\epsilon = 1 - c'\epsilon$, where $c' = 1 - 1/\sqrt{2}$ to provide the correct answer in each round. Hence, the probability that a strategy not involving the target state (or some state locally isometric to it) gives a correct answer in all $N$ rounds is

$$p \leq \mathrm{e}^{-D(1||p_\epsilon)N} \tag{5.28}$$

where $D(x||y) = x \log \frac{x}{y} + (1-x) \log \frac{1-x}{1-y}$ is the Kullback-Leibler divergence. Therefore, the confidence $C(\epsilon)$ of certifying the target state when actually the states more than $\epsilon$-far from it were always sent is lower bounded by

$$C(\epsilon) \geq 1 - \mathrm{e}^{-D(1||p_\epsilon)N}. \tag{5.29}$$

**Table 5.1.**: *Number of copies needed for reliable detection for various infidelities.*

| Infidelity $\epsilon$ | Number of copies DD method | Numer of copies DI method |
|---|---|---|
| 0.05 | 90 | 313 |
| 0.10 | 44 | 155 |
| 0.15 | 29 | 103 |
| 0.20 | 21 | 77 |
| 0.25 | 16 | 61 |
| 0.30 | 13 | 50 |

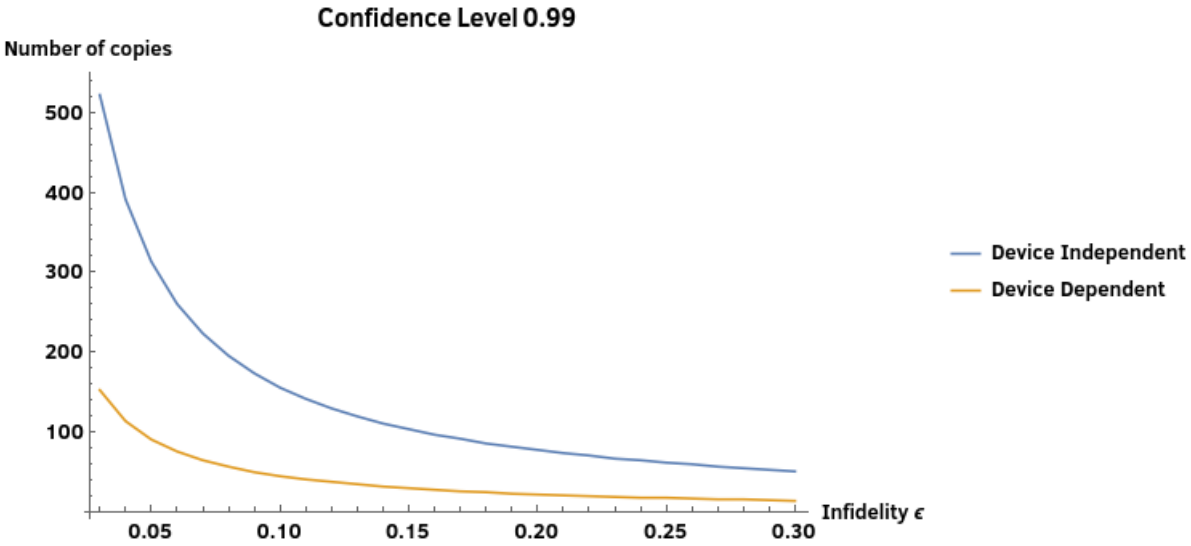


**Figure 5.1:** For a fixed minimal confidence level, we can compare the number of copies needed dependent on infidelity $\epsilon$.

By using (5.29) and approach provided in [96] we can compare number of instances of the prepared quantum state that will be sufficient to verify entanglement with confidence level 99% for a given infidelity $\epsilon$. The relevant results are given in the table above and in Figures 5.1 and 5.2.

What we see from Figure 5.1 is that for smaller infidelities, i.e. for very precise distinguishing between target and any other state, it is more resource-efficient to operate under a device-dependent scheme. On the other hand, for larger infidelities,

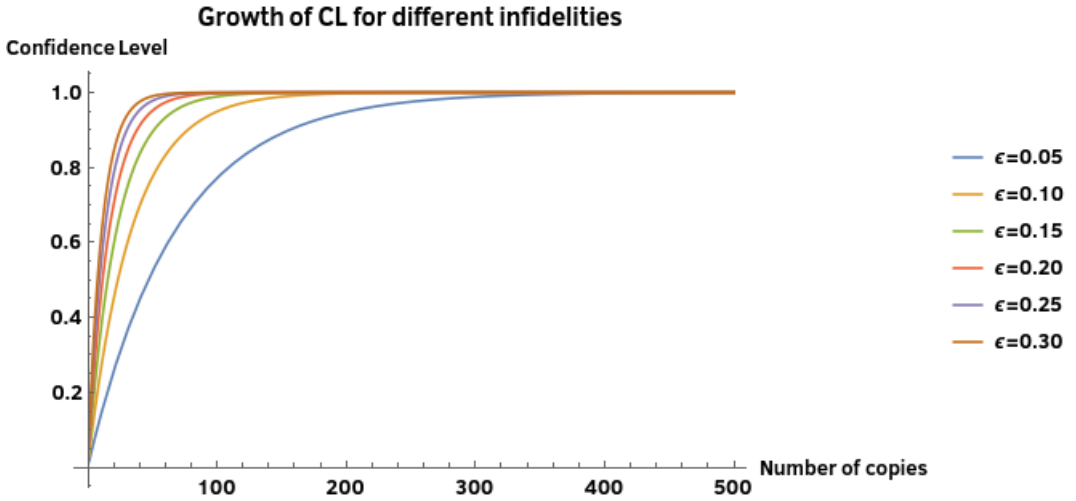


**Figure 5.2:** For different values of $\epsilon$, we compare the growth of the confidence level in function of the number of copies of the prepared quantum state.

device-independent and device-dependent scheme become comparable in terms of the number of instances of the provided quantum system.
Figure 5.2 shows stabilization of confidence level in the device-independent scenario with the number of copies of the quantum state for various infidelities. As expected, stabilization is the fastest in the case of higher infidelities, whereas, in the case of smaller infidelities, stabilization is slower and more copies are necessary for the same confidence level.

# 6 Convergence of quantum random variables

The basic motivation for this research was to investigate the limit distribution of relative frequency for correlated inputs subjected to strictly unsharp (POVM) quantum measurements. This means that individual results cannot have sharp values, i.e. the variance is strictly greater than zero. In our study, we have found two very different behaviours. For separable, classically correlated, inputs we recover asymptotic normality, which is given by our representation theorem. On the other hand, for entangled inputs, we found a different behaviour which is provided as "entanglement counterexample" [102]. The first result means that separable inputs indeed follow asymptotic normality. On the other hand, entangled inputs do not follow asymptotic normality in general, although all random variables are strictly unsharp, and one usually should expect asymptotic normality to follow from Lindenberg's Central Limit Theorem (CLT). An elementary review of probability theory is given in Appendix B.

In addition, we find such behaviour of entangled inputs relevant for quantum information processing. Therefore, we introduce a "quantum game" to distinguish entangled from separable states in the context of quantum information processing.

## 6.1 Unsharp quantum measurements

The essential feature of generalized quantum measurements (POVMs) is the "unsharpness" and production of an unavoidable noise during the measurement process [103]. The noise is a result of non-projective character of the measurement operators; thus, the measurement outcomes will inevitably fluctuate in the sequence of repeated experimental runs. By the repeated experimental run, here we consider independent measurements on a set of $N$ individual physical systems (e.g. qubits). Our aim here is to show that fluctuations can be very different depending on whether we perform unsharp measurements on separable or entangled inputs. To begin, we introduce some basic definitions. Consider a quantum measurement defined by the set of POVM elements $E_i$, with $E_i \geq 0$ and $\sum_i E_i = \mathbb{1}$. We define a random variable $X$ generated by measurement with the set of numbers $X \in \{x_1, x_2, \dots\}$ where each $x_i \in \mathbb{R}$ corresponds to the $i$th outcome (defined by $E_i$). It is convenient to define the expectation

$$\hat{M} = \sum_i x_i E_i \tag{6.1}$$

and the uncertainty operator [103]

$$\Delta\hat{V} = \sum_i x_i^2 E_i - \hat{M}^2. \tag{6.2}$$

For a given quantum state $\rho$, the expectation value and variance are easily evaluated

$$\langle X \rangle_\rho = \operatorname{Tr} \rho \hat{M} \tag{6.3}$$

and

$$\sigma^2 = \operatorname*{Var}_\rho[X] = \langle X^2 \rangle_\rho - \langle X \rangle_\rho^2 = \langle \hat{M}^2 \rangle_\rho - \langle X \rangle_\rho^2 + \operatorname{Tr} \rho \Delta\hat{V}. \tag{6.4}$$

We can see that the uncertainty operator produces additional noise that is solely due to the measurement (note that $\Delta\hat{V} \geq 0$ in general). For all projective, von Neumann measurements $\Delta\hat{V} = 0$, hence this term vanishes.

We focus on strictly unsharp measurements, i.e. we consider

$$\sigma_- \leq \sigma \leq \sigma_+, \tag{6.5}$$

with $\sigma_- > 0$ being strictly positive for all states $\rho$. Additionally, we assume that the third moment

$$r = \langle |X - \langle X \rangle_\rho|^3 \rangle_\rho \leq M \tag{6.6}$$

is bounded by some constant $M > 0$ for all $\rho$.

For a sequence of random variables $X_1, \ldots, X_N$ generated by repeated measurement with $X_i \in \{x_1, x_1, \ldots\}$, we set

$$X^{(N)} = X_1 + \cdots + X_N \tag{6.7}$$

and

$$R_N = \frac{1}{N} X^{(N)} \tag{6.8}$$

to be the relative frequency. Furthermore, we define the standardly normalized sum

$$S_N = \frac{1}{\sqrt{N}} (X^{(N)} - \langle X^{(N)} \rangle). \tag{6.9}$$

The distribution of the relative frequency $R_N$ is the central object of our investigation. The question that we want to answer is: what is the probability of $R_N$ taking some particular value in the limit of large number of experimental runs?

## 6.2 Separable inputs

The answer to the previous question heavily depends on the type of input state. For example, if one supplies in each run the same state $\rho$, the overall input state is described by an i.i.d. state $\rho^{(N)} = \rho^{\otimes N}$, where $N$ is the number of experimental runs. The weak law guarantees the convergence of the relative frequency converges to the mean value $\langle X \rangle_\rho$ and the Central Limit Theorem states that the distribution of $S_N$ converges to the normal distribution. A slightly more delicate example is the one of independent inputs, i.e. $\rho^{(N)} = \rho_1 \otimes \cdots \otimes \rho_N$, where $\rho_i$s are different in general. Here we can define the mean variance

$$\Sigma_N^2 = \frac{1}{N} \sum_{i=1}^{N} \sigma_i^2, \tag{6.10}$$

with $\sigma_i^2 = \mathrm{Var}_{\rho_i}[X]$ and the average mean

$$m_N = \frac{1}{N} \sum_{i=1}^{N} m_i, \tag{6.11}$$

with $m_i = \langle X \rangle_{\rho_i}$. Clearly $\langle X^{(N)} \rangle = N m_N$ and $\sigma_- \leq \Sigma_N \leq \sigma_+$ as each individual variance is bounded. We can apply the *Lindeberg's condition* for CLT [104], i.e.

$$\max_i \frac{\sigma_i^2}{\sum_{j=1}^N \sigma_j^2} = \max_i \frac{\sigma_i^2}{N\Sigma_N^2} \leq \frac{\sigma_+^2}{N\sigma_-^2} \to 0, \tag{6.12}$$

when $N \to +\infty$, therefore the normalized sum

$$\frac{X^{(N)} - \langle X^{(N)} \rangle}{(\sum_{i=1}^N \sigma_i^2)^{1/2}} = \frac{X^{(N)} - N x_N}{\sqrt{N}\Sigma_N} = \frac{S_N}{\Sigma_N} \tag{6.13}$$

converges to the standard normal distribution. To quantify the deviation for finite $N$, we can use the Berry-Esseen theorem [105, 106]. Let $P[S_N/\Sigma_N \leq x]$ be the cumulative distribution function (CDF) and $\Phi(x)$ is the CDF of the standard normal distribution, i.e. $\Phi(x) = 1/\sqrt{2\pi} \int_{-\infty}^{x} e^{-t^2/2} dt$. We have

$$\begin{aligned} \sup_{x \in \mathbb{R}} |P[S_N/\Sigma_N \leq x] - \Phi(x)| &\leq C_0 \frac{\sum_{i=1}^N r_i}{N^{3/2}\Sigma_N^3} \\ &\leq C_0 \frac{NM}{N^{3/2}\sigma_-^3} = \frac{C_0 M}{\sigma_-^3 \sqrt{N}}, \end{aligned} \tag{6.14}$$

where $r_i = \langle |X - \langle X \rangle_{\rho_i}|^3 \rangle_{\rho_i} \leq M$ and $C_0$ is an absolute constant. We see that any product input state is subjected to CLT because the measurements are strictly unsharp (the variance is strictly bounded from bellow by $\sigma_-$). From here, we are ready to establish the representation theorem for separable states. For a given separable input state

$$\rho^{(N)} = \sum_k \lambda_k \rho_k^{(N)}, \tag{6.15}$$

where

$$\rho_k^{(N)} = \rho_{1,k} \otimes \cdots \otimes \rho_{N,k}, \tag{6.16}$$

we set $m_{N,k} = \frac{1}{N}\sum_{i=1}^N m_{i,k}$, with $m_{i,k} = \langle X \rangle_{\rho_{i,k}}$ and $\Sigma_{Nk}^2 = \frac{1}{N}\sum_{i=1}^N \sigma_{i,k}^2$. Here $\sigma_{i,k}^2 = \mathrm{Var}_{\rho_{i,k}}[X]$.

**Theorem 6.1.** The CDF $F_N(x) = P[R_N \leq x]$ of the relative frequency satisfies the following bound:

$$\sup_{x\in\mathbb{R}} \left| F_N(x) - \sum_k \lambda_k \Phi\left(\frac{x - m_{N,k}}{\Sigma_{Nk}/\sqrt{N}}\right)\right| \leq \frac{C_0 M}{\sigma_-^3 \sqrt{N}}. \tag{6.17}$$

*Proof.* Firstly, note that $F_N(x) = P[R_N \leq x] = \sum_k \lambda_k P_k[R_N \leq x]$, where $P_k[R_N \leq x]$ is the CDF for the product state $\rho_k^{(N)} = \rho_{1,k} \otimes \cdots \otimes \rho_{N,k}$. We have

$$\begin{aligned}
& \sup_{x\in\mathbb{R}} \left| F_N(x) - \sum_k \lambda_k \Phi\left(\frac{x - m_{N,k}}{\Sigma_{Nk}/\sqrt{N}}\right)\right| \\
= & \sup_{x\in\mathbb{R}} \left| P\left[\frac{1}{N}X^{(N)} \leq x\right] - \sum_k \lambda_k \Phi\left(\frac{x - m_{N,k}}{\Sigma_{Nk}/\sqrt{N}}\right)\right| \\
= & \sup_{x\in\mathbb{R}} \left| \sum_k \lambda_k \left( P_k\left[\frac{1}{N}X^{(N)} \leq x\right] - \Phi\left(\frac{x - m_{N,k}}{\Sigma_{Nk}/\sqrt{N}}\right)\right)\right| \\
\leq & \sup_{x\in\mathbb{R}} \sum_k \lambda_k \left| P_k\left[\frac{1}{N}X^{(N)} \leq x\right] - \Phi\left(\frac{x - m_{N,k}}{\Sigma_{Nk}/\sqrt{N}}\right)\right| \\
= & \sup_{x\in\mathbb{R}} \sum_k \lambda_k \left| P_k\left[\frac{1}{N}X^{(N)} \leq \frac{\Sigma_{N,k}}{\sqrt{N}}x + m_{N,k}\right] - \Phi(x)\right| \\
= & \sup_{x\in\mathbb{R}} \sum_k \lambda_k \left| P_k\left[\frac{X^{(N)} - N m_{N,k}}{\sqrt{N}\Sigma_{N,k}} \leq x\right] - \Phi(x)\right| \\
= & \sup_{x\in\mathbb{R}} \sum_k \lambda_k \left| P_k\left[S_{N,k}/\Sigma_{N,k} \leq x\right] - \Phi(x)\right| \\
\leq & \sum_k \lambda_k \frac{C_0 M}{\sigma_-^3 \sqrt{N}} \\
= & \frac{C_0 M}{\sigma_-^3 \sqrt{N}}.
\end{aligned}$$

The last inequality follows from (6.14). □

Note that the bound (6.17) does not depend on any structure/symmetry of the underlying input state, which is in contrast to the de-Finetti-type representation theorems [107, 108, 109, 110, 111] that heavily rely on symmetry.

## 6.3 Convergence rates and quantum game

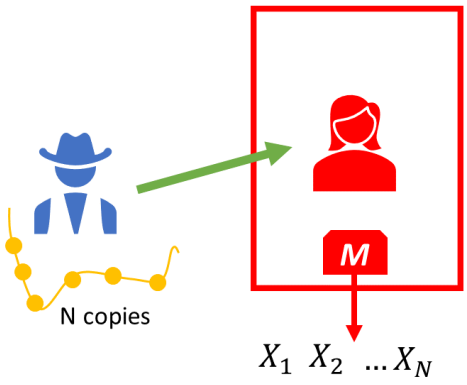


**Figure 6.1:** Bob prepares $N$ quantum particles in some state, where $N$ is fixed in advance and gives them to Alice who measures each particle. His goal is to make relative frequency as close as possible to some pre-defined value $X_c$.

In this section, we will show that entangled states can behave very differently in some instances compared to separable states concerning the distribution of the relative frequency. To illustrate our conclusions, we will define the problem as an information-theoretic game between two players, Alice and Bob, see Figure 6.1. Suppose that Alice performs some POVM and generates a random variable $X \in \{x_1, x_2, \dots\}$ which is strictly unsharp, i.e. $\mathrm{Var}[x]_\rho \geq \sigma_- > 0$ for all $\rho$. As before, we assume that third moments are bounded by $M > 0$. Then, Alice asks Bob to supply her with inputs, and his goal is to make the relative frequency $R_N = \frac{1}{N}(X_1 + \cdots + X_N)$ as close as possible to some pre-defined value $X_c$. More precisely, he will try to maximize the probability

$$P_N = P\left[|R_N - X_c| \leq \frac{\epsilon}{N^\alpha}\right], \tag{6.18}$$

with $\epsilon, \alpha > 0$ being fixed parameters. The parameter $\alpha$ quantifies the convergence rate of the relative frequency to the constant $X_c$. Our object is to show that the probability $P_N$ is negligible whenever $\alpha > 1/2$ for all separable states. And indeed, the bound (6.17) states that the distribution of $R_N$ is a mixture of Gaussians,

therefore the error (as quantified by the convergence rate) cannot scale better than $1/\sqrt{N}$. We fix $\alpha > 1/2$.

**Theorem 6.2.**

$$P_N \leq \sqrt{\frac{2}{\pi}} \frac{\epsilon}{\sigma_-} \frac{1}{N^{\alpha-\frac{1}{2}}} + \frac{2C_0 M}{\sigma_-^3 \sqrt{N}} \tag{6.19}$$

for all separable inputs.

*Proof.* For a separable input $\rho^{(N)} = \sum_k \lambda_k \rho_k^{(N)}$ we have $P_N = \sum_k \lambda_k P_{N,k}$. Therefore it is sufficient to prove (6.19) for a product state. We set $\rho^{(N)} = \rho_1 \otimes \cdots \otimes \rho_N$ and, as previously $\Sigma_N^2 = \frac{1}{N}\sum_{i=1}^N \sigma_i^2$. We have

$$\begin{aligned} P_N &= P\left[|R_N - X_c| \leq \frac{\epsilon}{N^\alpha}\right] \\ &= P\left[X_c - \frac{\epsilon}{N^\alpha} \leq \frac{1}{N} X^{(N)} \leq X_c + \frac{\epsilon}{N^\alpha}\right] \\ &= P\left[A_N - a_N \leq S_N/\Sigma_N \leq A_N + a_N\right] \\ &\leq \Phi(A_N + a_N) - \Phi(A_N - a_N) + \frac{2C_0 M}{\sigma_-^3 \sqrt{N}}, \end{aligned}$$

where

$$A_N = \frac{\sqrt{N}}{\Sigma_N}(X_c - \frac{1}{N}\langle X^{(N)}\rangle) \tag{6.20}$$

and

$$a_N = \frac{\epsilon}{\Sigma_N N^{\alpha-\frac{1}{2}}}. \tag{6.21}$$

The last inequality follows from the Berry-Esseen bound (6.14). For $a > 0$ the function $\Phi(x+a) - \Phi(x-a)$ reaches its absolute maximum for $x = 0$, hence $\Phi(x+a) - \Phi(x-a) \leq \Phi(a) - \Phi(-a) = 2\Phi(a) - 1$. Here, we used $\Phi(x) + \Phi(-x) = 1$. Furthermore, the function $\Phi(x)$ is concave for $x \geq 0$, therefore $\Phi(x) \leq \frac{1}{2} + \frac{x}{\sqrt{2\pi}}$. Finally, we have

$$\begin{aligned} P_N &\leq \Phi(A_N + a_N) - \Phi(A_N - a_N) + \frac{2C_0 M}{\sigma_-^3 \sqrt{N}} \\ &\leq 2\Phi(a_N) - 1 + \frac{2C_0 M}{\sigma_-^3 \sqrt{N}} \\ &\leq \sqrt{\frac{2}{\pi}} a_N + \frac{2C_0 M}{\sigma_-^3 \sqrt{N}} \\ &= \sqrt{\frac{2}{\pi}} \frac{\epsilon}{\Sigma_N N^{\alpha-\frac{1}{2}}} + \frac{2C_0 M}{\sigma_-^3 \sqrt{N}} \\ &\leq \sqrt{\frac{2}{\pi}} \frac{\epsilon}{\sigma_-} \frac{1}{N^{\alpha-\frac{1}{2}}} + \frac{2C_0 M}{\sigma_-^3 \sqrt{N}} \end{aligned}$$

□

The bound (6.19) states that the winning probability vanishes asymptotically $P_N \to 0$ with $N \to +\infty$, for all $\alpha > 1/2$. Therefore, Bob will fail to win the game

with certainty by using separable inputs. Now we will provide a simple example where entanglement can beat the bound given by (6.19).

## 6.4 Entanglement counterexample

Consider a qubit three-outcome POVM with the elements on "equilateral triangle"

$$E_i = \frac{1}{3}(\mathbb{1} + \vec{m}_i \cdot \vec{\sigma}), \tag{6.22}$$

where $\vec{m}_0 = (1,0,0)^T$, $\vec{m}_{\pm 1} = (-1/2, 0, \pm\sqrt{3}/2)^T$ and $\vec{\sigma} = \{\sigma_x, \sigma_y, \sigma_z\}$ is the vector of three Pauli matrices. We define the corresponding random variable with three possible values $X \in \{-1, 0, 1\}$ and we set $X_c = 0$. It is convenient to introduce two operators

$$A = \sum_i x_i E_i = -E_{-1} + E_1 = \frac{1}{\sqrt{3}}\sigma_z \tag{6.23}$$

and

$$B = \sum_i x_i^2 E_i = E_{-1} + E_1 = \frac{2}{3}\mathbb{1} - \frac{1}{3}\sigma_x. \tag{6.24}$$

We have

$$\operatorname*{Var}_\rho[X] = \langle B \rangle_\rho - \langle A \rangle_\rho^2 = \frac{2}{3} - \frac{x}{3} - \frac{z^2}{3}, \tag{6.25}$$

where $x$ and $z$ are components of the Bloch vector of the state $\rho$. Clearly $x^2 + z^2 \leq 1$. A simple calculation shows that $\operatorname{Var}_\rho[X] \geq \frac{1}{4}$, hence $\sigma_- = \frac{1}{4}$. Furthermore $|X| \leq 1$, thus the third moment is bounded and we have $M = 1$. The bound (6.19) applies to all separable inputs and $\alpha > 1/2$.

On the other hand, let Bob use the following input state

$$|\psi\rangle = \frac{1}{\sqrt{2L+1}} \sum_{m=-L}^{L} |J, m\rangle, \tag{6.26}$$

where we set $L = N^\beta$ with $0 < \beta < 1/2$. Here, we use the spin-$J$ representation for $N$-qubit permutational invariant pure state, i.e. any state can be written as

$$\sum_{m=-J/2}^{J/2} c_m |J, m\rangle, \tag{6.27}$$

with $J = N/2$ and $|J, J\rangle = |1\rangle^{\otimes N}$. The state (6.26) is very closed to the Dicke-squeezed state [112] introduced for the purposes of quantum metrology. Clearly, the

mean value

$$\langle X^{(N)}\rangle = \langle\psi|\sum_{i=1}^{N} A_i|\psi\rangle = \frac{2}{\sqrt{3}}\langle\psi|S_z|\psi\rangle = 0, \tag{6.28}$$

where $S_z = \frac{1}{2}\sum_i \sigma_{z,i}$ is the total spin operator along $z$-direction. Keeping in mind that $\langle X^{(N)}\rangle = X_c = 0$, we can lower-bound the winning probability by using the Chebyshev's inequality

$$\begin{aligned} P_N &= P\left[|\frac{1}{N}X^{(N)} - X_c| \leq \frac{\epsilon}{N^\alpha}\right] \qquad (6.29)\\ &= P\left[|X^{(N)} - \langle X^{(N)}\rangle| \leq \frac{\epsilon}{N^{\alpha-1}}\right] \\ &\geq 1 - \frac{N^{2(\alpha-1)}}{\epsilon^2}\,\mathrm{Var}[X^{(N)}] \\ &= 1 - s_N, \qquad (6.30) \end{aligned}$$

where $s_N = \frac{N^{2(\alpha-1)}}{\epsilon^2}\,\mathrm{Var}[X^{(N)}]$ upper-bounds the probability of failure. Our goal is to show that $s_N$ is negligible for large $N$. A simple calculation shows that

$$\mathrm{Var}[X^{(N)}] = \frac{N}{3} - \frac{2}{3}\langle\psi|S_x|\psi\rangle + \frac{4}{3}\Delta S_z^2. \tag{6.31}$$

Firstly, we calculate $\Delta S_z^2$ directly by substituting (6.26)

$$\begin{aligned} \Delta S_z^2 &= \frac{1}{2L+1}\sum_{m=-L}^{L} m^2 \\ &= \frac{1}{3}L(L+1). \qquad (6.32) \end{aligned}$$

The wavefunction $|\psi\rangle$ is real (with the respect to basis $|J,m\rangle$), hence

$$\langle\psi|S_x|\psi\rangle = \frac{1}{2}\langle\psi|(S_- + S_+)|\psi\rangle = \langle\psi|S_-|\psi\rangle, \tag{6.33}$$

where $S_-$ is the spin-ladder operator

$$S_-|J,m\rangle = \sqrt{J(J+1) - m(m-1)}|J,m-1\rangle. \tag{6.34}$$

We have

$$\begin{aligned} \langle\psi|S_-|\psi\rangle &= \frac{1}{2L+1}\sum_{m=-L+1}^{L}\sqrt{J(J+1) - m(m-1)} \\ &= \frac{\sqrt{J(J+1)}}{2L+1}\sum_{m=-L+1}^{L}\left(1 - \frac{m(m-1)}{J(J+1)}\right)^{\frac{1}{2}} \end{aligned}$$

$$
\begin{aligned}
&\geq \frac{J}{2L+1}\sum_{m=-L+1}^{L}\left(1-\frac{m(m-1)}{J(J+1)}\right)^{\frac{1}{2}} \\
&\geq \frac{J}{2L+1}\sum_{m=-L+1}^{L}\left(1-\frac{m(m-1)}{J(J+1)}\right) \\
&= \frac{J}{2L+1}\left(2L-\frac{2L(L^2-1)}{3J(J+1)}\right) \\
&= \frac{NL}{2L+1}-\frac{4L(L^2-1)}{3(2L+1)(N+2)} \\
&\geq \frac{NL}{2L+1}-\frac{2L^2}{3(N+2)}, \qquad (6.35)
\end{aligned}
$$

where we used $-\frac{L(L^2-1)}{2L+1} \geq -\frac{L^2}{2}$ for $L \geq 0$. The second inequality follows from concavity of $\sqrt{1-x}$ for $0 \leq x \leq 1$. Now we can derive the bound for variance

$$
\begin{aligned}
\mathrm{Var}[X^{(N)}] &= \frac{N}{3}-\frac{2}{3}\langle\psi|S_x|\psi\rangle+\frac{4}{3}\Delta S_z^2 \qquad (6.36)\\
&= \frac{N}{3}-\frac{2}{3}\langle\psi|S_x|\psi\rangle+\frac{4}{9}L(L+1) \\
&\leq \frac{N}{3}+\frac{4}{9}L(L+1)-\frac{2}{3}\frac{NL}{2L+1}+\frac{4L^2}{9(N+2)} \\
&= \frac{4}{9}L(L+1)+\frac{N}{3(2L+1)}+\frac{4L^2}{9(N+2)}=Q.
\end{aligned}
$$

For $L=N^\beta$ and $N$ being large, the right-hand side of the last inequality scales as

$$
Q \sim \frac{4}{9}N^{2\beta}+\frac{1}{6}N^{1-\beta}+\frac{4}{9}N^{2\beta-1}. \qquad (6.37)
$$

Since $\beta < 1/2$ the last therm is negligible. Furthermore, we see that the best rate is achieved for $\beta = 1/3$. Finally we get the estimation for the maximal error

$$
s_N \leq \frac{N^{2(\alpha-1)}}{\epsilon^2}Q \sim \frac{11N^{2\alpha-4/3}}{18\epsilon^2} \qquad (6.38)
$$

which is negligible for all $\alpha < 2/3$.

# 7 Conclusions

The main objective of the thesis was to find novel practical verification methods to overcome the difficulties of the standard methods when dealing with large-scale quantum systems. We have presented a probabilistic verification method which shows excellent performance for a variety of quantum states, most of which are of essential importance for the real applications of quantum technologies. In particular, we have shown our method to exhibit:

- A dramatic reduction of the resources needed for reliable detection of quantum correlations.
- A simple tool for the statistical analysis of experimental data.

Finally, the outcome of this doctoral research results in a concrete proof-of-principle experimental demonstration with the six-qubit cluster state. Our findings establish a step forward towards reliable quantum information processing with a very limited amount of experimental data. This is of the vital importance for the next generation of quantum experiments operating at an intermediate scale.

# A Probabilistic entanglement detection: Proofs

## A.1 Proof of the separable bound for $k$ producible and cluster states

As it has been elaborated in the main text, if the input state is a product state $\rho_{prod} = \rho_1 \otimes \cdots \otimes \rho_N$, the local cost functions $F_s$ can be seen as the independent binary (0/1) random variables with $\langle F_s \rangle = p_s \leq p$. We set $s = 1 \ldots K$. We proceed by the standard method for proving the Chernoff bound, i.e. by applying the Markov's inequality [104] (which will be proved in Appendix B)

$$P[X \geq X_0] \leq \frac{\langle X \rangle}{X_0}, \tag{A.1}$$

where $X$ is a positive random variable and $X_0 > 0$. We set $X = F_1 + \cdots + F_K$ and $X_0 = (p+\delta)K = qK$. For any $t > 0$ we have

$$P_{\rho_{prod}}[F_{[N]} = 1] \;\; = \;\; P_{\rho_{prod}}[X \geq X_0] = P_{\rho_{prod}}[e^{tX} \geq e^{tX_0}] \leq \frac{\langle e^{tX} \rangle}{e^{tX_0}}.$$

Thus,

$$P_{\rho_{prod}}[F_{[N]} = 1] \;\; \leq \;\; \prod_{s=1}^{K} \frac{\langle e^{tF_s} \rangle}{e^{tq}} = \prod_{s=1}^{K} \left( \frac{1 - p_s + p_s e^t}{e^{tq}} \right) \leq \left( \frac{1 - p + p e^t}{e^{tq}} \right)^K, \tag{A.2}$$

where the last inequality follows from $p_s \leq p$, i.e. $1 - p_s + p_s e^t \leq 1 - p + p e^t$, for all $s = 1 \ldots K$. The function $f(t) = \frac{1-p+pe^t}{e^{tq}}$ attains the minimal value for $t_m = \log \frac{(1-p)q}{(1-q)p}$ or equivalently $e^{t_m} = \frac{(1-p)q}{(1-q)p}$. If we substitute $e^{t_m}$ in the right hand side of (A.2) we get

$$P_{\rho_{prod}}[F_{[N]} = 1] \;\; \leq \;\; e^{-D(q||p)K} = e^{-D(p+\delta||p)K}. \tag{A.3}$$

The bound holds for any product states $\rho_{prod}$. For a separable state $\rho_{sep} = \sum_k \lambda_k \rho_{prod}^{(k)}$ we have

$$P_{\rho_{sep}}[F_{[N]} = 1] = \sum_k \lambda_k P_{\rho_{prod}^{(k)}}[F_{[N]} = 1] \leq e^{-D(p+\delta||p)K}, \tag{A.4}$$

which follows directly from (A.3). The bound for $k$ producible state is obtained for $K = N$ and $p = \frac{2}{3}$, whereas bound for cluster state follows for $K = L$ and $p = \frac{2}{3}$.

## A.2 General method for generating L-regular partitions of cluster states

Our task is to divide $N$ qubit linear cluster state into regular partitions containing $L$ 4-qubit clusters. Partition is regular if the neighbouring clusters overlap on at most one (border) qubit. Having fixed $N$, we see that number of clusters in the partition is in the interval:

$$[\frac{N}{4}]+1 \;\leq\; L \;\leq\; [\frac{N}{3}], \quad 4 \nmid N \tag{A.5}$$

and

$$[\frac{N}{4}] \;\leq\; L \;\leq\; [\frac{N}{3}], \quad 4 \mid N. \tag{A.6}$$

Now, we can fix $L$ within these intervals and count all possible partitions for a given $L$. First of all, we will introduce $m$-cluster chain, that represents $m$ overlapping neighbouring clusters. Maximal $m$-cluster chain that can fit into partition can either be $m = L$ or $m = L - 1$. However, in the special case when $4 \mid N$ and $L = \frac{N}{4}$, $m = 1$. From the previous example we see that the length $m$ of maximal cluster chain depends on $N$, $L$ and $N \mod 4$.
For a given $N$ and $L$ each partition consists of $a_1$ 1-cluster chains, $a_2$ 2-cluster chains,...and $a_m$ $m$-cluster chains. We can set the following equations:

$$\sum_{j=1}^{m} a_j \;(3j+1) \leq N, \qquad \sum_{j=1}^{m} j \;\; a_j = L. \tag{A.7}$$

From these two equations, we can find all possible values for cluster coefficients $a_j$. The number $n_{a_1,\ldots,a_m}$ of nonequivalent $L$ cluster partitions for one set of cluster coefficients $a_j$ can be obtained from the following formula:

$$n_{a_1,\ldots,a_m} = S_{a_1,\ldots,a_m} \frac{(\sum_j^m a_j)!}{a_1!\ldots a_m!}. \tag{A.8}$$

Here we include all possible permutations without repetition and a symmetry factor $S_{a_1,\ldots,a_m} = \frac{N}{\sum_{j=1}^{m} a_j}$ that counts the number of rotations by an angle $2\pi/N$ which don't produce the same configuration of clusters.
Finally, the total number of $L$ regular partitions is obtained by calculating the numbers $n_{a_1,\ldots,a_m}$ for each allowed set of cluster coefficients and adding those numbers up.

## A.3 Example of the set of regular partitions for $L = 2$ and $N = 6, 7, 8$

Here we list the set of all regular partitions (see main text) for the case $L = 2$ and $N = 6, 7, 8$, with $|\mathcal{C}_2| = 2, 4, 12$, respectively:

$$N = 6: \quad \mathcal{C}_2 = \{\{1,2,3,4\},\{4,5,6,1\}\},\{\{2,3,4,5\},\{5,6,1,2\}\}, \tag{A.9}$$

$$N = 7: \quad \mathcal{C}_2 = \{\{1,2,3,4\},\{4,5,6,7\}\},\{\{2,3,4,5\},\{5,6,7,1\}\}, \tag{A.10}$$
$$\{\{3,4,5,6\},\{6,7,1,2\}\},\{\{4,5,6,7\},\{7,1,2,3\}\},$$

$$N = 8: \quad \mathcal{C}_2 = \{\{1,2,3,4\},\{5,6,7,8\}\},\{\{2,3,4,5\},\{6,7,8,1\}\}, \tag{A.11}$$
$$\{\{3,4,5,6\},\{7,8,1,2\}\},\{\{4,5,6,7\},\{8,1,2,3\}\},$$
$$\{\{1,2,3,4\},\{4,5,6,7\}\},\{\{2,3,4,5\},\{5,6,7,8\}\},$$
$$\{\{3,4,5,6\},\{6,7,8,1\}\},\{\{4,5,6,7\},\{7,8,1,2\}\},$$
$$\{\{5,6,7,8\},\{8,1,2,3\}\},\{\{6,7,8,1\},\{1,2,3,4\}\},$$
$$\{\{7,8,1,2\},\{2,3,4,5\}\},\{\{8,1,2,3\},\{3,4,5,6\}\}.$$

## A.4 Proof of the separable bound and the entanglement bound for the ground states of local Hamiltonians

Firstly, let us analyze the case of a product input state $\rho_{prod} = \rho_1 \otimes \cdots \otimes \rho_N$. The probability of success reads

$$P_{\rho_{prod}}[F_{[N]} = 1] = P_{\rho_{prod}}[H_{[N]} \leq N(\epsilon_s - \delta)] = P_{\rho_{prod}}[h^{(1)} + \cdots + h^{(N)} \leq K], \tag{A.12}$$

where we recognize the probability that the sum of random variables $h^{(1)} + \cdots + h^{(N)}$ precedes certain bound of $K = \frac{N}{M^L}(\epsilon_s - \delta)$ with $0 < \delta < \epsilon_s - \epsilon_0 = g_E$. Unlike the case of cluster states, the variables $h^{(k)}$ are not independent (for the case of product inputs), therefore the straightforward application of Chernoff bound is not possible. However, as all $h^{(k)}$ depend only on finite number of $L$ "neighboring" variables, we expect to obtain the bound similar to the one for $k$ producible states.

In order to prove the target inequality, we will use the help of the McDiarmid's inequality [113]:

**Theorem A.1.** Let $x_1, \ldots, x_N$ be independent random variables taking values in the set $\mathcal{X}$. Further, let the function $S_{[N]} : \mathcal{X}^N \mapsto \mathbb{R}$ satisfy

$$\left|S_{x_1 \ldots x_k \ldots x_N} - S_{x_1 \ldots x'_k \ldots x_N}\right| \leq \alpha_k \tag{A.13}$$

for all $x_1, \ldots, x_N, x'_k \in \mathcal{X}$, then

$$P[S_{[N]} - \langle S_{[N]} \rangle \geq Q] \leq \exp\left[\frac{-2Q^2}{\sum_{k=1}^{N} \alpha_k^2}\right], \tag{A.14}$$

for all $Q > 0$.

*Proof.* Firstly, note that for the case of product inputs, the random variables $\{x_1, \ldots, x_N\}$ are independent because the probability distribution

$$P_{x_1 \ldots x_N} = \frac{1}{M^N} \operatorname{Tr} \rho_{prod} E_{x_1}^{(1)} \ldots E_{x_N}^{(N)} \tag{A.15}$$

is factorizable. We set $S_{[N]} = -(h^{(1)} + \cdots + h^{(N)})$. Furthermore, we label $\mathcal{N}(k) = \{n_{k,1}, \ldots, n_{k,L}\}$ the set of all neighbors of $k$ and we put $|h^{(k)}_{x_1 \ldots x_L}| \leq h_{\max}$ for all $k$ and all $x_k$. Since we are dealing with the finite-dimensional Hilbert spaces, $h_{\max}$ is always finite and well defined. We apply the condition for the McDiarmid's theorem and we get

$$\begin{aligned} \left| S_{x_1 \ldots x_k \ldots x_N} - S_{x_1 \ldots x'_k \ldots x_N} \right| &= \left| - \sum_{l \in \mathcal{N}(k)} h^{(l)}_{x_{n_{l,1}} \ldots x_{n_{l,L}}} + h^{(l)}_{x'_{n_{l,1}} \ldots x'_{n_{l,L}}} \right| \\ &\leq \sum_{l \in \mathcal{N}(k)} \left| h^{(l)}_{x_{n_{l,1}} \ldots x_{n_{l,L}}} \right| + \left| h^{(l)}_{x'_{n_{l,1}} \ldots x'_{n_{l,L}}} \right| \\ &\leq 2L h_{\max}, \end{aligned} \tag{A.16}$$

thus $\alpha_k = 2L h_{\max}$. The inequality (A.14) reads

$$P_{\rho_{prod}}[S_{[N]} - \langle S_{[N]} \rangle \geq Q] \leq \exp\left[\frac{-Q^2}{2NL^2 h_{\max}^2}\right], \tag{A.17}$$

for all product states $\rho_{prod}$ and all $Q > 0$. Now, we shall obtain the bound on probability of success (A.12). We have

$$\begin{aligned} P_{\rho_{prod}}[F_{[N]} = 1] &= P_{\rho_{prod}}[h^{(1)} + \cdots + h^{(N)} \leq K] \\ &= P_{\rho_{prod}}[S_{[N]} - \langle S_{[N]} \rangle \geq -K - \langle S_{[N]} \rangle] \\ &\leq \exp\left[\frac{-(K + \langle S_{[N]} \rangle)^2}{2NL^2 h_{\max}^2}\right] \\ &\leq \exp\left[\frac{-(K - \frac{N}{M^L}\epsilon_s)^2}{2NL^2 h_{\max}^2}\right] \\ &= \exp\left[-N\kappa^2\delta^2\right], \end{aligned} \tag{A.18}$$

where $\kappa^2 = 1/(2M^{2L}L^2 h_{\max}^2)$ and $\delta > 0$. The second inequality follows from the separable bound $\langle S_{[N]} \rangle \leq -\frac{N}{M^L}\epsilon_s$. □

On the other hand, if the ground state of $H$ is prepared, we show that entangle-

ment bound holds. Recall that $H_{[N]} = M^L \sum_{k=1}^N h^{(k)}$, thus $\langle H_{[N]} \rangle = M^L \sum_{k=1}^N \langle h^{(k)} \rangle$. We start by showing that the variance $\mathrm{Var}[H_{[N]}]$ grows linearly with $N$. By definition $\mathrm{Var}[H_{[N]}] = \langle H_{[N]}^2 \rangle - \langle H_{[N]} \rangle^2$ which we transform into

$$\mathrm{Var}[H_{[N]}] = \langle H_{[N]}^2 \rangle - \langle H^2 \rangle + \langle H_{[N]} \rangle^2 - \langle H \rangle^2 + \mathrm{Var}[H]. \tag{A.19}$$

As $\langle H_{[N]} \rangle = \langle H \rangle$ and $\mathrm{Var}[H] = 0$ (the state $|\psi_0\rangle$ is the ground-state of $H$), we get $\mathrm{Var}[H_{[N]}] = \langle H_{[N]}^2 \rangle - \langle H^2 \rangle$. The expression for the variance reads

$$\begin{aligned} \mathrm{Var}[H_{[N]}] &= \langle H_{[N]}^2 \rangle - \langle H^2 \rangle \\ &= M^{2L} \left\langle \left( \sum_{k=1}^N h^{(k)} \right)^2 \right\rangle - \langle H^2 \rangle \\ &= \sum_{j,k=1}^N M^{2L} \langle h^{(j)} h^{(k)} \rangle - \langle H^{(j)} H^{(k)} \rangle \\ &= \sum_{j,k \in *} M^{2L} \langle h^{(j)} h^{(k)} \rangle - \langle H^{(j)} H^{(k)} \rangle, \end{aligned} \tag{A.20}$$

where $*$ refers to the set of "crossing terms" only, i.e. those pairs $(j,k)$ that satisfy $j \in \mathcal{N}(k)$ or $k \in \mathcal{N}(j)$ ($j$ is in the "neighborhood" of $k$ or $k$ is in the "neighborhood" of $j$). For "non-crossing terms", we have $M^{2L} \langle h^{(j)} h^{(k)} \rangle = M^{2L} \langle h^{(j)} \rangle \langle h^{(k)} \rangle = \langle H^{(j)} \rangle \langle H^{(k)} \rangle = \langle H^{(j)} H^{(k)} \rangle$, thus the sum vanishes. Note that the total number of "crossing terms" is at most $2NL$, i.e. $\sum_{j,k \in *} 1 \leq 2NL$. We can bound particular terms in the sum as

$$\begin{aligned} |\langle h^{(j)} h^{(k)} \rangle| &= |\frac{1}{M^N} \langle \psi_0 | \sum_{x_1 \ldots x_N} h^{(j)}_{x_{n_{j,1}}, \ldots, x_{n_{j,L}}} h^{(k)}_{x_{n_{k,1}}, \ldots, x_{n_{k,L}}} E^{(1)}_{x_1} \ldots E^{(N)}_{x_N} | \psi_0 \rangle| \\ &\leq \frac{1}{M^N} \sum_{x_1 \ldots x_N} |h^{(j)}_{x_{n_{j,1}}, \ldots, x_{n_{j,L}}}| |h^{(k)}_{x_{n_{k,1}}, \ldots, x_{n_{k,L}}}| \langle \psi_0 | E^{(1)}_{x_1} \ldots E^{(N)}_{x_N} | \psi_0 \rangle \\ &\leq \frac{A^2}{M^N} \sum_{x_1 \ldots x_N} \langle \psi_0 | E^{(1)}_{x_1} \ldots E^{(N)}_{x_N} | \psi_0 \rangle = A^2, \end{aligned} \tag{A.21}$$

where $A = \max_{k,x_s} |h^{(k)}_{x_{n_{k,1}}, \ldots, x_{n_{k,L}}}|$. Here we used $\sum_{x_k} E^{(k)}_{x_k} = \sum_{m_k, i_k} E^{(k)}_{m_k, i_k} = M \mathbb{1}^{(k)}$. Furthermore, if we set $B = \max_k |\langle \psi_0 | H^{(k)} | \psi_0 \rangle|$, we get $|\langle H^{(j)} H^{(k)} \rangle| \leq B^2$, by the Cauchy-Schwarz inequality. Finally, we apply the inequality $|a - b| \leq |a| + |b|$ and by using the expression for variance given above we get

$$\mathrm{Var}[H_{[N]}] = \left| \sum_{j,k \in *} M^{2L} \langle h^{(j)} h^{(k)} \rangle - \langle H^{(j)} H^{(k)} \rangle \right| \tag{A.22}$$

$$
\begin{aligned}
&\leq \sum_{j,k\in *} M^{2L}|\langle h^{(j)}h^{(k)}\rangle| + |\langle H^{(j)}H^{(k)}\rangle| \\
&\leq \sum_{j,k\in *} M^{2L}A^2 + B^2 \\
&\leq 2NL(M^{2L}A^2 + B^2) = \beta^2 N,
\end{aligned}
$$

with $\beta^2 = 2L(M^{2L}A^2 + B^2)$.

Finally, the probability of success reads

$$
\begin{aligned}
P_{\psi_0}[F_{[N]} = 1] &= P_{\psi_0}[H_{[N]} \leq M^L K] \\
&= P_{\psi_0}[H_{[N]} - \langle H_{[N]}\rangle \leq N(\epsilon_s - \epsilon_0 - \delta)] \\
&= P_{\psi_0}[H_{[N]} - \langle H_{[N]}\rangle \leq N(g_E - \delta)] \\
&\geq P_{\psi_0}[H_{[N]} - \langle H_{[N]}\rangle < N(g_E - \delta)] \\
&= 1 - P_{\psi_0}[H_{[N]} - \langle H_{[N]}\rangle \geq N(g_E - \delta)] \\
&\geq 1 - P_{\psi_0}[H_{[N]} - \langle H_{[N]}\rangle \geq N(g_E - \delta)] - P_{\psi_0}[H_{[N]} - \langle H_{[N]}\rangle \\
&\leq -N(g_E - \delta)] \\
&= 1 - P_{\psi_0}[|H_{[N]} - \langle H_{[N]}\rangle| \geq N(g_E - \delta)] \\
&\geq 1 - \frac{\mathrm{Var}[H_{[N]}]}{N^2(g_E - \delta)^2} \\
&\geq 1 - \frac{\beta^2}{N(g_E - \delta)^2}.
\end{aligned}
\tag{A.23}
$$

The second last inequality follows from the Chebyshev's inequality [104].

# B Basic elements of Probability Theory

*Most of the content in this appendix is written using [114].*
Consider an experiment with a probabilistic outcome. The set of outcomes is called the sample space, and we will denote it with $\mathcal{S}$. All possible subsets of $\mathcal{S}$ are events and will be denoted by Latin letters $\{A, B, C...\}$. We are usually interested in the relations between events of the same sample space. We will define the most common relations: union, intersection and as a consequence, mutual independence and mutual exclusiveness of events.

**Definition B.1.** The union of two events $A$ and $B$ denoted by $A \cup B$ is a new event which occurs if any of the events in the union occur.

**Definition B.2.** The intersection of two events $A$ and $B$ is a new event $A \cap B$ that occurs if all the events in the intersection occur.

**Definition B.3.** Two events $A$ and $B$ are mutually exclusive if their intersection is empty $A \cap B = \emptyset$.

**Definition B.4.** An event $A$ is said to be independent of an event $B$ if $P(A \cap B) = P(A)P(B)$, where $P$ is the probability for the corresponding event to happen.

Now, we will state three basic axioms of probability.

1. Probability of event $A$ from the set $\mathcal{S}$ is positive and smaller than 1: $0 \leq P(A) \leq 1$.
2. Total probability of the complete set of events $\mathcal{S}$ is 1.
3. For any sequence of mutually exclusive events $\{A_1, A_2, ..., A_N\}$, $P(\cup_{i=1}^{N} A_i) = \sum_{i=1}^{N} P(A_i)$.

We are often interested in considering multiple outcomes of an experiment. Let us take an example of a coin toss and three tosses. For instance, in this particular example we could ask what is the probability to get three times tails in a row? In order to formalize the answer to that question, we need to introduce the notion of a random variable.

**Definition B.5.** A random variable is a function $X$ that for every point $\xi$ in the sample space $\mathcal{S}$ allocates a unique real value $X(\xi)$.

If a random variable is discrete, i.e. having a countable number of possible values, then correspondence is given by probability mass function. On the other hand, if a random variable is continuous, meaning that it has a continuous domain, we will use probability density function.

**Definition B.6.** For a discrete random variable $X$ a probability mass function $p(x)$ is defined by $p(x) = P(X = x)$.

**Definition B.7.** For a continuous random variable $X$ a probability density function $f(x)$ is defined such that for a subset $\mathcal{B} \in \mathbb{R}$: $P(X \in \mathcal{B}) = \int_{\mathcal{B}} f(x)\mathrm{d}x$.

Furthermore, we can introduce distribution function that measures if a random variable is smaller than a certain value.

**Definition B.8.** For a random variable $X$, the distribution function $F$ is defined by $F(x) = P(X \leq x)$.
For continuous random variables the last equation is as follows $F(x) = \int_{-\infty}^{x} f(t)\mathrm{d}t$.

Now, let define some basic features of a random variable, such as its average and spread.

**Definition B.9.** If $X$ is a discrete random variable with the probability mass function $p(x)$, its expected value $\mathrm{E}[X]$ is defined as $\mathrm{E}[X] = \sum_x xp(x)$.

**Definition B.10.** If $X$ is a continuous random variable with the probability density function $f(x)$, then its expected value is given by $\mathrm{E}[X] = \int_{-\infty}^{+\infty} xf(x)\mathrm{d}x$.

**Definition B.11.** If $X$ is a random variable having the mean value $\mathrm{E}[X]$, then the variance of $X$, $\mathrm{Var}(X)$ is given by $\mathrm{Var}(X) = \mathrm{E}[(X - \mathrm{E}[X])^2]$.

Our next task is to see how the mean value and variance are changed when we transform random variable. We will prove several interesting properties.

**Lemma B.1.** If $a$ and $b$ are constants, then

$$\mathrm{E}[aX + b] = a\mathrm{E}[X] + b \tag{B.1}$$

and

$$\mathrm{Var}(aX + b) = a^2\mathrm{Var}(X) \tag{B.2}$$

*Proof.*

$$\mathrm{E}[aX + b] = \sum_x (ax + b)p(x) = \sum_x axp(x) + \sum_x bp(x) = a\mathrm{E}[X] + b. \tag{B.3}$$

For simplicity, we will take $\mathrm{E}[X] = \mu$.

$$\mathrm{Var}[aX + b] = \mathrm{E}[(aX + b - a\mu - b)^2] = \mathrm{E}[a^2(X - \mu)^2] = a^2\mathrm{E}[(X - \mu)^2] = a^2\mathrm{Var}[X]. \tag{B.4}$$

□

**Lemma B.2.** If $X$ is a discrete random variable taking values $x_i$, $i \in \{1, ..., N\}$, with corresponding probabilities $p(x_i)$, then for any real-valued function $g$ we have

$$\mathrm{E}[g(X)] = \sum_i g(x_i)p(x_i). \tag{B.5}$$

*Proof.* We gather all the terms having the same value of $g(x_i) = y_k$. Therefore, we can write

$$\sum_i g(x_i)p(x_i) = \sum_k y_k \sum_{i:g(x_i)=y_k} p(x_i) = \sum_k y_k P(g(X) = y_k) = \mathrm{E}[g(X)]. \tag{B.6}$$

□

We can now derive simple consequence of lemma B.2.

**Lemma B.3.** If $X$ and $Y$ are discrete random variables with finite expected values, then

$$\mathrm{E}[X + Y] = \mathrm{E}[X] + \mathrm{E}[Y]. \tag{B.7}$$

*Proof.*

$$\begin{aligned} \mathrm{E}[X+Y] &= \sum_i \sum_j (x_i + y_j) P(X = x_i, Y = y_j) \\ &= \sum_i \sum_j x_i P(X = x_i, Y = y_j) + \sum_i \sum_j y_j P(X = x_i, Y = y_j) \\ &= \sum_i x_i P(X = x_i) + \sum_j y_j P(Y = y_j) = \mathrm{E}[X] + \mathrm{E}[Y]. \end{aligned} \tag{B.8}$$

□

One should be aware that we could prove all this properties for continuous random variables, just by changing discrete sum to the integral.

**Lemma B.4.** If $X$ and $Y$ are independent random variables, then

$$\mathrm{E}[XY] = \mathrm{E}[X]\mathrm{E}[Y] \tag{B.9}$$

and

$$\mathrm{Var}(X + Y) = \mathrm{Var}(X) + \mathrm{Var}(Y). \tag{B.10}$$

*Proof.* We will work out this proof for continuous random variables. In that case joint probability density function factorizes in probability density functions of random variables $X$ and $Y$

$$h(x, y) = f(x)g(y). \tag{B.11}$$

Thus, we have

$$\mathrm{E}[XY] = \int\int xyf(x)g(y)\mathrm{d}x\mathrm{d}y = \left(\int xf(x)\mathrm{d}x\right)\left(\int yg(y)\mathrm{d}y\right) = \mathrm{E}[X]\mathrm{E}[Y]. \tag{B.12}$$

Now, let us take $\mathrm{E}[X] = \mu$ and $\mathrm{E}[Y] = \eta$.

$$\mathrm{Var}(X+Y) = \mathrm{E}[(X+Y)^2] - (\mu+\eta)^2$$

$$
\begin{aligned}
&= \mathrm{E}[X^2] + \mathrm{E}[Y^2] + 2\mathrm{E}[XY] - \mu^2 - \eta^2 - 2\mu\eta \\
&= \mathrm{E}[X^2] - \mu^2 + \mathrm{E}[Y^2] - \eta^2 = \mathrm{Var}(X) + \mathrm{Var}(Y). \qquad \text{(B.13)}
\end{aligned}
$$

In the last step we used that $\mathrm{E}[XY] = \mu\eta$. □

We want to extend the concept of the mean value to the case where we are dealing with multiple random variables. In this situation, we calculate the sample mean.

**Definition B.12.** Let $X_1, ..., X_N$ be independent and identically distributed random variables with distribution function $F$ and expected value $\mu$. Such a sequence constitutes a sample from the distribution $F$. Given a sample, we define the sample mean $\hat{X}$ as follows

$$\hat{X} = \frac{1}{N} \sum_{i=1}^{N} X_i. \qquad \text{(B.14)}$$

Therefore we have

$$\mathrm{E}[\hat{X}] = \frac{1}{N} \sum_{i=1}^{N} \mathrm{E}[X_i]. \qquad \text{(B.15)}$$

The expectation values of powers of a random variable are called higher moments of a random variable.

**Definition B.13.** The $k$-th moment of a random variable $X$ is $\mathrm{E}[X^k]$, $k \in \mathbb{N}$.

For calculation of higher moments, it is very convenient to introduce the notion of moment generating function.

**Definition B.14.** The moment generating function $M(t)$ of a random variable $X$ is defined for all real values of $t$ by

$$M(t) = \mathrm{E}[e^{tX}]. \qquad \text{(B.16)}$$

For discrete random variable $X$ with probability mass function $p(x)$ it becomes:

$$\sum_x \mathrm{e}^{tx} p(x). \qquad \text{(B.17)}$$

On the other hand, if we deal with continuous random variable $X$, we have

$$\int_{-\infty}^{+\infty} \mathrm{e}^{tx} f(x) \mathrm{d}x. \qquad \text{(B.18)}$$

There are several interesting properties of moment generating function that will be exploited frequently throughout our derivation of the Central Limit Theorem. We will not derive them in details, just briefly comment on them, as they are direct consequences of lemmas already proved.
For independent random variables $X$ and $Y$, the moment generating function is

$$M_{X+Y}(t) = \mathrm{E}[\mathrm{e}^{t(X+Y)}] = \mathrm{E}[\mathrm{e}^{tX}]\mathrm{E}[\mathrm{e}^{tY}] = M_X(t)M_Y(t). \tag{B.19}$$

More importantly, all moments of a random variable can be calculated by differentiating moment generating function and evaluating its value at $t = 0$:

$$M^{(k)}(0) = \frac{\mathrm{d}^k}{\mathrm{d}t^k} M(t)|_{t=0} = \mathrm{E}[X^k]. \tag{B.20}$$

The last equation can be proved by using the method of induction.

In particular, we are interested in the normal random variable because of its specific properties that will lead us to the CLT.

**Definition B.15.** $X$ is normal random variable determined by the mean value $\mu$ and variance $\sigma^2$, if the probability density function of $X$ is given by

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}}. \tag{B.21}$$

By direct calculation, we can find the moment generating function of the normal random variable, i.e.

$$M_X(t) = \mathrm{E}[\mathrm{e}^{tX}] = \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{+\infty} \mathrm{e}^{tx} \mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}} \mathrm{d}x = \mathrm{e}^{\frac{\sigma^2 t^2}{2} + \mu t}. \tag{B.22}$$

Now, we will present some bounds on the distribution in terms of its mean value and variance.

**Lemma B.5.** *(Markov's inequality.)* If $X$ is a random variable that takes only positive values, then for any value $x_0 > 0$,

$$P(X \geq x_0) \leq \frac{\mathrm{E}[X]}{x_0}. \tag{B.23}$$

*Proof.* We define new random variable $Y$ such that

$$Y = \begin{cases} 1, & \text{for } X \geq x_0, \\ 0, & \text{otherwise.} \end{cases}$$

We distinct two cases:

- If $Y = 1$, then $X \geq x_0$, thus $Y \leq \frac{X}{x_0}$ since $X \geq 0$ and $x_0 > 0$.
- If $Y = 0$, then $X < x_0$, but $\frac{X}{x_0} \geq 0$, as $X \geq 0$ and $x_0 > 0$.

We see that the inequality $Y \leq \frac{X}{x_0}$ holds in general. Taking expectations of the preceding inequality gives

$$\mathrm{E}[Y] \leq \frac{\mathrm{E}[X]}{x_0}. \tag{B.24}$$

By examination of $\mathrm{E}[Y]$ we get:

$$\mathrm{E}[Y] = P(X \geq x_0) \tag{B.25}$$

which proves the result. □

Using Markov's inequality, we can prove more complicated bounds, such as Chebyshev's inequality.

**Lemma B.6.** *(Chebyshev's inequality.)* If X is a random variable with finite mean $\mu$ and variance $\sigma^2$ , then, for any value $\kappa > 0$

$$P\{|X - \mu| \geq \kappa^2\} \leq \frac{\sigma^2}{\kappa^2} \tag{B.26}$$

*Proof.* As $(X - \mu)^2$ is nonnegative random variable, we apply Markov's inequality with $x_0 = \kappa^2$ and obtain

$$P\{(X - \mu)^2 \geq \kappa^2\} \leq \frac{\mathrm{E}[(X - \mu)^2]}{\kappa^2}. \tag{B.27}$$

Here we notice that $(X - \mu)^2 \geq \kappa^2$ iff $|X - \mu| \geq \kappa$, so we rewrite the last equation

$$P\{|X - \mu| \geq \kappa\} \leq \frac{\mathrm{E}[(X - \mu)^2]}{\kappa^2} = \frac{\sigma^2}{\kappa^2}, \tag{B.28}$$

which completes the proof. □

**Theorem B.1.** *The Weak Law of Large Numbers.* Let $\{X_1, X_2, ..., X_N\}$ be a sequence of independent and identically distributed random variables, each having finite mean value $\mathrm{E}[X_i] = \mu$ and variance $\sigma^2$. Then, for any $\epsilon > 0$

$$P\left\{\left|\frac{X_1 + X_2 + ... + X_N}{N} - \mu\right| \geq \epsilon\right\} \to 0, \quad \text{as} \quad N \to \infty. \tag{B.29}$$

*Proof.* In order to prove the theorem, we will make the additional assumption that the random variables have a finite variance $\sigma^2$. Since $\mathrm{E}\left[\frac{X_1+...+X_N}{N}\right] = \mu$ and $\mathrm{Var}\left(\frac{X_1+...+X_N}{N}\right) = \frac{\sigma^2}{N}$, from Chebyshev's inequality follows that

$$P\left\{|\frac{X_1 + ... + X_N}{N} - \mu| \geq \epsilon\right\} \leq \frac{\sigma^2}{N\epsilon^2}. \tag{B.30}$$

If we take the limit of large $N$, the result is proven. □

**Definition B.16.** Let $\{X_1, X_2, ...\}$ be a sequence of random variables with cumulative distribution functions $\{F_1, F_2, ...\}$ and let $X$ be a random variable with cumulative distribution $F$. We say that sequence $\{X_N\}$ converges in distribution to $X$ if

$$\lim_{N\to\infty} F_N(x) = F(x) \tag{B.31}$$

at every point at which $F$ is continuous.

Direct consequence of convergence in distribution is the next lemma, that we will use for the proof of the CLT.

**Lemma B.7.** *Continuity Theorem.* Let $\{X_N\}$ be a sequence of random variables with cumulative distribution functions $\{F_N(x)\}$ and moment generating functions $\{M_N(t)\}$. Let $X$ be a random variable with cumulative distribution function $F(x)$ and moment generating function $M(t)$. If

$$M_N(t) \to M(t) \tag{B.32}$$

for all $t$ in an open interval containing zero, then

$$F_N(x) \to F(x) \tag{B.33}$$

at all continuity points of $F$.

**Theorem B.2.** Let $\{X_1, X_2, ..\}$ be a sequence of independent and identically distributed random variables, each having mean $\mu$ and variance $\sigma^2$. Let us define

$$S_N = \sum_{i=1}^{N} X_i. \tag{B.34}$$

Then

$$\frac{S_N - N\mu}{\sigma\sqrt{N}} \tag{B.35}$$

converges to the standard normal distribution $\mathcal{N}(0,1)$ as $N \to \infty$.
Equivalently, for $x_0 \in \mathbb{R}$

$$P\left\{\frac{S_N - N\mu}{\sigma\sqrt{N}} \leq x_0\right\} \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x_0} \mathrm{e}^{-x^2/2} \mathrm{d}x \tag{B.36}$$

as $N \to \infty$.

*Proof.* Without loss of generality, we will assume that $\mu = 0$. We define new random variable $Z_N$ and since $S_N$ is sum of $N$ i.i.d. random variables, moment generating functions are

$$M_{S_N}(t) = (M(t))^N \tag{B.37}$$

and

$$M_{Z_N}(t) = (M(\frac{t}{\sigma\sqrt{N}}))^N, \tag{B.38}$$

Taking a Taylor series expansion of $M(t)$ around 0 gives

$$\begin{aligned} M(t) &= M(0) + M'(0)t + \frac{1}{2}M''(0)t^2 + O(t^3) \\ &= 1 + \frac{1}{2}\sigma^2 t^2 + O(t^3), \end{aligned} \tag{B.39}$$

as we have $M(0) = 1$, $M'(0) = \mu = 0$ and $M''(0) = \sigma^2$.
Therefore we have

$$\begin{aligned} M(\frac{t}{\sigma\sqrt{N}}) &= 1 + \frac{1}{2}\sigma^2(\frac{t}{\sigma\sqrt{N}})^2 + O((\frac{t}{\sigma\sqrt{N}})^3) \\ &= 1 + \frac{t^2}{2N} + O(\frac{1}{N^{3/2}}). \end{aligned} \tag{B.40}$$

This gives

$$M_{Z_N}(t) = (1 + \frac{t^2}{2N} + O(\frac{1}{N^{3/2}}))^N \to_{N\to\infty} \mathrm{e}^{t^2/2}. \tag{B.41}$$

which by B.7 proves the statement of the theorem. □

# Bibliography


[1] Harrow, A. W. and Montanaro, A. Quantum computational supremacy. *Nature* **549**(7671), 203 (2017).

[2] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review* **41**(2), 303-332 (1999).

[3] Castelvecchi, D. Quantum computers ready to leap out of the lab in 2017. *Nature* **541**, 9 (2017).

[4] Dowling, J. P. and Milburn, G. J. Quantum technology: the second quantum revlution. *Philos. Trans. R. Soc. Lond. A: Math., Phys. Eng. Sci.* **361**, 1655 (2003).

[5] Preskill, J. Quantum Computing in the NISQ era and beyond. *Quantum* **2**, 79 (2018).

[6] Yan, B. et al. Realizing a lattice spin model with polar molecules. *Nature* **501**, 521(2013).

[7] Hart, R. A. et al. Observation of anti-ferromagnetic correlations in the Hubbard model with ultra-cold atoms. *Nature* **519**, 211 (2015).

[8] Takei, N. et al. Direct observation of ultrafast many-body electron dynamics in an ultra-cold Rydberg gas. *Nat. Commun.* **7**, 13449 (2016).

[9] Campbell, S. L. et al. A Fermi-degenerate three-dimensional optical lattice clock. *Science* **358**(6359), 90-94 (2017).

[10] Britton, J. W. et al. Engineered two-dimensional Ising interactions in a trapped-ion quantum simulator with hundreds of spins. *Nature* **484**, 489 (2012).

[11] Paraoanu, G. S. Recent progress in quantum simulation using superconducting circuits. *Journal of Low Temperature Physics* **175**(5-6), 633-654 (2014).

[12] Arrazola, J. M. et al. Reliable entanglement verification. *Phys. Rev. A.* **87**, 062331 (2013).

[13] Yang, T.H., Vertesi, T., Bancal, J. D., Scarani, V. and Navascués, M. Robust and versatile black-box certification of quantum devices. *Phys. Rev. Lett.* **113**, 040401 (2014).

[14] Christandl, M. and Renner, R. Reliable quantum state tomography. *Phys. Rev. Lett.* **109**, 120403 (2012).

[15] Fitzsimons, J. F. and Kashefi, E. Unconditionally verifiable blind quantum computation. *Phys. Rev. A.* **96**, 012303 (2017).

[16] Tura, J., Augusiak, R., Sainz, A. B., Vértesi, T., Lewenstein, M. and Acín, A. Detecting nonlocality in many-body quantum states. *Science* **344** (6189), 1256-1258 (2014).

[17] Šupić, I., and Bowles, J. Self-testing of quantum systems: a review. arXiv preprint arXiv:1904.10042 (2019).

[18] Von Neumann, J., Mathematical foundations of quantum mechanics. Princeton University Press, 1996.

[19] Nielsen, M. A. and Chuang, I.L. Quantum Computation and Quantum Information. Cambridge University Press, 2010, ISBN: 9781107002173.

[20] Paris, M. G. The modern tools of quantum mechanics. *The European Physical Journal Special Topics* **203**(1), 61-86 (2012).

[21] Nielsen, M. A. Conditions for a Class of Entanglement Transformations. *Phys. Rev. Lett.* **83**, 436 (1999).

[22] Chitambar, E., Leung, D., Mančinska, L., Ozols, M. and Winter, A. Everything You Always Wanted to Know About LOCC (But Were Afraid to Ask). *Commun. Math. Phys.* **328**, 303-326 (2014).

[23] Wootters, W. K. Entanglement of formation and concurrence. *Quantum Information & Computation* **1**(1), 27-44 (2001).

[24] Gühne, O. and Tóth, G. Entanglement detection. *Phys. Rep.* **474**, 1 (2009).

[25] Bell, J. S. On the Einstein Podolsky Rosen paradox. *Physics* **1**(3), 195 (1964).

[26] Einstein, A., Podolsky, B. and Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* **47**, 777 (1935).

[27] Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. and Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419 (2014).

[28] Clauser, J. F., Horne, M. A., Shimony, A. and Holt, R. A. Proposed experiment to test local hidden-variable theories. *Physical review letters* **23**(15), 880 (1969).

[29] Friis, N., Vitagliano, G., Malik, M. and Huber, M. Entanglement Certification - From Theory to Experiment. *Nature Reviews Physics* **1**(1), 72-87 (2019).

[30] Bisio, A., Chiribella, G., D'Ariano, G. M., Facchini, S. and Perinotti, P. Optimal quantum tomography. *IEEE J. Sel. Top. Quant. Elect.* **15**, 1646 (2009).

[31] Horodecki, M., Horodecki, P. and Horodecki, R. Separability of mixed states: necessary and sufficient conditions. *Phys. Letts. A* **223**, 1 (1996).

[32] Terhal, B. M. Detecting quantum entanglement. *Theor. Comput. Sci.* **287**, 313 (2002).

[33] Brukner, Č. and Vedral, V. Macroscopic thermodynamical witnesses of quantum entanglement. arXiv preprint quant-ph/0406040 (2004).

[34] Tóth, G. Entanglement witnesses in spin models. *Phys. Rev. A.* **71**, 010301 (2005).

[35] Dowling, M. R., Doherty, A. C. and Bartlett, S. D. Energy as an entanglement witness for quantum manybody systems. *Phys. Rev. A* **70**, 062113 (2004).

[36] Knips, L., Schwemmer, C., Klein, N., Wieniak, M. and Weinfurter, H. Multipartite entanglement detection with minimal effort. *Phys. Rev. Lett.* **117**, 210504 (2016).

[37] Gühne, O. and Lütkenhaus, N. J. Nonlinear entanglement witnesses, covariance matrices and the geometry of separable states. *Phys. Conf. Ser.* **67**, 012004 (2007).

[38] Badziag, P., Brukner, Č., Laskowski, T., Paterek, T. and Żukowski, M. Experimentally friendly geometrical criteria for entanglement. *Phys. Rev. Lett.* **100**, 140403 (2008).

[39] Arrazola, J. M., Gittsovich, O. and Lütkenhaus, N. Accessible nonlinear entanglement witnesses. *Phys. Rev. A.* **85**, 062327 (2012).

[40] Wang, Z., Singh, S. and Navascués, M. Entanglement and nonlocality in infinite 1D systems. **Phys. Rev. Lett. 118**(23), 230401 (2017).

[41] Baccari, F., Cavalcanti, D., Wittek, P. and Acín, A. Efficient device-independent entanglement detection for multipartite systems. *Phys. Rev. X* **7**(2), 021042 (2017).

[42] Pezzé, L. and Smerzi, A. Entanglement, nonlinear dynamics, and the Heisenberg limit. *Phys. Rev. Lett.* **102**, 100401 (2009).

[43] Hyllus, P. et al. Fisher information and multipartite entanglement. *Phys. Rev. A* **85**, 022321 (2012).

[44] Tóth, G. Multipartite entanglement and high-precision measurements. *Phys. Rev. A.* **85**, 022322 (2012).

[45] Pezzé, L., Li, Y., Li, W. and Smerzi, A. Witnessing entanglement without entanglement witness operators. *Proc. Natl. Acad. Sci.* **113**, 11459 (2016).

[46] Tran, M. C., Dakić, B., Arnault, F., Laskowski, W. and Paterek, T. Quantum entanglement from random measurements. *Phys. Rev. A.* **92**, 050301 (2015).

[47] Tran, M. C., Dakić, B., Laskowski, W. and Paterek, T. Correlations between outcomes of random measurements. *Phys. Rev. A.* **94**, 042302 (2016).

[48] Szangolies, J., Kampermann, H. and Bruß, D. Detecting entanglement of unknown quantum states with random measurements. *New. J. Phys.* **17**, 113051 (2015).

[49] Horodecki, R., Horodecki, P., Horodecki, M. and Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* **81**, 865 (2009).

[50] Chruściński, D. and Sarbicki, G. Entanglement witnesses: construction analysis and classification. *J. Phys. A Math. Theor.* **47**, 483001 (2014).

[51] Reed, M. and Simon, B. Methods of Modern Mathematical Physics I: Functional Analysis. Academic Press, New York and London, 1972.

[52] Xu, P. et al. Implementation of a measurement-device-independent entanglement witness.*Phys. Rev. Lett.* **112**(14), 140506 (2014).

[53] Wang, X. L. et al. Experimental ten-photon entanglement. *Phys. Rev. Lett.* **117**, 210502 (2016).

[54] Blume-Kohout, R. Optimal, reliable estimation of quantum states. *New J. Phys.* **12**, 043034 (2010).

[55] Jungnitsch, B. et al. Increasing the statistical significance of entanglement detection in experiments. *Phys. Rev. Lett.* **104**, 210401 (2010).

[56] Banaszek, K., D'Ariano, G. M., Paris, M. G. A. and Sacchi, M. F. Maximum-likelihood estimation of the density matrix. *Phys. Rev. A* **61**, 010304 (1999).

[57] Schack, R., Brun, T. A. and Caves, C. M. Quantum Bayes rule. *Phys. Rev. A* **64**, 014305 (2001).

[58] Helstrom, C. W. Quantum Detection and Estimation Theory. Academic Press, New York, 1976. ISBN: 0123400503.

[59] Paris, M. and Rehacek, J. Quantum State Estimation. *Lecture Notes in Physics*, vol. 649, Springer-Verlag, Heidelberg, 2004.

[60] H"affner, H. et al. Scalable multi-particle entanglement of trapped ions. *Nature* **438**, 643-646 (2005).

[61] Tillé, Y. in *International Encyclopedia of Statistical Science*, (ed. Lovric, M.) 1273–1274, Springer, Berlin, Heidelberg, 2011.

[62] Buhrman, H., Cleve, R., Massar, S. and de Wolf, R. Nonlocality and communication complexity. *Rev. Mod. Phys.* **82**, 665 (2010).

[63] Gross, D., Liu, Y.-K., Flammia, S. T., Becker, S. and Eisert, J. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.* **105**, 150401 (2010).

[64] Flammia, S. T. and Liu, Y.-K. Direct fidelity estimation from few Pauli measurements. *Phys. Rev. Lett.* **106**, 230501 (2011).

[65] Mayers, D. and Yao, A. Self testing quantum apparatus. arXiv preprint arXiv:quant-ph/0307205 (2003).

[66] McKague, M. Self-testing graph states. In *Conference on Quantum Computation, Communication, and Cryptography* (pp. 104-120). Springer, Berlin, Heidelberg (2011).

[67] Bancal, J.-D., Navascués, M., Scarani, V., Vértesi, T. and Yang, T. H. Physical characterization of quantum devices from nonlocal correlations. *Phys. Rev. A.* **91**, 022115 (2015).

[68] Miller, C. A. and Shi, Y. Optimal robust quantum self testing by binary nonlocal XOR games. arXiv preprints arXiv:1207.1819 (2012).

[69] Reichardt, B. W., Unger, F. and Vazirani, U. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. arXiv preprint arXiv:1209.0448 (2012).

[70] McKague, M., Yang, T. H. and Scarani, V. Robust self-testing of the singlet. *Journal of Phys. A: Math. Theor.* **45**, 455304 (2012).

[71] Aolita, L., Gogolin, C., Kliesch, M. and Eisert, J. Reliable quantum certification of photonic state preparations. *Nat. Commun.* **6**, 8498 (2015).

[72] Hangleiter, D., Kliesch, M., Schwarz, M. and Eisert, J. Direct certification of a class of quantum simulations. *Quantum Sci. Technol.* **2**, 015004 (2017).

[73] Marin, A. and Markham, D. Practical sharing of quantum secrets over untrusted channels. arXiv preprints arXiv:1410.0556 (2014).

[74] Pappa, A., Chailloux, A., Wehner, S., Diamanti, E. and Kerenidis, I. Multipartite entanglement verification resistant against dishonest parties. *Phys. Rev. Lett.* **108**, 260502 (2012).

[75] McCutcheon, W. et al. Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* **7**, 13251 (2016).

[76] Dimić, A. and Dakić, B., Single-copy entanglement detection. *NPJ Quantum Information* **4(1)**, 11 (2018).

[77] Gühne, O., Tóth, G. and Briegel, H. Multipartite entanglement in spin chains. *New Journal of Physics* **7**, 229 (2005).

[78] Briegel, H. J. and Raussendorf R. Persistent Entanglement in Arrays of Interacting Particles. *Phys. Rev. Lett.* **86**, 910 (2001).

[79] Pérez-García, D., Verstraete, F., Wolf, M. M. and Cirac, J. I. Matrix product state representations. *Quantum Inf. Comput.* **7**, 401 (2007).

[80] Verstraete, F., Murg, V. and Cirac, J. I. Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems. *Adv. Phys. 57* **143** (2008).

[81] Pérez-García, D., Verstraete, F., Cirac, J. I. and Wolf, M. M. PEPS as unique ground states of local Hamiltonians. *Quant. Inf. Comp.* **8**, 0650-0663 (2008).

[82] Chernoff, H. A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations. *Ann. Math. Stat.* **23**, 493 (1952).

[83] Hein, M., Eisert, J. and Briegel, H. J. Multiparty entanglement in graph states. *Phys. Rev. A.* **69**, 062311 (2004).

[84] Eldar, L. and Harrow, A. W. Local Hamiltonians Whose Ground States are Hard to Approximate, arXiv:1510.02082 (2015).

[85] Van den Nest, M., Luttmer, K., Dür, W. and Briegel, H. J. Graph states as ground states of many body spin-1/2 Hamiltonians. *Phys. Rev. A.* **77**, 012301 (2008).

[86] Renes, J. M., Blume-Kohout, R., Scott, A. J. and Caves, C. M. Symmetric informationally complete quantum measurements. *J. Math. Phys.* **45**, 2171 (2004).

[87] Ahnert, S. E. and Payne, M. C. General implementation of all possible positive-operator-value measurements of single-photon polarization states. *Phys. Rev. A.* **71**, 012330 (2005).

[88] Tóth, G. and Gühne, O. Entanglement detection in the stabilizer formalism. *Phys. Rev. A.* **72**, 022340 (2005).

[89] Saggio, V., Dimić, A., Greganti, C., Rozema, L. A., Walther, P. and Dakić, B. Experimental few-copy multipartite entanglement detection. *Nature Physics* **15**, 935-940 (2019).

[90] Blume-Kohout, R. Robust error bars for quantum tomography. arXiv preprints arXiv:1202.5270 (2012).

[91] Lu, C. Y., Zhou, X. Q., Gühne, O., Gao, W. B., Zhang, J., Yuan, Z. S. and Pan, J. W. Experimental entanglement of six photons in graph states. *Nature Physics* **3**(2), 91 (2007).

[92] Tóth, G. and Gühne, O. Detecting genuine multipartite entanglement with two local measurements. *Phys. Rev. Lett.* **94**(6), 060501(2005).

[93] Gerke, S., Vogel, W. and Sperling, J. Numerical construction of multipartite entanglement witnesses. *Phys. Rev. X* **8**, 031047 (2018).

[94] Natarajan, C. M., Tanner, M. G., and Hadfield, R. H., Superconducting nanowire single-photon detectors: physics and applications. *Superconductor science and technology* **25(6)**, 063001 (2012).

[95] Marsili, F. et al. Detecting single infrared photons with 93% system efficiency. *Nat. Photon.* **7(3)**, 210 (2013).

[96] Pál, K. F., Vértesy, T. and Navascués, M. Device-independent tomography of multipartite quantum states. *Phys. Rev. A* **90**, 042340 (2014).

[97] Dimić, A., Šupić, I. and Dakić, B. Resource-efficient device-independent quantum state verification (in preparation) (2019).

[98] Tóth, G., Gühne, O. and Briegel, H. J. Two-setting Bell Inequalities for Graph States *Phys. Rev. A* **73**, 022303 (2006).

[99] Mermin, N. D. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.* **65**, 1838 (1990).

[100] Kaniewski, J. and Wehner, S. Device-independent two-party cryptography secure against sequential attacks. *New Journal of Physics* **18**, 055004 (2016).

[101] Kaniewski, J. Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities. *Phys. Rev. Lett.* **117**, 070402 (2016).

[102] Dimić, A. and Dakić, B. On the central limit theorem for unsharp quantum random variables. *New J. Phys.* **20**, 063051 (2018).

[103] Massar, S. Uncertainty relations for positive-operator-valued measures. *Phys. Rev. A* **76**, 042114 (2007).

[104] Billingsley, P. *Probability and Measure* (New York : Wiley, 1995).

[105] Berry, A. C. The accuracy of the Gaussian approximation to the sum of independent variates. *Trans. Amer. Math. Soc.* **49**, 122-136 (1941).

[106] Esseen, C. G. On the Liapounoff limit of error in the theory of probability. *Ark. Mat. Astr. Fys.* **28**, 1-19 (1942).

[107] De Finetti, B. Theory of Probability. Wiley, New York, (1990).

[108] Diaconis, P. A dozen de Finetti-style results in search of a theory. *Ann. Inst. Henri Poincaré* **25**, 397-423 (1987).

[109] Caves, C. M., Fuchs, C. A. and Schack, R. Unknown Quantum States: The Quantum de Finetti Representation. *J. Math. Phys.* **43**, 4537 (2002).

[110] Christandl, M., König, R., Mitchison, G. and Renner, R. One-and-a-Half Quantum de Finetti Theorems. *Comm. Math. Phys.* **273**(2), 473-498, (2007).

[111] Li, K. and Smith, G. Quantum de Finetti Theorem under Fully-One-Way Adaptive Measurements. *Phys. Rev. Lett.* **114**, 160503 (2015).

[112] Zhang, Z. and Duan, L. Quantum metrology with Dicke squeezed states. *New J. Phys.* **16**, 103037 (2014).

[113] McDiarmid, C. Surveys in Combinatorics **141**, 148 (1989).

[114] Ross, S. M. A first course in probability. Upper Saddle River, N.J: Pearson Prentice Hall (2006).

.

# Biografija

Aleksandra Dimić, rođena je 17.05.1991. godine u Zagrebu, Socijalistička Federativna Republika Jugoslavija. Matematičku gimnaziju (MG) u Beogradu završila je 2010. godine kao nosilac diplome "Vuk Stefanović Karadžić". Tokom svog gimnazijskog obrazovanja učestvovala je na međunarodnim takmičenjima u oblasti fizike i astronomije i ostvarila zapažene rezultate. Osvojila je 4 olimpijske medalje u naučnim disciplinama, a najveći uspeh na takmičenjima je srebrna medalja na Međunarodnoj fizičkoj olimpijadi 2010. godine u Hrvatskoj.

Nakon završetka srednje škole, postaje saradnik za dodatnu nastavu i pripremu za takmičenja iz fizike u svojoj matičnoj školi MG, kao i saradnik Regionalnog centra za talente "Beograd 2". Fizički fakultet u Beogradu, upisala je 2010. godine, a završila u predviđenom roku, 2014. godine sa prosekom 10, kao student generacije na smeru Teorijska i eksperimentalna fizika. Tokom osnovnih studija bila je praktikant u Centru za fotoniku, Instituta za fiziku u Zemunu u oblasti biofizike i nelinearne mikroskopije. Master studije završila je 2015. godine na Fizičkom fakultetu u Beogradu, pod mentorstvom prof. dr Đorđa Spasojevića i prof. dr Milorada Kuraice u oblasti kvantne optike i primenama u fizici magnetnih materijala. Tema master teze bile su "Magnetne i optičke osobine ferofluida kobalt-ferita". Tokom master studija radi kao saradnik u nastavi na Fizičkom fakultetu u Beogradu na predmetima Metode matematičke fizike i Teorijska fizika plazme. Tokom svog školovanja bila je stipendistkinja Fonda za mlade talente - "Dositeja" - Ministarstva omladine i sporta. Nakon master studija primljena je na praksu na Institut za Fotoniku u Barseloni, Španija, gde je radila u grupi za Eksperimentalnu kvantnu informaciju prof. dr Morgan Mitchell-a. Uže oblasti njenog istraživanja bile su magnetometrija i ograničenja u kvantnim eksperimentima.

Upisala je doktorske studije na katerdni za Kvantnu, matematičku i nano-fiziku, Fizičkog fakulteta u Beogradu pod rukovodstvom prof. dr Milana Damnjanovića u saradnji sa istraživačima Austrijske akademije nauka, dr Borivojem Dakićem koji je mentor doktorskih studija i prof. dr Časlavom Buknerom. Tokom doktorskih studija zaposlena je kao istraživač pripravnik, a zatim i saradnik na projektu ON171035 Ministarstva prosvete i nauke i angažovana je u nastavi na Fizičkom fakultetu (kursevi: Kvantna mehanika, Metode/Osnove matematičke fizike, Teorijska fizika plazme i Elektromagnetizam). Sa svojim mentorom drži i priprema mini kurs Kvantne informacije u okviru predmeta Kvantna mehanika 2. Angažovana je i kao saradnik u nastavi u Matematičkoj gimnaziji u Beogradu. Tokom leta 2017. godine dobila je stipendiju Austrijske agencije za mobilnost studenata, za studijski boravak u Beču na Fizičkom fakultetu i Institutu za kvantnu optiku i kvantnu

informaciju. član je i COST asocijacije za usavršavanje i umrežavanje studenata, preko koje je učestvovala na dve letnje škole.

Uža naučna oblast Aleksandre Dimić je kvantna informacija, a uključena je u istraživanja u oblasti teorijskog zasnivanja kvantne mehanike i informacionog pogleda na kvantnu gravitaciju, što su trenutno svetske najaktuelnije fizičke oblasti.

# Изјава о ауторству

Име и презиме аутора **Александра Димић**

Број индекса **8017/2015**

**Изјављујем**

да је докторска дисертација под насловом

**Detection of quantum correlations**

**(Детекција квантних корелација)**

- резултат сопственог истраживачког рада;
- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

**Потпис аутора**

Александра Димић

У Београду, **18.11.2019.** године

# Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора **Александра Димић**

Број индекса **8017/2015**

Студијски програм **Физика – Квантна и математичка физика**

Наслов рада **Detection of quantum correlations (Детекција квантних корелација)**

Ментори **проф. др Боривоје Дакић**

**проф. др Милан Дамњановић**

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањена у **Дигиталном репозиторијуму Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

**Потпис аутора**

Александра Димић

У Београду, **18.11.2019.** године

# Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

**Detection of quantum correlations**

**Детекција квантних корелација**

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)

2. Ауторство – некомерцијално (CC BY-NC)

3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)

4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)

5. Ауторство – без прерада (CC BY-ND)

6. Ауторство – делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци.
Кратак опис лиценци је саставни део ове изјаве).

**Потпис аутора**

Александра Дилић

У Београду, **18.11.2019.** године

1. **Ауторство**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. **Ауторство – некомерцијално**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. **Ауторство – некомерцијално – без прерада**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. **Ауторство – некомерцијално – делити под истим условима**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. **Ауторство – без прерада**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. **Ауторство – делити под истим условима**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.