A STUDY ON VARIOUS DISCRIMINATION TASKS AND THEIR IMPLICATIONS IN QUANTUM INFORMATION PROCESSING

Thesis submitted for the partial fulfillment of the requirements for the degree Doctor of Philosophy in Science

by

Samrat Sen

Department of Physics
Faculty of Natural and Mathematical Sciences
Presidency University
Kolkata, India

2025

A STUDY ON VARIOUS DISCRIMINATION TASKS AND THEIR IMPLICATIONS IN QUANTUM INFORMATION PROCESSING

Thesis submitted for the partial fulfillment of the requirements for the degree Doctor of Philosophy in Science

by

Samrat Sen

Under the Supervision of

Dr. Manik Banik
Department of Physics of Complex Systems
S. N. Bose National Centre for Basic Sciences
Kolkata, India

Department of Physics
Faculty of Natural and Mathematical Sciences
Presidency University
Kolkata, India

2025

Thesis details

Thesis Title: A STUDY ON VARIOUS DISCRIMINATION TASKS AND THEIR IMPLICATIONS IN QUANTUM INFORMATION PROCESSING

Name of the Candidate: Samrat Sen

Registration Number: RC001-22RS209110346

Date of Registration: 12th August, 2022

Department: Department of Physics

Samrat Sen
03/03/2025
Signature of the Candidate with date

To my world—my parents, Sankar Sen and Sujata Sen—whose unwavering love, sacrifices, and guidance have made this journey possible.

Acknowledgement

I would like to express my deepest gratitude to everyone who has supported and inspired me throughout my PhD journey.

First and foremost, I am profoundly grateful to my supervisor, Dr. Manik Banik, for allowing me to work under his guidance. His unwavering support, constant encouragement, and confidence in my abilities have been instrumental in shaping this thesis. Our insightful discussions not only strengthened my scientific reasoning but also broadened my perspective on the subject. I am especially thankful for the freedom he granted me to explore my research interests independently, which has been invaluable to my learning experience.

I also extend my heartfelt gratitude to Prof. Guruprasad Kar, Prof. Somshubhro Bandyopadhyay, Prof. Sibasish Ghosh and Prof. Archan S. Majumdar for their invaluable guidance and enriching discussions—both scientific and beyond—which have deeply influenced my PhD journey.

A special thanks to my group members, past and present, who became my second family: Ramkrishna (Ramu), Snehasish (Bhhhai), Sahil, Edwin, Govind, Ananya, Kunika, Jayashree, Dr. Amit Mukherjee (Amit Da), Dr. Mir Alimuddin (Mir Da), Dr. Pratik Ghosal (Pratik Da), and Dr. Ananda Maity (Ananda Da). I am especially grateful to Ramu, who showed me that true friends do indeed exist. He introduced me to table tennis, a sport I immediately fell in love with, and patiently taught me everything he knew about the game. His unwavering support during my toughest moments is something I will cherish forever.

To Arun Da, Subhankar, Bivas, Saheli, Pritam, and Sudip—thank you for the engaging discussions and for making this journey brighter.

I also fondly remember my time at IISER Thiruvananthapuram and the lifelong friendships I formed there. A heartfelt toast to our "Greater IISER group"—Wasim, Soumya, Dweep, Ritobroto, Manika, and Debu—for making those years unforgettable.

A special mention to Nikhil, the best roommate and friend anyone could ask for, and to Anindita, "The Ancient One," whose wisdom and warmth made this journey even more special.

To my PSB 3203 family—Nitu, Kallol Da, Abhinava, Arun Bhaiya, and Tahir Da—thank you for your companionship and support. Your friendship brought a sense of belonging that enriched my Ph.D. experience in countless ways.

I am also deeply grateful to my closest collaborators— Dr. Arup Roy (Arup Da), Dr. Ashutosh Rai (Ashu Da), Dr. Tamal Guha (Tamal Da), Dr. Some Sankar Bhattacharya (Some Da), Dr. Sutapa Saha (Sutapa Di), Subhendu, Dr. Anandamay Das Bhowmik (Ananda Da), and Tathagata—for their support and intellectual exchange, which have been instrumental in shaping my research in quantum information and foundations.

I cannot express enough gratitude to Gobindo Kaku and Chanchu Kaku—wherever you are, your presence and influence remain deeply cherished.

To my family—Bobi, Nanu, Mashibhai, Duttababu, Fulmashi, Chhotomama, Moni Mashi, Tatai—and to my dearest cousins, Ronnie Dada, Joi Dada, Piyali Didi, Didia, Tui, Gogoldada, Mimididi, Dadabhai, and Didibhai—my deepest love and gratitude. Your unwavering support and affection mean the world to me.

To my Amma and Didan, I hope I have made you proud. Please keep watching over us.

Above all, words fall short of expressing my deepest gratitude to my parents for their unconditional love, encouragement, and unwavering belief in me. You mean everything to me. Your support has been my pillar of strength throughout this journey. Only we know how far we have come, and I will be forever grateful for your sacrifices and presence in my life.

Finally, I sincerely thank the S. N. Bose National Centre for Basic Sciences (SNBNCBS), Kolkata, for its financial support and access to essential research facilities, which were instrumental in carrying out this work. I also extend my gratitude to Presidency University for offering the CRPI program to SNBNCBS students and providing valuable academic resources and opportunities.

Samrat Sen
03/03/2025
Signature of the Candidate with date

Declaration

I hereby declare that this thesis contains original research work carried out by me under the guidance of Dr. Manik Banik, Associate Professor, Department of Physics of Complex Systems, S.N. Bose National Centre for Basic Sciences (SNBNCBS), Kolkata, India as part of the PhD programme.

All information in this document have been obtained and presented in accordance with academic rules and ethical conduct.

I also declare that, as required by these rules and conduct, I have fully cited and referenced all materials and results that are not original to this work.

I also declare that, this work has not been submitted for any degree either in part or in full to any other institute or University before.

Samrat Sen
03/03/2025
Signature of the Candidate with date

S. N. Bose National Centre for Basic Sciences
(Under Department of Science and Technology, Govt. of India)
JD Block, Sector-III, Salt Lake City, Kolkata - 700 106, India
Tel.+91-33-2335 5706/07/08 (extn: 210)
E-mail:manik.banik@bose.res.in

CERTIFICATE

This is to certify that the thesis entitled "A STUDY ON VARIOUS DISCRIMINATION TASKS AND THEIR IMPLICATIONS IN QUANTUM INFORMATION PROCESSING" submitted by **Shri Samrat Sen**, Registration Number RC001-22RS209110346 and date of registration 12th August, 2022, in partial fulfilment of the requirements for the award of "Doctor of Philosophy", is a record of bona-fide research work carried out by him under my supervision.

Neither his thesis nor any part of the thesis has been submitted for any degree/diploma or any other academic award anywhere before.

Manik Banik

Dr. Manik Banik
Associate Professor
Department of Physics of Complex Systems
S. N. Bose National Centre for Basic Sciences

Dr. MANIK BANIK
Associate Professor
Department of Physics of Complex Systems
S. N. Bose National Centre for Basic Sciences
Block JD, Sector III, Salt Lake, Kol-106

Abstract

Quantum information theory builds upon its classical counterpart by incorporating uniquely quantum phenomena such as superposition, entanglement, and measurement incompatibility. This unlocks powerful advantages in several information processing tasks, including quantum parallelism in computation and unprecedented security in cryptography, as exemplified by quantum key distribution. Any information processing task—be it computation, communication, or cryptography—relies on the process of discrimination at its core. This is because regardless of the complexity of the task, it will fundamentally involve a sender encoding information into distinguishable states of an object and a receiver attempting to decode the information. It is important to note that the importance of the discrimination process is not restricted to mere information extraction. It also helps reveal the underlying features and limitations of a theoretical framework. This thesis uses discrimination tasks in various scenarios, exploring their implications for quantum information processing.

First, we propose the task of local state marking (LSM), a novel variant of the local state discrimination (LSD) task. While mutually orthogonal states can always be marked exactly under global operations, this is in general not the case under the LOCC framework in which the parties can only perform local quantum operations (LO) on their respective subsystems and can communicate with each other classically (CC). We show that the LSM task is distinct from the vastly explored LSD task— perfect LSD always implies perfect LSM, whereas we establish that the converse does not hold in general. More precisely, we establish that local unmarkability is a stronger form of nonlocality than local indistinguishability. We also explore entanglement-assisted marking of states that are otherwise locally unmarkable and report intriguing entanglement-assisted catalytic LSM phenomenon.

Thereafter, we use a discrimination task to comment on the theoretical frameworks guiding the composition of local quantum systems. We contrast the communication utilities of the maximal tensor product theory and quantum theory. This demonstrates that these frameworks yield distinct utilities in a simple communication game involving two players in a pairwise distinguishability task. Since bipartite correlations from this broader maximal tensor product state space in Bell-type experiments are quantum simulable, our findings suggest that a beyond-quantum composite structure can produce non-quantum correlations in a timelike scenario. Our results also indicate that the gap in communication utility between these two theories can be increased further by considering more elementary systems. Hence it welcomes new principles to isolate the quantum correlations from the beyond quantum ones. Additionally, we establish a no-go result showing that the classical information capacity of these alternative compositions cannot exceed that of the corresponding quantum composite systems.

Finally, we turn our attention to Bell nonlocality, a phenomenon of profound theoretical significance and immense practical utility in quantum information science. Bell inequalities are useful in discriminating post-classical or nonlocal correlations from classical ones. The utilization of nonlocal correlations in suitable information-theoretic tasks offers distinct advantages over classical correlations, underscoring their inherent resourcefulness. With this in mind, we investigate nonlocality distillation, a process that uses a natural set of free operations, called wirings, on multiple copies of weakly nonlocal systems to produce correlations with stronger nonlocality. In the simplest Bell scenario, we propose a protocol, the logical OR-AND wiring, which can distill nonlocality to a significantly high degree starting from arbitrarily weak quantum correlations. This distillation procedure will be shown to be effective in discriminating post-quantum correlations from quantum ones as well.

Samrat Sen
03/03/2025

List of publications

Publications and communicated works relevant to the thesis:

- "*Local quantum state marking* ": **Samrat Sen**, Edwin Peter Lobo, Sahil Gopalkrishna Naik, Ram Krishna Patra, Tathagata Gupta, Subhendu B. Ghosh, Sutapa Saha, Mir Alimuddin, Tamal Guha, Some Sankar Bhattacharya, and Manik Banik; Phys. Rev. A **105**, 032407 (2022).

- "*Timelike correlations and quantum tensor product structure*": **Samrat Sen**, Edwin Peter Lobo, Ram Krishna Patra , Sahil Gopalkrishna Naik, Anandamay Das Bhowmik, Mir Alimuddin , and Manik Banik Phys. Rev. A **106**, 062406 (2022).

- "*Distilling Nonlocality in Quantum Correlations*": Sahil Gopalkrishna Naik, Govind Lal Sidhardh, **Samrat Sen**, Arup Roy, Ashutosh Rai, and Manik Banik Phys. Rev. Lett. **130**, 220201 (2023).

Additional publications during the Ph.D. thesis but not forming part of it:

- "*Unlocking the advantage of qubit communication in multi-node network configurations*": Ananya Chakraborty, Sahil Gopalkrishna Naik, Edwin Peter Lobo, Ram Krishna Patra, **Samrat Sen**, Mir Alimuddin, Amit Mukherjee* and Manik Banik; New J. Phys. **27** 023027 (2025)

- "*Classical analogue of quantum superdense coding and communication advantage of a single quantum system*": Ram Krishna Patra, Sahil Gopalkrishna Naik, Edwin Peter Lobo, **Samrat Sen**, Tamal Guha, Some Sankar Bhattacharya, Mir Alimuddin, and Manik Banik; Quantum **8**, 1315 (2024).

- "*Principle of Information Causality Rationalizes Quantum Composition*": Ram Krishna Patra, Sahil Gopalkrishna Naik, Edwin Peter Lobo , **Samrat Sen**, Govind Lal Sidhardh, Mir Alimuddin, and Manik Banik ; Phys. Rev. Lett. **130**, 110202(2023).

- "*Advantage of Hardy's nonlocal correlation in reverse zero-error channel coding*": Mir Alimuddin, Ananya Chakraborty, Govind Lal Sidhardh, Ram Krishna Patra , **Samrat Sen**, Snehasish Roy Chowdhury, Sahil Gopalkrishna Naik, and Manik Banik ; Phys. Rev. A **108**, 052430 (2023).

- "*Certifying beyond quantumness of locally quantum no-signaling theories through a quantum-input Bell test*": Edwin Peter Lobo, Sahil Gopalkrishna Naik, **Samrat Sen**, Ram Krishna Patra , Manik Banik, and Mir Alimuddin; Phys. Rev. A **106**, L040201(Letter) (2022).

- "*Composition of Multipartite Quantum Systems: Perspective from Timelike Paradigm*": Sahil Gopalkrishna Naik, Edwin Peter Lobo, **Samrat Sen**, Ram Krishna Patra, Mir Alimuddin, Tamal Guha, Some Sankar Bhattacharya, and Manik Banik; Phys. Rev. Lett. **128**, 140401 (2022).

- "*Mutually unbiased balanced functions and generalized random access codes*": Vaisakh M, Ram krishna Patra, Mukta Janpandit, **Samrat Sen**, Manik Banik and Anubhav Chaturvedi; Phys. Rev. A **104**, 012420 (2021).

Additional communicated article during the Ph.D. thesis but not forming part of it:

- "*Asymptotic Birkhoff-Violation in Operational Theories: Thermodynamic Implications and Information Processing*": Ananya Chakraborty, Sahil Gopalkrishna Naik, **Samrat Sen**, Ram Krishna Patra, Pratik Ghosal, Mir Alimuddin, Manik Banik;

  arXiv:2406.08803v1 [quant-ph].

- "*Local-Data-Hiding and Causal Inseparability: Probing Indefinite Causal Structures with Cryptographic Primitives*": Sahil Gopalkrishna Naik, **Samrat Sen**, Ram Krishna Patra, Ananya Chakraborty, Mir Alimuddin, Manik Banik, Pratik Ghosal;

  arXiv:2407.20543v1 [quant-ph].

- “*Scalable & Noise-Robust Communication Advantage of Multipartite Quantum Entanglement*": Ananya Chakraborty, Ram Krishna Patra, Kunika Agarwal, **Samrat Sen**, Pratik Ghosal, Sahil Gopalkrishna Naik, Manik Banik;

  arXiv:2409.13223v2 [quant-ph].

- “*Nonlocality Assisted Enhancement of Error-Free Communication in Noisy Classical Channels*": Kunika Agarwal, Sahil Gopalkrishna Naik, Ananya Chakraborty, **Samrat Sen**, Pratik Ghosal, Biswajit Paul, Manik Banik, and Ram Krishna Patra;

  arXiv:2412.04779 [quant-ph]

Table of contents

List of figures

Chapter 1

General Introduction

1.1 Motivation

We are currently living in the age of information, which began with the groundbreaking work of Claude Shannon in 1948 [1], often referred to as the "father of information theory." His pioneering research established a mathematical framework for quantifying information, introducing key concepts such as entropy, data compression, and channel capacity. Shannon's theorem outlines the limits of reliable communication over noisy channels, forming the foundation for digital communication, data storage, and error correction.

At the core of reliable communication—and, more broadly, any information-processing protocol—lies the essential discrimination task. Extracting information relies on the ability to effectively distinguish the objects encoding that information. Since communication deals with the sending of classified information among several parties, security concern is an important issue here. In the presence of adversaries attempting to intercept communication between parties, security is compromised. To facilitate secure communication between parties, the RSA encryption was developed [2]. The security of the RSA encryption scheme assumes that adversaries have limited computational power. This limitation is a cornerstone of the scheme's cryptographic strength. Specifically, the RSA encryption relies on the difficulty of factoring large composite numbers into their prime factors, which becomes computationally infeasible as the key size increases. However, in 1994, Peter Shor gave an algorithm based on the adversary using a quantum algorithm [3]. He showed that his algorithm can efficiently factorize large integers, thus breaking the foundation on which RSA encryption relied. His algorithm, along with the protocol put forward by Charles

H. Bennett and Gilles Brassard in 1984 [4], commonly known as the seminal BB84 protocol, marked a significant breakthrough in quantum computing because of its profound implications for cryptography, particularly for widely used schemes like RSA. This was the first proposed quantum cryptographic protocol, essentially based on the ideas by Stephen Wiesner, developed in the late 1960s [5]. The security of the BB84 protocol leverages a uniquely quantum mechanical property: non-orthogonal pure quantum states cannot be reliably distinguished [6]. Consequently, a fundamental limitation in discrimination within quantum theory, when strategically utilized, proves to be more advantageous than classical methods. This underscores the significance of discrimination tasks, which extend beyond mere information extraction. When appropriately designed, such tasks can effectively harness the distinctive features of an underlying theory within an information-theoretic framework.

Quantum theory stands as the most precise framework to date for describing the physical universe. Apart from gravity, it offers an exact mathematical representation of natural phenomena, encompassing everything from molecular structures to the behavior of elementary particles. Fundamentally, however, quantum theory diverges significantly from classical physics. One of the main features distinguishing it from classical theory is the existence of entangled states, which has led to several information-processing tasks that are impossible in the classical regime, such as Super-Dense Coding [7] and Quantum Teleportation [8]. Among several foundational protocols, these particularly highlight the advantages that quantum theory offers over classical approaches, made possible by the existence of entanglement. Moreover, quantum theory allows for correlations between spatially separated systems, which have no counterpart in classical physics. Such correlations necessitate the existence of entangled states. While these quantum correlations adhere to the no-signaling principle—ensuring that information cannot be transmitted faster than the speed of light in vacuum—it also exhibit properties that cannot be explained by any local deterministic hidden variable model. Such correlations, known as "nonlocal correlations," are at the heart of the phenomenon referred to as "quantum nonlocality" [9, 10]. However, contrary to Bell nonlocality, where separable and thus product states cannot exhibit nonlocality, a discrimination task revealed that a different form of quantum nonlocality can indeed exist without entanglement. This was first demonstrated by Asher Peres and William K. Wootters in 1991 in the context of local state discrimination of product states [11]. Later, in 1999, Charles H. Bennett and his collaborators expanded on this work [12], demonstrating a stronger result using orthogonal product states, whereas Peres and Wooters had used non-orthogonal ones. Hence, the works referenced in [11] and [12] play a pioneering role in proving that the nonlocal behaviors witnessed in quantum theory do not always require entanglement and thus motivate further information-processing tasks using such nonlocality. Since then, the investigation of various discrimination tasks within the LOCC framework has become an active area of research, with applications in cryptographic primitives such as data hiding [13, 14] and secret sharing [15–19], secured key distribution [20, 21] quantum cryptography [22], and other aspects of quantum information theory.

The specific form of nonlocality discussed here is investigated within the distant laboratory paradigm, which is captured by the framework of Local Operations (LO) and Classical Communication (CC), commonly abbreviated as LOCC (See [23] for an in-depth understanding). This nonlocality is termed as local indistinguishability. In this context, spatially separated parties operate in distant laboratories, wherein a referee selects a state from a known set of multipartite states and distributes individual subsystems to each party. Under this setup, each party is restricted to performing local measurements and can only communicate via classical channels. The LOCC paradigm effectively models such distant laboratory scenarios, where questions of entanglement manipulation of the shared state and the transformation of one state to another are other important considerations. Specifically, the results in [12] demonstrate that certain bipartite orthogonal product quantum states, though locally preparable by two parties, require a joint measurement for perfect discrimination—something unachievable by spatially separated parties within the LOCC framework. This phenomenon is inconceivable in the classical regime, where states distinguishable globally can also be distinguished locally through classical communication. The difference in discrimination probabilities between global and local scenarios highlights the nature of the nonlocality in question.

In the local state distinguishability task, a referee selects a state from a given set and distributes its corresponding subsystems to the parties, who then collaborate under the LOCC paradigm to identify the distributed state. A natural question arises: what if, instead of distributing a single state, the referee distributes all the states from the set simultaneously, but in a specific permutation, requiring the parties to use LOCC to determine this permutation? This scenario introduces a novel variant of the local state discrimination problem. The key question, then, is whether these two tasks are fundamentally equivalent or intrinsically different.

Moving forward, it is important to recognize that discrimination tasks can reveal the limitations of a theory by demonstrating its inability to perform certain operational tasks. For instance, a color-blind individual cannot distinguish between two distinctly colored objects, such as a red ball and a green ball, whereas a person with normal color vision can. Similarly, discrimination tasks serve as a crucial tool for uncovering the fundamental characteristics and constraints of a theory, as illustrated by the analogy of color blindness.

Given the valuable insights that discrimination tasks provide into the structure of a theory, it is worth investigating whether alternative mathematically consistent frameworks governing local quantum systems might yield novel and intriguing results. Quantum mechanics has already shown significant advantages in information-theoretic protocols and thus from a theoretical standpoint, this raises a compelling question: could these alternative theories surpass quantum mechanics in information-processing tasks which is ultimately related to discrimination?

The quantum composition rule is one of the several postulates of quantum theory which is ad-hoc in nature, lacking direct physical justification. In contrast, Generalized Probabilistic Theories (GPTs) have garnered significant attention within the physics community, particularly due to their potential to reconstruct quantum mechanics from first principles [24–36]. The framework of GPT [27–31, 37] serves as a valuable tool for analyzing various composite models. Physical principles, such as no-signaling and local tomography, constrain composite state spaces between two boundaries [38–41]: the minimal tensor product (denoted as separable or SEP theory), which includes only separable states, and the maximal tensor product (denoted as $\overline{\text{SEP}}$ theory), which encompasses states that extend beyond quantum states, being positive on product tests (POPT) and consistent with the unentangled Gleason's theorem [42–44]. Under the 'no-restriction' hypothesis [45], the effect spaces are defined to incorporate all effects that are mathematically consistent within the theoretical framework.

If such alternative theories do indeed outperform quantum mechanics in specific information-processing tasks, this could provide insights into why we exclusively adhere to the quantum mechanical tensor product rule. Such findings may pave the way for new principles that isolate quantum correlations from those that extend beyond quantum mechanics, ultimately challenging the physical validity of these beyond quantum correlations. The minimal composition (or SEP theory) is a local theory, and hence there is no way of demarcating it from quantum theory, at least in the space-like separated scenario, which is the Bell scenario. However, when considering the maximal composition also known as the $\overline{\text{SEP}}$ theory, there appears to be a substantial possibility for the generation of stronger-than-quantum correlations. For bipartite systems, however, Acín *et al.* [46] and Barnum *et al.* [47] provide a conclusive response, showing that no such composition produces correlations exceeding quantum limits in Bell-type experiments. Consequently, there is no clear distinction between quantum theory and the $\overline{\text{SEP}}$ theory, suggesting no compelling reason to favor quantum theory over $\overline{\text{SEP}}$ theory. This invites further exploration of the issue.

The previous discussion focused on the composition of quantum subsystems. However, when we relax the requirement that subsystems must be quantum, we encounter various theoretical models that allow for correlations more Bell-nonlocal than those permitted by quantum theory—commonly referred to as "post-quantum correlations". For instance, within the framework of the box world theory, the maximal tensor product composition of two square bits, under suitable measurements, yields a Bell correlation that attains the algebraic maximum 4 in the CHSH inequality [48], commonly referred to as the PR box correlation [49]. While both PR box correlation and quantum correlations respect the no-signaling principle, quantum theory imposes additional constraints on the degree of nonlocality, thereby limiting the extent of nonlocal correlations it can generate (See [50]). This distinction influences the information-processing capabilities of the two theories for various information-theoretic tasks. In general, Bell inequalities play a crucial role in distinguishing classical correlations from post-classical ones. Post-classical, or nonlocal, correlations offer advantages for information-theoretic applications, including device-independent protocols for secure key distribution, randomness certification, and related tasks [51–61].

The study of Bell nonlocality has played a crucial role in deepening our understanding of the nature and limitations of quantum correlations [62–66]. In the simplest Bell scenario—where two parties each have two possible inputs and two possible outputs—two fundamental measures have emerged: the degree of CHSH inequality violation [67] and the success probability in Hardy's test of nonlocality [68, 69]. These measures, along with principles inspired by observations of nature, are not only essential for characterizing nonlocality but also serve as possible indicators for distinguishing physical correlations from unphysical ones. For instance, isotropic no-signaling correlations that yield a CHSH value exceeding $4\sqrt{\frac{2}{3}}$ are considered unphysical, as they trivialize communication complexity tasks by violating the principle of Nontrivial Communication Complexity [70] (see also [71–73]). However, when the degree of nonlocality of a correlation lies within the quantum-achievable threshold, determining whether it is a quantum or a post-quantum correlation remains a challenging task.

Since Bell nonlocality is a resource, it is essential to identify and amplify weaker nonlocal correlations to generate correlations with greater nonlocal strength. Moreover, the fact that the set of quantum correlations is closed under wirings [74, 75] ensures that the amplified correlations remain quantum when the initial one is a quantum correlation. This observation suggests that such an amplification—or more precisely, a distillation procedure, could be useful for certifying and distinguishing whether a given Bell correlation is post-quantum or not, when the nonlocality of the initial correlation lies within the quantum-achievable threshold.

1.2 Brief Outline of the Thesis:

This thesis explores the role of various discrimination tasks and their implications in quantum information processing. By carefully designing and analyzing these tasks, it aims to address key questions raised in the preceding discussions. A brief overview of the thesis is given as follows:

Chapter 2 thoroughly presents the essential mathematical foundations required to understand the results in the subsequent chapters. It begins with an in-depth exploration of the fundamental postulates of quantum theory and proceeds to a detailed examination of basic quantum systems, specifically focusing on qubit and two-qubit systems. Additionally, this chapter provides a comprehensive overview of key concepts, including the EPR paradox, Bell's theorem, Hardy's nonlocality, and the generalized probabilistic theory (GPT) framework, with sufficient details on how quantum theory functions as a GPT.

In Chapter 3, we explore the problem of quantum state distinguishability in the LOCC paradigm, introducing a variant of the local state discrimination (LSD) task known as local state marking (LSM). This new approach highlights key distinctions from conventional methods and its implications for information-theoretic protocols. To support the study of local quantum state discrimination, we provide a comprehensive discussion on various measurements and their associated restrictions. This chapter is based on results from one of our works [76]. We demonstrate the inequivalence between LSM and LSD, underscoring the unique characteristics of these two tasks. Furthermore, we establish the concept of local unmarkability as a stronger manifestation of quantum nonlocality within the LOCC framework compared to local indistinguishability. Additionally, we show that LSM offers a more resource-efficient alternative to conventional multi-copy LSD for a specific information-processing task.

Next, we focus on the fact that the unentangled Gleason's theorem permits a state space in which density operators form a proper subset of all possible composite states. In Chapter 4, which is based on the results obtained in one of our works [77], we analyze the communication utilities of these different composite models and show that they can lead to distinct utilities in a simple communication game related to the task of pairwise distinguishability involving two players. This shows that composite structures extending beyond quantum mechanics can lead to correlations exceeding quantum limits in timelike scenarios. As a result, it calls for the formulation of new principles to distinguish quantum correlations from those that go beyond quantum mechanics. We also prove a no-go that the classical information carrying capacity of different such compositions cannot be more than the corresponding quantum composite systems.

In Chapter 5, which is based on our work [78], a protocol in the simplest Bell scenario is given, which can distill nonlocality to a significantly high degree starting from arbitrarily weak nonlocal correlations. Examples of correlations will be given, whose post-quantum nature will be detected using our protocol, while established information principles—such as nontrivial communication complexity and information causality—fail to do so. Therefore, our protocol is effective in distinguishing post-quantum correlations from quantum ones as well. It is also shown that the subsets of no-signaling and quantum correlations that allow for nonlocality distillation occupy a non-zero measure within the full eight-dimensional correlation space.

In Chapter 6, we conclude the thesis by giving a brief summary and possible future directions.

Chapter 2

Preliminaries

2.1 Quantum Theory

Newtonian mechanics and Maxwell's equations governing classical electrodynamics were remarkably successful until the late 19th century when experiments at atomic scales were conducted. It became evident that the outcomes of these experiments were inconsistent with the predictions made by classical theories. This discrepancy led to the development of a new framework that, while mathematically complex, provided highly accurate predictions aligning with experimental results. This new mathematical theory is known as quantum mechanics. Werner Heisenberg formulated a theory that successfully accounted for the quantization effects observed in atomic spectra. Although matrix mechanics was mathematically rigorous, Erwin Schrödinger's wave mechanics quickly gained popularity after demonstrating its physical equivalence to matrix mechanics.

The following sections introduce the fundamental mathematical formalism of quantum theory. At the conclusion of this chapter, a brief outline of the present thesis will be provided.

2.1.1 Postulates of Quantum Mechanics

Quantum mechanics, unlike other physical theories, starts with abstract mathematical postulates. Let us have a look at the postulates [79] which are as follows—

- **System and State**

  Associated with every quantum mechanical system S, there is a separable complex Hilbert space $\mathscr{H}_S$. A state describing this system corresponds to a positive operator ρ of trace one , known as 'density operator', acting on $\mathscr{H}_S$.

The most basic quantum mechanical system is represented by a two-dimensional Hilbert space, commonly referred to as a qubit. A qubit can represent either the polarization degree of freedom of a single photon or the spin degree of freedom of a spin-$\frac{1}{2}$ particle. The state space for this system comprises all positive, trace-one, self-adjoint linear operators, denoted as $\mathscr{D}(\mathscr{H}_S)$, acting on the Hilbert space $\mathscr{H}_S$. Therefore, the state space consists of elements ρ that fulfill the following conditions: (i) $\rho \geq 0$, (ii) $\mathrm{Tr}(\rho) = 1$, and (iii) $\rho = \rho^\dagger$. (Note that since we are dealing with a complex field, the condition $\rho \geq 0$ implies that $\rho = \rho^\dagger$.) This collection forms a convex compact subset of the linear operators acting on $\mathscr{H}_S$. Density operators can be classified into two categories: pure states and mixed states.

Pure state: A state $\rho \in \mathscr{D}(\mathscr{H}_S)$ is called a pure state if it cannot be written as a convex combination of other states in $\mathscr{D}(\mathscr{H}_S)$. Thus, in the convex state space of a system $\mathscr{D}(\mathscr{H}_S)$, pure states are the extreme points. $|\psi\rangle\langle\psi| \in \mathscr{D}(\mathscr{H}_S)$, are rank-one projection operators and they correspond to pure states, where $|\psi\rangle$ is a vector of unit norm in $\mathscr{H}_S$. Therefore, pure states are typically represented by a unit vector $|\psi\rangle \in \mathscr{H}_S$. The mathematical criterion for determining whether a given state ρ represents a pure state is: $\rho^2 = \rho$. This condition further implies that $\mathrm{Tr}(\rho^2) = 1$ if and only if ρ is a pure state.

Mixed state: A density operator in $\mathscr{D}(\mathscr{H}_S)$ which can be decomposed as a convex combination of pure states is termed a mixed state. A mixed state ρ can be represented as $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, where p_i refer to the probability linked with state $|\psi_i\rangle$. In comparison to the pure states, $\mathrm{Tr}(\rho^2) < 1$. The non-unique decomposition of mixed states is one crucial non-classical feature found in quantum mechanics. This phenomenon is not observed in classical theories, as the state spaces in classical frameworks are simplex structures. A quantum mixed state can be represented by infinitely many distinct convex decompositions involving pure states. To be more precise, if ρ is a mixed state, then there exists infinitely many possible ensemble of states like $\{|\psi\rangle_m\}$ or $\{|\phi\rangle_n\}$ such that $\rho = \sum_m p_m |\psi_m\rangle\langle\psi_m| = \sum_n q_n |\phi_n\rangle\langle\phi_n|$ where $\{p_m\}$ and $\{q_n\}$ are the probabilities *i.e.*, $p_m \geq 0, q_n \geq 0$ and $\sum_m p_m = \sum_n q_n = 1$. In short, these different ensembles of quantum states ($\{|\psi\rangle_m\}$ and $\{|\phi\rangle_n\}$) yield the same density operator.

■ **Evolution**

The time evolution of a closed quantum system is described by a unitary transformation. If the state of the system evolves from $\rho(t_0)$ at time t_0 to the state $\rho(t_1)$ at time $t_1(> t_0)$, then $\rho(t_1)$ is related to $\rho(t_0)$ by a unitary operator $U(t_0,t_1)$ which depends only on the times t_0 and t_1, i.e.,

$$\rho(t_1) = U(t_0,t_1)\rho(t_0)U(t_0,t_1)^\dagger$$

This discrete-time description of quantum state evolution using unitary operators can be obtained from the continuous time description of the Schrödinger equation.

$$i\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

Here H is the Hamiltonian operator associated with the closed system and $\hbar$ is the *Planck's constant*. From the above equation the evolution of a quantum state from $|\psi_0\rangle$ at time t_0 to the state $|\psi_1\rangle$ at time t_1 is given by

$$|\psi_1\rangle = \exp[-\frac{i}{\hbar}\int_{t_0}^{t_1} Hdt]|\psi_0\rangle$$

For closed quantum systems, the evolution is unitary. However, for systems interacting with other systems (say environment), the evolution is described by the notion of quantum operations or channel. A quantum channel is a convex-linear completely positive trace non-increasing map from the set of density matrices on some input Hilbert space to the set of density matrices on some output Hilbert space [79]. Considering the important special case where input and output Hilbert spaces are same, the action of a trace-preserving quantum channel $\mathscr{N} : \mathscr{D}(\mathscr{H}) \to \mathscr{D}(\mathscr{H})$ can be expressed as $\mathscr{N}(\rho) = \sum_k E_k \rho E_k^\dagger \quad \forall \rho \in \mathscr{D}(\mathscr{H})$ where $\sum_k E_k^\dagger E_k = \mathbb{I}$. The operators $\{E_k\}$ beloning in the operator space of system Hilbert space are called Kraus operators corresponding to the channel $\mathscr{N}$. However, for a given quantum channel, the choice of Kraus operators are not unique [79].

■ **Measurement**

Quantum measurements are described by a collection of operators $\{M_k\}$ acting on the Hilbert space of the system, satisfying the completeness relation $\sum_k M_k^\dagger M_k = \mathbb{I}$. If a measurement M associated with the collection of operators

$\{M_k\}$ is performed on a system prepared in some state ρ, the probability that k^{th} outcome will occur is given by

$$p(k\,|\rho,M) = Tr(M_k^{\dagger} M_k\;\rho)$$

and the post-measurement state conditioned that the k^{th} outcome has occured, is given by

$$\rho_k = \frac{M_k \rho M_k^{\dagger}}{Tr(M_k^{\dagger} M_k \rho)}$$

When a system is closed, or non-interacting. the evolution of the state of the system can be described by unitary dynamics. However this is no longer the case when the system is interacting with the measurement apparatus which gives rise to the measurement collapse problem. Depending on the outcome of the measurement process, the state of the system is sudden and is due to the measurement process.

$$\rho \rightarrow \frac{M_m \rho {M_m}^{\dagger}}{p(m)}$$

In the following quote from the introduction of chapter 3 *The Copenhagen Interpretation of Quantum Theory* pp. 46-57 in **Physics and Philosophy (1958)** by Werner Heisenberg, it talks about Heisenberg's belief that quantum system is no longer closed when a measurement process happen:

"We have to add some comments on the actual procedure in the quantum-theoretical interpretation of atomic events. It has been said that we always start with a division of the world into an object, which we are going to study, and the rest of the world, and that this division is to some extent arbitrary. It should indeed not make any difference in the final result if we, e.g., add some part of the measuring device or the whole device to the object and apply the laws of quantum theory to this more complicated object. It can be shown that such an alteration of the theoretical treatment would not alter the predictions concerning a given experiment. This follows mathematically from the fact that the laws of quantum theory are for the phenomena in which Planck's constant can be considered as a very small quantity approximately identical with the classical laws. But it would be a mistake to believe that this application of the quantum-theoretical laws to the measuring device

could help to avoid the fundamental paradox of quantum theory.

The measuring device deserves this name only if it is in close contact with the rest of the world, if there is an interaction between the device and the observer. Therefore, the uncertainty with respect to the microscopic behaviour of the world will enter into the quantum-theoretical system here just as well as in the first interpretation. If the measuring device would be isolated from the rest of the world, it would be neither a measuring device nor could it be described in the terms of classical physics at all."

Projective measurement:

A special class of quantum measurements $\{M_i\}_{i=1}^n$ is called a projective measurement if $M_i^\dagger = M_i$ and $M_i M_j = \delta_{i,j} M_i,\ \forall\ i, j$ along with satisfying the completeness relation $\sum_i M_i = \mathbb{I}$. Thus, measurement operators for projective measurements are orthogonal projection operators. Every rank-one projector M_i can be assigned to a unit vector $|\psi_i\rangle$ as $M_i = |\psi_i\rangle\langle\psi_i|$ and hence, the maximum value, the index n can take will be the dimension of the quantum system, on which the measurement is performed. From this point foreward, projective measurement operators will be denoted by P_i instead of M_i. Thus, if a set of orthogonal projectors $\{P_i\}$ refer to a projective measurment, then $\sum_i P_i = \mathbb{I}$. It is possible to devise a Hermitian operator $\hat{A}$ by assigning a set of real numbers (λ_i) to each of the projectors of a collection $\{P_i\}_{i=1}^n$, such that $\hat{A} = \sum_{i=1}^n \lambda_i P_i = \sum_{i=1}^n \lambda_i |\psi_i\rangle\langle\psi_i|$ which can be considered as an observable of the quantum system. If we restrict our consideration to projective measurements, the aforementioned postulate can be reformulated as follows: any quantum observable is represented by a self-adjoint operator acting on the Hilbert space of the system. The outcome of the measurement corresponding to the operator $\hat{A}$ when performed on a system prepared in a quantum state $|\psi\rangle$, will be one of the eigenvalues of $\hat{A}$ and the probability of obtaining the i^{th} eigenvalue λ_i as outcome is given by, $p(i) = |\langle\psi|\,\psi_i\rangle|^2$. The post measurement state will be that corresponding eigenvector $|\psi_i\rangle$. Therefore, the expectation value for any Hermitian operator $\hat{A}$ on the quantum state $|\psi\rangle$ can be written as $\langle\hat{A}\rangle_\psi = \sum_i p(i)\lambda_i = \sum_i |\langle\psi|\,\psi_i\rangle|^2 \lambda_i = \langle\psi|A|\psi\rangle$.

Positive-Operator-Valued Measure (POVM):

This represents a more general class of quantum measurements that can be applied to a system. It is defined as a collection of positive operators $\{E_i\}$, such that $\sum_i E_i = \mathbb{I}$. The POVM elements E_i, are commonly referred to as effects. When a POVM $\{E_i\}$ is performed on a system prepared in state ρ, the probability with which the i^{th} outcome clicks is given by $p(i) = \text{Tr}[\rho E_i]$. To incorporate the POVM formalism within the general measurement framework, one can consider a set of measurement operators $\{M_i\}$ as $M_i = \sqrt{E_i}$, such that $E_i = M_i^\dagger M_i$. However, for a given POVM measurement, the selection of measurement operators $\{M_i\}$ is not unique [79]. Notably, any POVM can be understood as a projective measurement in a Hilbert space of higher dimension [80]. One obvious question that can be raised here is that how POVM formalism actually differs from the general measurement prescription. The measurement postulate deals with two elements. First, it states the rule of getting the probabilities corresponding to different possible outcomes. Second, it provides the rule to obtain the post-measurement state of the system. However, there are several applications where it is of little interest to know the post-measurement states while the main object of interest being the probabilities of different outcomes. In such scenarios, the POVM formalism is especially useful.

- **Composition**

The Hilbert space associated with a composite quantum system is the tensor product of the Hilbert spaces associated with its component quantum systems. i.e.,

$$\mathscr{H}_{1,2,\cdots,n} = \mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \ldots \otimes \mathscr{H}_n$$

An n-partite composite quantum state is described by a density operator $\rho_{1,2,\cdots,n}$ belonging in $\mathscr{D}(\mathscr{H}_{1,2,\cdots,n})$, where $\mathscr{H}_{1,2,\cdots,n} = \mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \ldots \otimes \mathscr{H}_n = \bigotimes_{i=1}^n \mathscr{H}_i$. If a composite state $\rho_{1,2,\cdots,n} \in \mathscr{D}(\bigotimes_{i=1}^n \mathscr{H}_i)$ can be expressed as $\rho_{1,2,\cdots,n} = \rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$, where $\rho_i \in \mathscr{D}(\mathscr{H}_i)$, then it is called a product state. Convex combinations of such product states are referred to as separable states. Consider the simplest case where the number of component systems is two, *i.e.*, a composite quantum system AB with only two subsystems A and B. For such a system comprised of two subsystems, any separable state

ρ_{AB}^{sep} takes the following form :

$$\rho_{AB}^{sep} = \sum_j p_j \rho_A^j \otimes \rho_B^j \tag{2.1}$$

where $p_j \geq 0\ \forall j$ and $\sum_j p_j = 1$. The collection of all separable states constitutes a strict subset of the composite quantum state space $\mathscr{D}(\mathscr{H}_A \otimes \mathscr{H}_B)$. Thus, if $sep(\mathscr{H}_A \otimes \mathscr{H}_B)$ refer to the set of separable states, then $sep(\mathscr{H}_A \otimes \mathscr{H}_B) \subset \mathscr{D}(\mathscr{H}_A \otimes \mathscr{H}_B)$. Composite states that are not part of $sep(\mathscr{H}_A \otimes \mathscr{H}_B)$ are referred to as entangled states. Hence, if $\rho_{AB} \in \mathscr{D}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is entangled, then it cannot be represented as a convex combination of product states *i.e.*, given in Eq. (2.1).

2.1.2 Elementary quantum system: The Qubit

A qubit, or quantum bit, is the quantum mechanical analogue of a classical bit, representing the state space of a classical system with two degrees of freedom. Almost all prevalent quantum mechanical phenomena can be observed in qubit systems. Qubits are extensively studied due to their mathematical simplicity. The pure state corresponding to a two-dimensional quantum system, a qubit, is represented by a vector $|\psi\rangle \in \mathbb{C}^2$ which corresponds to the Hilbert space associated with this qubit. Mathematically, we have an equivalence relation that:

$$|\psi\rangle \sim |\psi'\rangle \Leftrightarrow |\psi\rangle = c\,|\psi'\rangle\,;\ \text{for some non-zero}\ \ c \in \mathbb{C}$$

where $|\psi\rangle$ and $|\psi'\rangle$ are non-zero vectors in $\mathbb{C}^2$. Thus it is sufficient to consider normalized state vectors $|\psi\rangle$ such that $|\langle\ \psi|\psi\ \rangle|^2 = 1$.

Bloch sphere representation: The state space of a single qubit is the collection of all density operators on the Hilbert space $\mathbb{C}^2$. Hence it is a convex subset of the space of all linear operators $\mathbb{L}(\mathbb{C}^2)$ which is a four dimensional vector space. One particular basis set for $\mathbb{L}(\mathbb{C}^2)$ is comprised of the identity matrix and the three Pauli operators, expressed as follows:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Any qubit state ρ can be expressed as a linear combination of the above basis set as the following : $\rho = (c_0\mathbb{I} + c_1\sigma_x + c_2\sigma_y + c_3\sigma_z)$, where $c_i \in \mathbb{C}\ \forall\ i$. By imposing the conditions required for a valid density operator, we find that an arbitrary qubit state can be expressed as follows:

$$\rho = \frac{1}{2}(\mathbb{I} + n_x\sigma_x + n_y\sigma_y + n_z\sigma_z) = \frac{1}{2}(\mathbb{I} + \vec{n}.\vec{\sigma}), \tag{2.2}$$

where $\vec{n} \equiv (n_x, n_y, n_z)$ refers to a real vector in $\mathbb{R}^3$ with $|\vec{n}| \leq 1$. This vector has a special name. It is called Bloch vector for the state ρ. Here $\vec{n}.\vec{\sigma} \equiv n_x\sigma_x + n_y\sigma_y + n_z\sigma_z$ and $\vec{\sigma} \equiv (\sigma_x, \sigma_y, \sigma_z)$. This representation of an arbitrary qubit state possesses an elegant geometrical interpretation. Each ρ corresponds uniquely to its Bloch vector (n_x, n_y, n_z) which satisfies $|\vec{n}| \leq 1$ where equality is attained solely for pure states. Hence, the qubit state space $\mathscr{D}(\mathbb{C}^2)$ is isomorphic to that of a sphere in a three-dimensional real space, and all the pure states are represented by points on the surface of the Bloch sphere (see Fig. 2.1). The magnitude of the Bloch vector $|\vec{n}|$ denotes the distance from the centre to the position of ρ. $|\vec{n}| < 1$ for mixed states. Hence, mixed states are situated strictly within the Bloch sphere at a distance $|\vec{n}|$ from the centre of the sphere. The maximally mixed state $\frac{\mathbb{I}}{2}$ is located at the centre. Geometrically, the Bloch sphere upholds the convexity of the quantum state space, where any chord within the sphere that passes through a specific quantum state ρ represents one of its possible convex

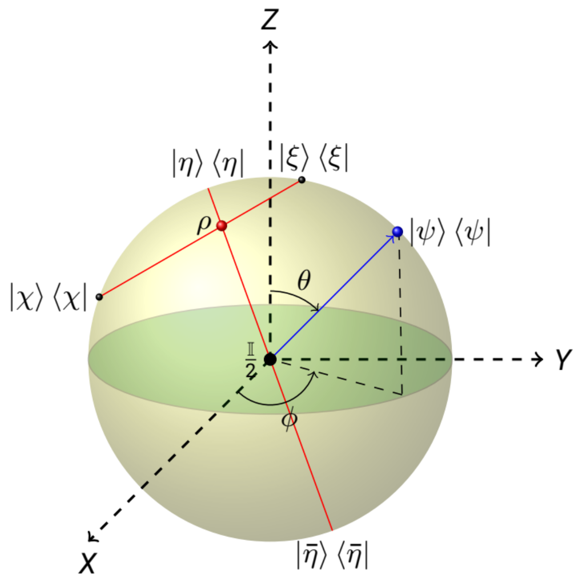

FIG. 2.1 The locations of both pure and mixed states on the Bloch sphere are depicted, with points corresponding to pure states positioned on the surface of the sphere. The non-unique decomposition of a mixed state ρ is illustrated, where $\rho = p|\alpha\rangle\langle\alpha| + (1-p)|\beta\rangle\langle\beta| = q|\psi\rangle\langle\psi| + (1-q)|\bar{\psi}\rangle\langle\bar{\psi}|$. The angles θ and ϕ correspond to the conventional polar and azimuthal angles, respectively.

decompositions. Since ρ can lie on infinitely many such chords, this visualization effectively illustrates the non-unique decomposition of mixed states.

As previously noted, pure states of a qubit are typically regarded as normalized vectors in the Hilbert space $\mathbb{C}^2$. An arbitrary pure state of qubit can be represented as a linear combination of an orthonormal basis. Conventionally the orthogonal eigenvectors of Pauli σ_z operator, denoted by $|0\rangle$ and $|1\rangle$, are used as the computational basis. A pure state $|\psi\rangle$, situated at the (θ,ϕ) point (where $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$) on the surface of the Bloch sphere, can be represented as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \tag{2.3}$$

2.1.3 Elementary Composite System: The Two-Qubit System

The two-qubit composite system is the simplest of all bipartite quantum states wherein Bell nonlocality is observed at the correlation level. At the state distinguishability level, a gap is observed in the distinguishability using entangled measurements which is a global measurement, and between measurements that are allowed when the two parties are spatially separated and can communicate classically.

Let us denote by AB, the two qubit system whose Hilbert space is the $\mathbb{C}^2 \otimes \mathbb{C}^2$. For simplicity, let the particle A be held by a party Alice and B be held by Bob. We denote by $\{|0\rangle_A, |1\rangle_A\}$ an orthonormal basis for Hilbert space of system A and $\{|0\rangle_B, |1\rangle_B\}$ an orthonormal basis for Hilbert space of system B. According to quantum mechanics, any pure state of the joint system AB can be expressed as a linear combination of $\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\}$, which form the basis for the two qubit-state.

Now, let us consider the following state vector in $\mathbb{C}^2 \otimes \mathbb{C}^2$

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

$|\psi\rangle_{AB}$ exhibits the intriguing property that it cannot be expressed as $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\phi\rangle_B$ where $|\phi\rangle_A$ and $|\phi\rangle_B$ refer to any state-vector in $\mathbb{C}^2$. This represents an example of a two-qubit entangled state. As previously discussed, if a bipartite state $\rho_{AB} \in \mathscr{D}(\mathscr{H}_A \otimes \mathscr{H}_B)$ can be written as $\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i$ where $\rho_A^i \in \mathscr{D}(\mathscr{H}_A)$ and $\rho_B^i \in \mathscr{D}(\mathscr{H}_B)$, then ρ_{AB} is called a separable state. Spatially separated parties can prepare separable states through local quantum operations and classical communication. As mentioned earlier, states that are not separable are referred to as entangled states. The two-qubit state space $\mathscr{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ constitutes a convex subset of the space of linear operators $\mathscr{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. Clearly, $\mathscr{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ has a dimension of 16. An arbitrary two-qubit state ρ_{AB} can be expressed as a linear combination of the basis elements of $\mathscr{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. In the Hilbert-Schmidt representation, ρ_{AB} assumes the following form:

$$\rho_{AB} = \frac{1}{4}\left(\mathbb{I}_A \otimes \mathbb{I}_B + \hat{r}.\vec{\sigma}_A \otimes \mathbb{I}_B + \mathbb{I}_A \otimes \hat{s}.\vec{\sigma}_B + \sum_{i,j=1}^{3} t_{ij}\sigma_{i_A} \otimes \sigma_{j_B}\right) \tag{2.4}$$

where in order to be a valid density operator, the following conditions must be satisfied:

$$|\hat{r}|^2 + |\hat{s}|^2 + \sum_{i,j=1}^{3} t_{ij}^2 \leq 3 \tag{2.5}$$

The equality is satisfied only for pure states and $\vec{r}$ and $\vec{s}$ are the Bloch vectors of the subsystems and $t_{ij} = \mathrm{Tr}((\sigma_{i_A} \otimes \sigma_{j_B})\rho_{AB})$ and similarly, $r_i = \mathrm{Tr}((\sigma_{i_A} \otimes \mathbb{I}_B)\rho_{AB})$ and $s_i = \mathrm{Tr}((\mathbb{I}_A \otimes \sigma_{i_B})\rho_{AB})$.Therefore, if two spatially separated parties, namely Alice and Bob, are provided with multiple copies of an unknown state, they can identify the state by performing local measurements and communicating the results of these measurements. This feature is generic, meaning it applies not only to two-qubit states but also to any composite state. This phenomenon is referred to as the local tomographic nature of quantum theory. Specifically, the state of a composite system can be determined from the statistics of local measurements performed on its subsystems [81]. Consequently, joint measurements on the entire system are not required to ascertain the state.

Subsystem of a Composite System:

Given the state of the composite system, the state of the subsystems *i.e.*, the marginal state can be determined using what is known as the partial trace. Let ρ_{AB} be the corresponding density operator for a bipartite system of two subsystems, say A and B. Then the marginal state of subsystem A is

$$\rho_A \equiv \mathrm{Tr}_B[\rho_{AB}]$$

where Tr_B is known as partial trace over subsystem B, which is a linear map from $\mathscr{D}(\mathscr{H}_A \otimes \mathscr{H}_B)$ to $\mathscr{D}(\mathscr{H}_B)$. It is defined as,

$$\mathrm{Tr}_B(|\psi_A\rangle\langle\phi_A| \otimes |\eta_B\rangle\langle\theta_B|) \equiv |\psi_A\rangle\langle\phi_A| \mathrm{Tr}[|\eta_B\rangle\langle\theta_B|] = |\psi_A\rangle\langle\phi_A| \langle\theta_B|\eta_B\rangle$$

2.2 Quantum Correlations and its Nonlocality

Quantum correlations refer to the collection of input-output probability statistics which is obtained when the respective parties perform local measurements on their respective subsystems of the multi-partite quantum state. For simplicity, we will only consider bipartite composite states. Such input-output statistics are denoted by $p(ab|xy) = \mathrm{Tr}[(E_a^x \otimes E_b^y)\rho_{AB}]$, where E_a^x refers to the POVM element corresponding to the outcome a of the measurement x and E_b^y refers to that of the b of the measurement y. This presents significant information-theoretic advantages, which will be discussed shortly.

In the following section, we outline the conceptual progression that culminated in the formulation of Bell's theorem, beginning with the renowned Einstein-Podolsky-Rosen (EPR) paradox.

2.2.1 EPR Paradox

Quantum mechanics is fundamentally a probabilistic theory. If this probabilistic framework is regarded as a *complete description* of a physical system, then the probabilities assigned by a pure quantum state to the outcomes of an observable can no longer be interpreted as mere subjective ignorance about the pre-existing definite values of that observable. Instead, these probabilities specify the likelihood of obtaining a particular value upon measuring that observable. This raises the question of the status of the observable when no measurement has been conducted. Quantum mechanics does not provide an answer to this inquiry. In 1935, Einstein, Podolsky, and Rosen published a seminal paper [82] in which they contended that, while quantum mechanics is internally consistent, it remains an incomplete description of reality. Their primary argument was founded on the following assumptions:

- Necessary condition for completeness: This says that a necessary condition for a theory to be complete is that "every element of the physical reality must have a counterpart in the physical theory".

- Sufficient condition for reality : "If, without in any way disturbing a system, we can predict with certainty (*i.e.*, with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity".

- Locality : "Elements of reality belonging to one system can not be affected (instantaneously) by measurements performed on another system which is spatially separated from the former".

These criteria were subsequently applied by EPR to a composite quantum system consisting of two spatially separated particles in an entangled state. In their original paper, the authors focused on position and momentum as observable quantities. To illustrate their reasoning, we present a simplified example involving two qubits in a pure entangled state, a scenario first introduced by Bohm [83].

Alice and Bob are two spatially separated parties who share a bipartite two-qubit entangled state

$$|\psi\rangle_{AB} = \frac{1}{2}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

The qubits previously interacted in their common past. However they are now spatially separated (let, qubit A be in Alice's lab and B be in Bob's lab). In this context, $|0\rangle$ and $|1\rangle$ refer to the normalised eigenstates of Pauli σ_z operator. On careful observation, it can be seen that the state $|\psi\rangle_{AB}$, interestingly can also be written as

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|+\rangle_A \otimes |-\rangle_B - |-\rangle_A \otimes |+\rangle_B)$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ refer to the normalised eigenstates of Pauli σ_x operator. Thus, if both Alice and Bob perform the same measurement on their respective individual subsystems (*i.e.*, both of them either measure σ_z or σ_x)), their outcomes will be anti-correlated. Hence, if Alice performs σ_z measurement on her qubit A, by observing her outcome, she can predict with certainty what will be Bob's outcome, if he performs σ_z measurement on his qubit B as well. This happens without in any way affecting Bob's qubit B. EPR articulated their position with the statement, *"since at the time of measurement the two systems no longer interact, no real change can take place in the second system in consequence of anything that may be done to the first system"*. Consequently, the observable σ_z associated with Bob's qubit is considered to possess an "element of physical reality." Conversely, Alice may opt to perform a σ_x measurement instead of σ_z. In this case, Alice can predict with certainty, without disturbing qubit B, the outcome of a potential σ_x measurement on qubit B. Thus, by the same rationale, the observable σ_x of qubit B also corresponds to an "element of physical reality." However, quantum mechanics prohibits the assignment of definite values to both observables σ_z and σ_x, given that these observables do not commute. This leads to their conclusion that quantum theory offers an incomplete depiction of nature.

2.2.2 Bell's Theorem

Following the conclusions drawn by EPR, a pertinent question arises regarding the potential for quantum theory to be augmented by a more fundamental hidden variable theory. In 1964 [84] (also see [85]), John S. Bell approached this inquiry by exploring whether any local realistic theory could replicate the statistical measurements predicted by quantum mechanics. For any theory that possesses an underlying local hidden variable framework, Bell established an inequality governing the bipartite correlations inherent to that theory. Each term in this inequality can be empirically measured. A more detailed formulation of this inequality is provided by J. Clauser *et al.* in Ref. [67]. In this section, we will succinctly outline Bell's inequality, as a more comprehensive discussion will be presented in the subsequent chapter. Let us consider two spatially separated parties, Alice and Bob, who share an arbitrary correlation.Let $\{A_0,A_1\}$ be Alice's measurements on her subsystem and $\{B_0,B_1\}$ are that of Bob's. The measurements are performed at random. The outcome of every measurement can either be 0 or 1. We denote Alice's and Bob's outcome by "a" and "b" respectively. Now, if Alice and Bob measure A_i and B_j on their respective subsystems, with a and b denoting their respective outcomes, the joint probability is denoted by $p(ab|A_i,b_j)$. Existence of a hidden variable description implies that

$$p(ab|A_i,B_j) = \int \mu(\lambda)p(ab|A_i,B_j,\lambda)d\lambda$$

where, $\mu(\lambda)$ refers to the probability distribution over the hidden variable λ. Locality condition implies that $p(a|A_i,B_j,\lambda) = p(a|A_i,B_{j'},\lambda)\ \forall i,j,j'$ and $p(b|A_i,B_j,\lambda) = p(b|A_{i'},B_j,\lambda)\ \forall j,i,i'$. *Reality*, (sometimes referred to as 'determinism'), on the other hand, asserts that $p(ab|A_i,B_j,\lambda) \in \{0,1\}, \forall a,b,\ A_i,B_j$. If the hidden variable model fulfills both the criteria of reality and locality, then the correlations observed at the operational level must adhere to the following inequality, known as the CHSH inequality [10]:

$$|\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle| \leq 2,$$

where, $\langle A_iB_j\rangle = \sum_{a,b=-1,+1} abp(ab|A_iB_j)$ denotes the expectation value associated with the measurements A_i and B_j which can be computed from the input-output statistics $p(ab|A_i,b_j)$. Importantly, there exist entangled quantum states and appropriate choices of measurements for Alice and Bob that can result in a violation of the CHSH inequality [9, 10, 86]. The implications are significant; local realism—the perspective grounded in classical intuition—cannot coexist with any hidden variable model that accurately replicates quantum statistical outcomes. For example, consider the state $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$ shared between Alice and Bob. Let $A_0 = \sigma_z,\ A_1 = \sigma_x,\ \ B_0 = \frac{\sigma_z+\sigma_x}{\sqrt{2}}$ and $B_1 = \frac{\sigma_z-\sigma_x}{\sqrt{2}}$. Applying the Born rule, the CHSH expression evaluates to $2\sqrt{2}$. This value represents the maximal violation of the CHSH inequality permissible within quantum theory, referred to as Cirel'son's bound [87].

2.2.3 2-2-2 Bell scenario and the NS set:

As discussed above, the simplest Bell scenario considers two parties, Alice and Bob, with their respective inputs to the box denoted as x and y, and outputs from the box denoted as a and b, respectively, where $x,y,a,b \in \{0,1\}$; and this is generally called the 2-2-2 Bell scenario. Correlation generated by a box P is the set of joint input-output probabilities, *i.e.*, $\mathrm{P} \equiv \{p(ab|xy)\}$. Set of boxes satisfying the no-signaling (NS) condition forms an 8-dimensional polytope $\mathbb{NS}$ having 24 vertices [63]: 8 non-local vertices (Popescu-Rohrlich (PR) boxes [49]) given by $\mathrm{P}_{NL}^{\alpha\beta\gamma} \equiv \{p(ab|xy) = \frac{1}{2}\delta_{(a\oplus b,\ xy\oplus\alpha x\oplus\beta y\oplus\gamma)}\}$ where $\alpha,\beta,\gamma \in \{0,1\}$, and 16 local deterministic vertices given by $\mathrm{P}_L^{\alpha_1\alpha_2\beta_1\beta_2} \equiv \{p(ab|xy) = \delta_{(a,\alpha_1 x\oplus\alpha_2)}\ \delta_{(b,\beta_1 y\oplus\beta_2)}\}$ where $\alpha_1,\alpha_2,\beta_1,\beta_2 \in \{0,1\}$. Collection of all local correlations forms a sub polytope $\mathbb{L}$, within $\mathbb{NS}$, with 16 local deterministic boxes as their vertices. Correlations obtained from local quantum measurements performed on some bipartite quantum state are called quantum correlations. Set of all quantum correlations $\mathbb{Q}$ forms a convex set (but not a polytope) lying strictly in between local and NS polytope, *i.e.*, $\mathbb{L} \subsetneq \mathbb{Q} \subsetneq \mathbb{NS}$ [88]. No signaling correlations that do not belong to the set $\mathbb{L}$ are called nonlocal as they do not allow a local-causal description [84]. First note that any NS correlation $\mathrm{C} \in \mathbb{NS}$ can be represented in the following matrix form:

$$\mathrm{C} \equiv \begin{array}{c c} xy/ab & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{pmatrix} p(00|00) & p(01|00) & p(10|00) & p(11|00) \\ p(00|01) & p(01|01) & p(10|01) & p(11|01) \\ p(00|10) & p(01|10) & p(10|10) & p(11|10) \\ p(00|11) & p(01|11) & p(10|11) & p(11|11) \end{pmatrix} \end{array} \tag{2.6}$$

where $p(ab|xy)$ denotes the probability of obtaining outcome a on Alice's side and outcome b on Bob's side given there inputs x and y respectively; $a,b,x,y \in \{0,1\}$. We consider one of the eight symmetries for the nonlocal correlations witnessed by the Bell CHSH inequality

$$\mathscr{B} \equiv \langle 00 \rangle - \langle 01 \rangle - \langle 10 \rangle - \langle 11 \rangle \leq 2, \tag{2.7}$$

where $\langle xy \rangle := \sum_{a,b} (-1)^{a \oplus b}\ p(ab|xy)$. Then, only one PR-box violates the inequality maximally, *i.e.*, yields CHSH value $\mathscr{B} = 4$ and there are exactly eight extremal local boxes that saturate the local bound. These nine boxes, which form an eight dimensional simplex [89], are as follows

$$\{\mathrm{P}_{NL}^{110}\} \Rightarrow \mathscr{B}=4, \quad \left\{ \begin{array}{c} \mathrm{P}_{L_1}^{0001},\ \mathrm{P}_{L_2}^{0100},\ \mathrm{P}_{L_3}^{0111}, \\ \mathrm{P}_{L_4}^{1101},\ \mathrm{P}_{L_5}^{1111},\ \mathrm{P}_{L_6}^{1000}, \\ \mathrm{P}_{L_7}^{0010},\ \mathrm{P}_{L_8}^{1010} \end{array} \right\} \Rightarrow \mathscr{B}=2. \tag{2.8}$$

The CHSH value $\mathscr{B} < 2$ for all the remaining extremal nonlocal or local boxes. The choice of this symmetry is due to the simple OR-AND function description of our distillation protocol. One can always apply local reversible relabellings to switch to any of the eight symmetries (then the protocol become suitably relabelled OR-AND). From here on, we will simply refer to the nine boxes in Eq. (2.8) by dropping their superscripts.

These boxes are given by,

$$\mathrm{P}_{NL} \equiv \mathrm{P}_{NL}^{110} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix};$$

$$\mathrm{P}_{L_1} \equiv \mathrm{P}_{L_1}^{0001} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \mathrm{P}_{L_2} \equiv \mathrm{P}_{L_2}^{0100} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix};$$

$$\mathrm{P}_{L_3} \equiv \mathrm{P}_{L_3}^{0111} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \mathrm{P}_{L_4} \equiv \mathrm{P}_{L_4}^{1101} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix};$$

$$\mathrm{P}_{L_5} \equiv \mathrm{P}_{L_5}^{1111} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \mathrm{P}_{L_6} \equiv \mathrm{P}_{L_6}^{1000} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix};$$

$$\mathrm{P}_{L_7} \equiv \mathrm{P}_{L_7}^{0010} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \mathrm{P}_{L_8} \equiv \mathrm{P}_{L_8}^{1010} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

2.2.4 Nonlocality without Inequality:

The seminal result of Bell was later extended by Lucien Hardy through a different approach [68, 69]. Hardy's argument involves two spatially separated parties, Alice and Bob, who share a bipartite system and perform measurements on their respective subsystems. Alice chooses between measurements A_0 and A_1, while Bob selects between B_0 and B_1, with outcomes either 0 or 1. From the set of 16 joint probabilities in this scenario, Hardy selects four specific joint probabilities:

$$p_{\text{Hardy}} \equiv p(0,0|A_0,B_0) > 0, \tag{2.9}$$
$$p(0,0|A_0,B_1) = p(0,0|A_1,B_0) = p(1,1|A_1,B_1) = 0,$$

The probability p_{Hardy} in Eq.(2.9) quantifies strength of nonlocality of Hardy correlations. If the first condition holds, then for some local hidden variable λ (since $q > 0$), we have $A_0^\lambda = 0$ and $B_0^\lambda = 0$. The second and third conditions imply $B_1^\lambda = 1$ and $A_1^\lambda = 1$, which contradicts the fourth condition.

Interestingly, every non-maximally entangled pure two-qubit state exhibits Hardy's nonlocality, while the maximally entangled states do not [90, 91]. Moreover, unlike Bell-CHSH violations, mixed states of two-qubit systems do not display Hardy's nonlocality [92]. While the maximum value of p_{Hardy} in no-signaling set is $1/2$ (achieved with PR box), its optimal value in quantum mechanics turns out to be $(5\sqrt{5}-11)/2 \approx 0.09$ [93] (see also [94, 95]), and it is achieved on a pure two qubit state with projective measurements. The correlation yielding the maximum Hardy nonlocality in quantum theory reads

$$\begin{aligned} \mathrm{H}_Q^{\max} &= (5\sqrt{5}-11)\ \mathrm{P}_{NL} \\ &\quad + \frac{1}{2}(7-3\sqrt{5})\ \sum_{i=1}^{4} \mathrm{P}_{L_i} + (\sqrt{5}-2)\ \mathrm{P}_{L_5}, \end{aligned} \tag{2.10}$$

and it has been shown to be an extreme point of the set $\mathbb{Q}$ [88].

In addition to its foundational significance, nonlocal correlations from quantum states have practical applications in communication complexity [96, 97], quantum cryptography [20, 98, 99], device-independent cryptography [100, 101], randomness certification [51–60], and device-independent randomness generation [102–107].

2.2.5 No-Signalling Principle and Quantum Correlations

Quantum correlations exhibit nonlocality, yet they cannot facilitate faster-than-light communication [108]. To understand this more generally, consider a scenario where Alice and Bob are spatially separated at large distance between themselves and share a bipartite quantum state ρ_{AB}. Bob's marginal state is given by $\mathrm{Tr}_A(\rho_{AB}) := \rho_B$. If Alice performs a local operation, (suppose a measurement) $\mathscr{E}_A$ on her part of the subsystem of the composite state ρ_{AB}, the joint state ρ_{AB} will accordingly transform to

$$\rho'_{AB} = (\mathscr{E}_A \otimes \mathbb{I}_B)\rho_{AB} = \sum_k M_k \otimes \mathbb{I}_B(\rho_{AB})M_k^\dagger \otimes \mathbb{I}_B$$

where $\{M_k\}$ are the Kraus elements corresponding to Alice's measurement $\mathscr{E}_A$ satisfying $\sum_k M_k^\dagger M_k = \mathbb{I}$. (while $\{M_k \otimes \mathbb{I}_B\}$ are the Kraus operators corresponding $\mathscr{E}_A \otimes \mathbb{I}_B$). After Alice's operation, the reduced state of Bob's subsystem becomes $\rho'_B = \mathrm{Tr}_A(\rho'_{AB})$. Now if $\rho'_B \neq \rho_B$, Alice could send information to Bob instantaneously, violating the no-signaling principle. However, upon calculating:

$$\rho'_B = \mathrm{Tr}_A(\sum_k M_k \otimes \mathbb{I}_B(\rho_{AB})M_k^\dagger \otimes \mathbb{I}_B) = \mathrm{Tr}_A(\sum_k M_k^\dagger M_k \otimes \mathbb{I}_B(\rho_{AB})) = \mathrm{Tr}_A(\rho_{AB}) = \rho_B.$$

we see that the reduced state of Bob's subsystem remains unchanged by Alice's local actions. This ensures compliance with the no-signaling principle, preventing superluminal communication. Consequently, all correlations derived from composite quantum states inherently respect the no-signaling condition. This compatibility between quantum mechanics and special relativity has profound implications in quantum information theory. For example, foundational results such as the no-cloning and no-deleting theorems can be derived as consequences of the no-signaling principle [109, 110].

Here, we provide a concise demonstration of why a universal quantum cloning device is impossible, based on the no-signalling principle.

No Cloning Theorem from No-signalling Principle:

The no-cloning theorem is a foundational result in quantum information theory, asserting the impossibility of perfectly copying an arbitrary unknown quantum state [111]. This theorem has been shown to follow from the principle that quantum mechanics prohibits faster-than-light communication [109, 112]. Additionally, Gisin established a bound on the fidelity of an imperfect quantum cloning machine [109]. Here, we outline a proof demonstrating the impossibility of a perfect universal quantum cloning device as a direct consequence of the no-signalling principle. Suppose Alice and Bob are spatially separated and share an entangled state:

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B)$$

. Assume further that Bob has access to a universal cloning device $\mathscr{C}$. By performing a σ_z measurement on her subsystem, Alice can remotely prepare an ensemble at Bob's location consisting of $|1\rangle_B\langle 1|$ and $|0\rangle_B\langle 0|$ with equal probability, resulting in the mixed state:If Bob's state is $|1\rangle_B\langle 1|$, the action of the cloning device $\mathscr{C}$ on $|1\rangle_B\langle 1|\otimes|B\rangle_R\langle B|$ produces the output:$|1\rangle_B\langle 1|\otimes|1\rangle_R\langle 1|$, where $|B\rangle_R$ represents the fixed initial state of an ancillary system, *i.e.*,

$$|1\rangle_B\langle 1|\otimes|B\rangle_R\langle B| \xrightarrow{\mathscr{C}} |1\rangle_B\langle 1|\otimes|1\rangle_R\langle 1|$$

On the other hand, at Bob's side, if the state is $|0\rangle_B\langle 0|$, then after action of $\mathscr{C}$ on $|0\rangle_B\langle 0|\otimes|B\rangle_R\langle B|$ we get $|0\rangle_B\langle 0|\otimes|0\rangle_R\langle 0|$ *i.e.*,

$$|0\rangle_B\langle 0|\otimes|B\rangle_R\langle B| \xrightarrow{\mathscr{C}} |0\rangle_B\langle 0|\otimes|0\rangle_R\langle 0|$$

Thus, if Alice performs a σ_z measurement on her subsystem of the state $|\psi^-\rangle_{AB}$, and Bob subsequently applies the cloning operation $\mathscr{C}$ to his subsystem along with a fixed state of an ancillary system, the ensemble generated at Bob's side becomes an equal mixture of $|1\rangle_B\langle 1|\otimes|1\rangle_R\langle 1|$ and $|0\rangle_B\langle 0|\otimes|0\rangle_R\langle 0|$, *i.e.*,

$$\frac{1}{2}\Big\{|1\rangle_B\langle 1|\otimes|1\rangle_R\langle 1|)+|0\rangle_B\langle 0|\otimes|0\rangle_R\langle 0|\Big\}.$$

If Alice measures σ_x instead of σ_z, the ensemble prepared on Bob's side will be a mixture of $|x\rangle_B\langle x|$ and $|\bar{x}\rangle_B\langle\bar{x}|$, *i.e.*, $\frac{1}{2}(|x\rangle_B\langle x|+|\bar{x}\rangle_B\langle\bar{x}|)$, where $|x\rangle := |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $|\bar{x}\rangle := |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$, the eigenstates of the Pauli σ_x operator. Using a similar approach, the final ensemble at Bob's side (after applying the cloning device to Bob's subsystem and the ancillary system) is given by the following:

$$\frac{1}{2}\Big\{|x\rangle_B\langle x|\otimes|x\rangle_R\langle x|+|\bar{x}\rangle_B\langle\bar{x}|\otimes|\bar{x}\rangle_R\langle\bar{x}|\Big\}.$$

Note that,

$$\frac{1}{2}\Big\{|x\rangle_B\langle x|\otimes|x\rangle_R\langle x|+|\bar{x}\rangle_B\langle\bar{x}|\otimes|\bar{x}\rangle_R\langle\bar{x}|\Big\}\neq\frac{1}{2}\Big\{|1\rangle_B\langle 1|\otimes|1\rangle_R\langle 1|+|0\rangle_B\langle 0|\otimes|0\rangle_R\langle 0|\Big\}.$$

This breaches the no-signalling principle, as Alice can convey her message through her choice of measurement. Following the operation of the universal cloning machine $\mathscr{C}$, the resulting density matrices differ. Consequently, Bob can infer from the observed statistics which ensemble Alice has remotely prepared, allowing him to determine whether Alice performed a σ_z or σ_x measurement on her subsystem. Thus, the harmonious coexistence of quantum theory and special relativity would be disrupted if the existence of a universal quantum cloning device were assumed.

2.3 Convex Operational Theories:

Quantum mechanics is the most successful theory till date. Its postulates are mathematical but even then the mathematical structure is elegant. In the simplest Bell scenario, we have seen that quantum mechanics proves to be a nonlocal theory. However it is not "maximally" nonlocal— the maximum CHSH expression obtainable from quantum theory cannot go beyond $2\sqrt{2}$, let alone reach the algebraic maximum 4. Hence this "power" of quantum theory is limited.

The operational implications of this beautiful theory led to the birth of quantum information theory which has in many aspects has more information processing power than classical information theory. Researchers wanted to study both these theories in a broader class of theories which encompasses both these theories. The theory of quantum mechanics is built on ad-hoc mathematical postulates that cry out for physical justification. On the other hand, the study of generalized probability theory (GPT) has garnered significant attention from the physics community, especially regarding the broader goal of reconstructing quantum mechanics from first principles [24–36]. Within this broader framework, simple toy models are explored that exhibit non-classical features, providing deeper insights into the foundations of quantum mechanics [32–36]. These GPTs help us to address many nonclassicalities found in quantum theory from a broader point of view. A deeper understanding of quantum theory is brought about by contrasting these theories with quantum mechanics in several information processing scenarios.

Keeping only in mind that any operational theory should have a concept of preparation or states, the measurements or effects which acts on the states and the transformations or dynamics governing the evolution of the state, the generalization of classical probability theory led to the creation of these broader class of theories. Convexity is a natural assumption and thus convex operational theories were born in which both classical and quantum theory were members.

2.3.1 States and Effects

We start by briefly recalling the framework of GPT. For a detailed overview of this framework we refer to the works [27–31, 37]. In the recent past several interesting results have been reported within this framework [33, 113–118]. A GPT is specified by a list of system types and the composition rules specifying combination of several systems, where a system S is specified by identifying the three-tuple $(\Omega_S, \mathscr{E}_S, \mathscr{T}_S)$ of the state space, effect space, and the set of transformations. In a prepare and measure scenario, which will be considered in this work, it is sufficient to describe Ω_S and $\mathscr{E}_S$ only.

State space [Ω_S]: A state ω_S for a system S is a mathematical entity that provides the probabilities of outcomes for all possible measurements on the system. The collection of all permissible states constitutes the state space Ω_S, which is typically regarded as a compact and convex set situated within a real vector space V. Convexity ensures that if ω_1 and ω_2 are valid states, their classical mixture $p\omega_1 + (1-p)\omega_2$ is also a valid state. Compactness, on the other hand, guarantees no physical difference exists between states that are prepared exactly and those prepared to an arbitrary degree of accuracy [119]. The extreme points of Ω_S are referred to as pure states, representing states of maximal knowledge.

Effect space [$\mathscr{E}_S$]: The mathematical structure of measurements in GPTs is encapsulated by effects. An effect e is a linear functional acting on V such that $e : \Omega_S \to [0,1]$. The unit effect is defined by $u(\omega) = 1,\ \forall\ \omega \in \Omega_S$. The set of all proper effects $\mathscr{E}_S \equiv \{e \mid 0 \leq e(\omega) \leq 1,\ \forall\ \omega \in \Omega_S\}$ is the convex hull of zero effect, unit effect and the extremal effects and embedded in the vector space $V^\star$ dual to V. A measurement $\mathscr{M}$ is a collection of effects that sum to the unit effect, *i.e.* $\mathscr{M} \equiv \{e_i \in \mathscr{E}_S \mid \sum_i e_i = u\}$.

State and effect cones: Sometimes it is mathematically convenient to work with the notion of unnormalized states and effects. The set of unnormalized states $V_+ \subset V$ is the conical hull of Ω_s, *i.e.*, $r\omega \in V_+$ for $r \geq 0$ and $\omega \in \Omega_S$. The set of unnormalized effects is its dual cone $V_+^\star \subset V^\star$, *i.e.*, $V_+^\star \equiv \{e \mid e(\omega) \geq 0,\ \forall\ \omega \in V_+\}$. The formulation generally assumes the 'no-restriction hypothesis' which demands that the state and effect cones are dual to each other [29].

2.3.2 Joint System

Composite system: Given two systems with state spaces $\Omega_A \subset V_A$ and $\Omega_B \subset V_B$, the state space Ω_{AB} for the composite systems is embedded in the vector space V_{AB}

which is the tensor product of the component vector spaces, *i.e.* $V_{AB} = V_A \otimes V_B$ [120]. The choice of Ω_{AB} is however not unique which brings forth several interesting ways of relating Ω_A, Ω_A with Ω_{AB}. Instead of arbitrary composition rules which might be mathematically valid, from a physical point of view, the no signaling principle and tomographic locality postulate [27] bound the choices within two extremes – the minimal tensor product space and maximal tensor product space [38].

1. For a pair of effects (e_A, e_B), where $e_A \in \varepsilon_A$ and $e_B \in \varepsilon_B$, every joint state $\omega_{AB} \in \Omega_{AB}$ must assign consistent joint probabilities.

2. **The no-signalling principle:** This states that the joint statistics on a joint system AB should be such that the marginal probability distribution for the outcomes of a measurement on one part B should not be affected by the measurements performed on the other part A and vice-versa.

3. **The local tomography principle:** This states that given arbitrary copies of a state AB, it should be possible to identify the state of the joint system AB through local measurements performed by the parties on their respective subsystems. The parties need to be communicating classically. Thus joint statistics is sufficient to pinpoint the joint state of the system AB.

More formally,

$$\begin{aligned}
\Omega_{AB}^{\min} \equiv \{\omega_{AB} = \sum_i p_i \omega_A^i \otimes \omega_B^i \mid \omega_A^i \in \Omega_A, \\
\omega_B^i \in \Omega_B;\ p_i \geq 0 \ \&\ \sum_i p_i = 1\}, \\
\Omega_{AB}^{\max} \equiv \{\omega_{AB}\ \in V_{AB} \mid 1 \geq\ e_A \otimes e_B(\omega_{AB}) \geq 0, \\
\forall\ e_A \in \mathscr{E}_A \ \&\ e_B \in \mathscr{E}_B\}\,.
\end{aligned}$$

It is not hard to see that the cone $(V_{AB}^{\min})_+$ is isomorphic to the dual cone $(V_{AB}^{\max})_+$. Therefore, in accordance with the no-restriction hypothesis for the case of minimal composition, the effect cone $(V_{AB}^{\min})_+^\star \cong (V_{AB}^{\max})_+$, and for the case of maximal composition, the effect cone $(V_{AB}^{\max})_+^\star \cong (V_{AB}^{\min})_+$. The symbol $\cong$ denotes isomorphism.

2.4 Quantum Theory: a GPT

Quantum theory can be seen as a special instance of a GPT. State space of a d-level quantum system associated with complex Euclidean space $\mathbb{C}^d$ is the set of density operators acting on $\mathbb{C}^d$, *i.e.*, $\Omega(\mathbb{C}^d) \equiv \mathscr{D}(\mathbb{C}^d)$. The set $\mathscr{D}(\mathbb{C}^d)$ is a compact and convex set embedded within $\mathbb{R}^{d^2-1}$. The unnormalized state cone is the set of all non-negative operators $\mathscr{P}(\mathbb{C}^d) := \{\lambda\rho \mid \lambda \geq 0 \;\&\; \rho \in \mathscr{D}(\mathbb{C}^d)\}$, which is also the unnormalized effect cone. In other words, quantum theory is self dual. The minimal composition of two quantum systems associated with Hilbert spaces $\mathbb{C}^{d_A}$ and $\mathbb{C}^{d_B}$ allows only separable state we call it as SEP composition and denote the resulting system as the triplet $S^{AB}_{\text{SEP}} \equiv \left[\mathbb{C}^{d_A}, \mathbb{C}^{d_B}, \bigotimes_{\text{SEP}}\right]$. Formally the state space for the SEP composition is given by

$$\begin{aligned}\Omega_{\text{SEP}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}) := \Bigg\{ & \rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i \mid p_i \geq 0 \\ & \& \sum_i p_i = 1;\ \rho_A^i \in \mathscr{D}(\mathbb{C}^{d_A}),\ \rho_B^i \in \mathscr{D}(\mathbb{C}^{d_B}) \Bigg\}.\end{aligned}$$

Since $\Omega_{\text{SEP}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$ contains only separable states, the corresponding effect space $\mathscr{E}_{\text{SEP}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$ contains effects that are not allowed in quantum theory. Entanglement witness operators yielding positive probability on separable states are valid effects in this composition although they are not allowed in quantum theory. On the other extreme, the maximal composition, which we will call $\overline{\text{SEP}}$, and the resulting system denote as $S^{AB}_{\overline{\text{SEP}}} \equiv \left[\mathbb{C}^{d_A}, \mathbb{C}^{d_B}, \bigotimes_{\overline{\text{SEP}}}\right]$, has the state space

$$\begin{aligned}\Omega_{\overline{\text{SEP}}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}) := \Big\{ & W_{AB} \in \text{Herm}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}) \mid \\ & \text{Tr}(W_{AB}) = 1, \text{Tr}[W_{AB}(\pi_A \otimes \pi_B)] \geq 0 \\ & \forall\ \pi_A \in \mathscr{P}(\mathbb{C}^{d_A}), \pi_B \in \mathscr{P}(\mathbb{C}^{d_B}) \Big\}.\end{aligned}$$

Here $\text{Herm}(\mathscr{X})$ denotes the set of Hermitian operators acting on the space $\mathscr{X}$, and normalization demands $\text{Tr}(W_{AB}) = 1\ \forall\ W_{AB} \in \Omega_{\overline{\text{SEP}}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$. The unnormalized effect cone corresponding to $\mathscr{E}_{\overline{\text{SEP}}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$ is identical to the unnormalized state cone corresponding to the set $\Omega_{\text{SEP}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$. For the quantum case $S^{AB}_Q \equiv \left[\mathbb{C}^{d_A}, \mathbb{C}^{d_B}, \bigotimes_Q\right]$ we have $\Omega_Q(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}) = \mathscr{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$, and the effect cone is identical to the state cone which represents the self duality of quantum theory. The following set inclusion relations are immediate

$$\begin{aligned}\Omega_{\text{SEP}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}) \subset \Omega_Q(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}) \subset \Omega_{\overline{\text{SEP}}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}), \\ \mathscr{E}_{\overline{\text{SEP}}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}) \subset \mathscr{E}_Q(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}) \subset \mathscr{E}_{\text{SEP}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}).\end{aligned}$$

Between SEP and $\overline{\text{SEP}}$, many other compositions can be defined by appending/deducting suitable states/effects. Among these, quantum composition is the only one that is self-dual.

Chapter 3

A Local Quantum State Discrimination Problem

3.1 Motivation

Distinct objects or perfectly distinguishable states of a system can be used to store information which assures the readability of the information without any ambiguity. Pure classical states are always perfectly distinguishable and hence can be used for encoding and decoding. In the quantum world, however, encoding in any pure state would not be a wise idea, as all the information protocols such as [4, 5, 121–124], are governed by rules that are fundamentally different from our classical worldview. For instance, classical information encoded in non-orthogonal quantum states, either pure or mixed, cannot be perfectly decoded since the no-cloning theorem [6] (more generally the no-broadcasting theorem [125]) puts restrictions on their perfect discrimination.

Distinguishability of two states in quantum theory boils down to their orthogonality. Such a constraint is strictly quantum (more precisely, non-classical [32, 126]) in nature. The reason is that the state space of a classical system having a finite number of perfectly distinguishable states is described by some simplex embedded in some $\mathbb{R}^d$ where extreme points of the simplex correspond to the pure states. On the other hand, distributions on phase space represent mixed state while delta distributions, *i.e.,* the phase space points correspond to pure states that are unaccountably many in numbers but perfectly distinguishable at least in principle.

Now even the set of perfectly distinguishable quantum states becomes further constrained under restricted measurement settings, such as local operations and classical communication (LOCC) [12, 127–135], separable operations (SEP)

[136–138], or positivity of partial transposition (PPT) preserving operations [139, 140]. A notable nonclassical feature of multipartite quantum systems, often regarded as a signature of *nonlocality*, is that there exist sets of multipartite states that cannot be discriminated locally but can be perfectly distinguished when complete global access is granted. In contrast to Bell-type nonlocality, which only manifests in entangled states, Bennett *et al.* [12] demonstrated that this form of nonlocality can also arise in sets of orthogonal product quantum states. Since product states can be prepared locally, their restricted distinguishability through local operations on subsystems held by each party unveils another form of quantum nonlocality, termed *quantum nonlocality without entanglement*.

During the last two decades LSD has been studied in great detail resulting in a plethora of interesting conclusions [141–156] and it also finds applications in useful tasks [157, 13, 158, 15, 159]. Apart from LSD and more general quantum state discrimination problems [160–162], several other discrimination tasks, *eg.* channel/sub-channel discrimination, process discrimination, circuit discrimination, have been studied during the recent past [163–166] that subsequently motivate several novel information protocols [167–171].

In this chapter, which is based on one of our works [76] we shall present the Local State Marking (LSM) task, wherein a subset of states chosen randomly from a known set of multipartite states is provided to spatially separated parties without revealing the identities of the individual states. The aim is to mark the identities of the states under the operational paradigm of LOCC. For a given set of multipartite states $\mathscr{S}$ one can define a class of discrimination tasks denoted by m-LSM. Here $1 \leq m \leq |\mathscr{S}|$ with 1-LSM corresponding to the task of LSD and the $|\mathscr{S}|$-LSM task we will denote simply as LSM where $|\mathscr{S}|$ is the cardinality of set $\mathscr{S}$.

This chapter has been arranged as follows: in Section 3.2, we first discuss the LOCC framework in short, although it has been discussed in Chapter 1. In Section 3.3, we explicitly discuss the concept of *quantum nonlocality without entanglement* by providing an example of the set of mutually orthogonal product states that are locally indistinguishable. In Section 3.4, we discuss the various constraints that can be imposed on measurements. We then briefly discuss the problem of local state discrimination (LSD) in Section 3.5. In Sections 3.6 and 3.7, we discuss the seminal results of Walgate *et. al.* and Hayashi *et. al.*, which anyone working local state discrimination must necessarily know. Section 3.8 deals with what we mean by the task of local state marking (LSM) and presents a few observations. Some generic implications between m-LSM and m'-LSM tasks are also analyzed when $m \neq m'$. In Section 3.9, we find that the task of LSM is distinct from the task of LSD. In particular, we show that the local distinguishability of an arbitrary set of states always implies local markability, but the converse does not always hold. This result is shown by providing an example of mutually orthogonal states that are locally markable but not locally distinguishable. We then provide examples of orthogonal states that can neither be distinguished nor marked perfectly under local operations in Section 3.10. Then in Section 3.11, we study entanglement-assisted local marking of states where additional entanglement is provided as a resource to mark the states that are otherwise locally unmarkable. There we report an intriguing entanglement assisted catalytic LSM phenomenon– a locally unmarkable set of states can be perfectly marked when additional entanglement is supplied as a resource. Interestingly, the entanglement is returned (either partially or completely) once the marking task is done. In Section 3.12, we then consider an information-theoretic task, wherein we show that choosing LSM over the conventional multi-copy LSD proves to be more economical in conveying classical messages from the referee to the parties. Then we finally conclude in Section 3.13.

3.2 The LOCC framework

In the multipartite scenario, when different parts of the quantum systems are held by spatially separated parties, the class of operations LOCC captures the 'distant lab' paradigm. Although it is extremely hard to characterize the structure of LOCC operations [23], this restricted paradigm plays a crucial role in understanding the resource of quantum entanglement and it constitutes the scenario for the task of m-LSM which will be discussed later. In the well-established framework of Local Operations and Classical Communication (LOCC), one envisions multiple parties spatially separated in distinct laboratories. A referee selects a random state from a set of multipartite states, which are known to the parties, and distributes individual subsystems to each participant. Due to the setup, each party is restricted to local measurements and can only collaborate via classical communication.

3.3 Nonlocality from Unentangled States

Here, the nonlocality we refer to is in the context of state discrimination under the LOCC framework, which we have discussed in Chapter 1. Peres and Wootters demonstrated that, in the task of distinguishing between three carefully chosen bipartite product states within the LOCC framework, global measurements are optimal, whereas local measurements on individual subsystems prove to be suboptimal [11]. This result implies that certain bipartite product states, although locally preparable by two parties, require a joint measurement for optimal discrimination—a procedure that cannot be implemented by spatially separated parties constrained to classical communication.

In 1999, Charles H. Bennett and his collaborators went a step further and showed that it can so happen that a set of bipartite product orthogonal quantum states are perfectly distinguishable when there is access to both the subsystems, but cannot be distinguished when the subsystems are in two spatially separated parties' laboratories [12]. The unavailability of the access of the two subsystems together shows its signature in the optimal distinguishing probability of those states.

When the composite system is available, any global operation can be implemented, which helps in the distinguishability task. However, when the spatially separated parties have only access to their respective subsystem, only local operations can be implemented by the parties, which has been shown to be a strict subset of global operations, even if the parties are allowed to communicate classically. This is the LOCC scenario where LO stands for local operations and CC for classical communication. This gap in the distinguishing probability between the two scenarios mentioned above is the nonlocality that is being referred to.

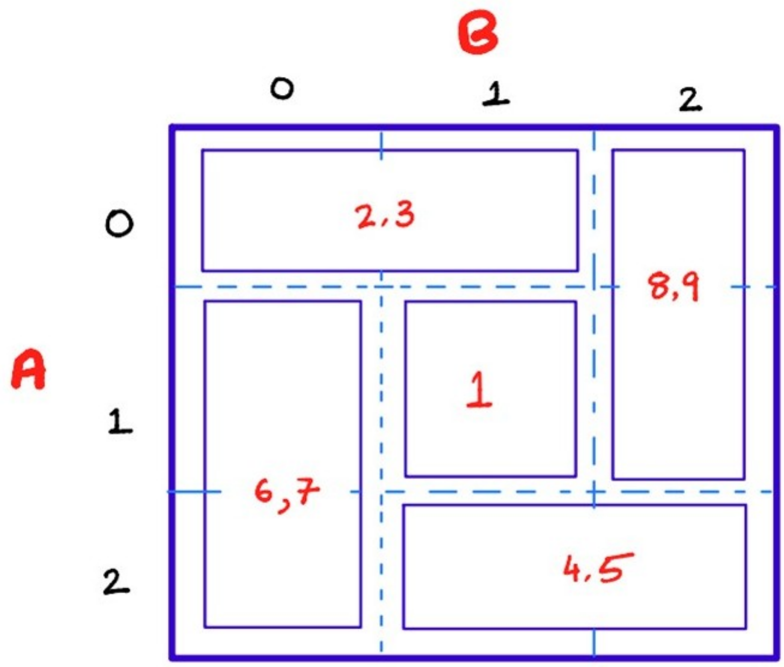

FIG. 3.1 A graphical representation of the nine mutually orthogonal states, illustrated as a set of dominoes.

According to [12], the following set of nine orthogonal product states, in $\mathbb{C}^3 \otimes \mathbb{C}^3$ could not be distinguished under LOCC

$$
\begin{aligned}
|\psi_1\rangle_{AB} &= |1\rangle_A |1\rangle_B \\
|\psi_2\rangle_{AB} &= |0\rangle_A |0+1\rangle_B \\
|\psi_3\rangle_{AB} &= |0\rangle_A |0-1\rangle_B \\
|\psi_4\rangle_{AB} &= |2\rangle_A |1+2\rangle_B \\
|\psi_5\rangle_{AB} &= |2\rangle_A |1-2\rangle_B \\
|\psi_6\rangle_{AB} &= |1+2\rangle_A |0\rangle_B \\
|\psi_7\rangle_{AB} &= |1-2\rangle_A |0\rangle_B \\
|\psi_8\rangle_{AB} &= |0+1\rangle_A |2\rangle_B \\
|\psi_9\rangle_{AB} &= |0-1\rangle_A |2\rangle_B
\end{aligned}
$$

The normalization constant has been ignored for the sake of simplicity. Also $|p \pm q\rangle := (|p\rangle \pm |q\rangle)$ with $p \in \{0,1\}$ and $q \in \{1,2\}$.

A simpler proof for the local indistinguishability of the above set can be found in [128]. In that paper, the authors have shown mathematically that there exists no nontrivial orthogonality preserving local measurement for any of the parties A or B which can eliminate some of the possibilities of given $|\psi_k\rangle_{AB}$, $k \in \{1, 2, \cdots, 9\}$.

Thus, it is through a discrimination task that seemingly "classical" product states were able to reveal their nonlocality, a property that has since proven immensely useful in various cryptographic and information-theoretic tasks.

The primary goal of this chapter is to explore local state discrimination tasks, which hold potential applications in various information-theoretic contexts. Before this, we will examine the range of measurements that can be performed on composite systems under various imposed constraints.

3.4 Measurements: Global vs PPT vs SEP vs LOCC

When the subsystems of a composite system are available, any global operation can be implemented which is allowed in quantum theory. However, it is interesting to see what operations can be performed when constraints start being imposed.

We know that a Positive Operator-Valued Measure (POVM) on $\mathscr{H}$ having n outcomes is a set of n linear operators $\{M_i\}_{i=1}^n$, where $M_i \geq 0 \ \forall i$ and $\sum_i M_i = \mathbb{I}_{\mathscr{H}}$, where $\mathbb{I}_{\mathscr{H}}$ denotes the identity operator on $\mathscr{H}$. When we consider multipartite systems, the set of measurements shows a richer structure than what is observed for measurements acting on single systems.

Let us consider for simplicity a bipartite system. Hilbert spaces associated with the subsystems are denoted as $\mathscr{H}_A$ and $\mathscr{H}_B$ respectively.

- **Global measurement:** These are all the measurements that can be implemented on the joint state. Mathematically, we have a set of n operators $\{M_i\}_{i=1}^n$ s.t $M_i \in \text{Pos}(\mathscr{H}_A \otimes \mathscr{H}_B) \ \forall i$ and $\sum_i M_i = \mathbb{I}_{\mathscr{H}_A \otimes \mathscr{H}_B}$ where $I_{\mathscr{H}_A \otimes \mathscr{H}_B}$ is the identity operator on $\mathscr{H}_A \otimes \mathscr{H}_B$.

- **PPT-POVMs:** We call a positive semidefinite operator $E \in \mathscr{L}(\mathscr{H}_A \otimes \mathscr{H}_B)$ to be a PPT operator if $E^{T_A} \geq 0$ where T_A refers to the partial transpose operation with respect to the party A, *i.e*

$$(|ij\rangle \langle kl|)^{T_A} = |kj\rangle \langle il| \tag{3.1}$$

A Positive-Operator-Valued-Measure (POVM) on with n outcomes *i.e* $\mathbb{M} := \{M_i\}_{i=1}^n$ s.t $M_i \in \text{Pos}(\mathscr{H}_A \otimes \mathscr{H}_B)$ $\forall i$ and $\sum_i M_i = I_{\mathscr{H}_A \otimes \mathscr{H}_B}$, is said to be a PPT-POVM if each M_i is PPT, where $I_{\mathscr{H}_A \otimes \mathscr{H}_B}$ is the identity operator on $\mathscr{H}_A \otimes \mathscr{H}_B$.

- **SEP-POVMs:** A Positive-Operator-Valued-Measure (POVM) $\mathbb{M}$ with n outcomes is called a SEP-POVM if $\{M_i\}_{i=1}^n$ is a POVM on $\mathscr{H}_A \otimes \mathscr{H}_B$ s.t $M_i/Tr(M_i)$ is a separable quantum state $\forall$ i and $\sum_{i=i}^n M_i = \mathbb{I}_{\mathscr{H}_A \otimes \mathscr{H}_B}$ where $I_{\mathscr{H}_A \otimes \mathscr{H}_B}$ is the identity operator on $\mathscr{H}_A \otimes \mathscr{H}_B$.

- **LOCC:**While LOCC is the natural class of operations for many essential quantum information tasks, its mathematical structure remains complex and challenging to characterize. See [23] for an in-depth understanding.

It is known that any POVM that can be realized using an LOCC protocol is a PPT POVM. Moreover, all SEP-POVMs are trivially PPT-POVMs but not the converse. Hence, we have

$$\text{LOCC-POVMs} \subset \text{SEP-POVMs} \subsetneq \text{PPT-POVMs}$$

The result by Bennett *et al.* discussed in the previous section showed that it is not always possible to implement separable superoperators locally.
Thus,

$$\text{LOCC POVMs} \subsetneq \text{SEP-POVMs} \subsetneq \text{PPT-POVMs}$$

See [172, 173] for an in-depth understanding.

3.5 Local Quantum State Discrimination (LSD)

As we have discussed before, while a set of mutually orthogonal quantum states can always be distinguished perfectly when no restrictions on operations are there, interesting situations arise for multipartite quantum systems when discriminating operations among the spatially separated parties holding different

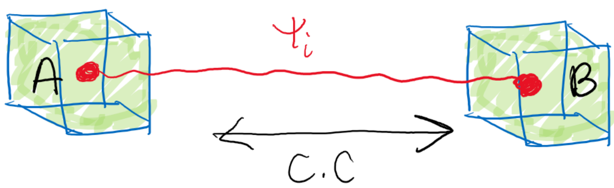

FIG. 3.2 The task of Local State Discrimination

subsystems are limited to local quantum operation assisted with classical communication (LOCC). This constitutes the framework for the problem of local state discrimination (LSD) [174–181].

A state chosen randomly from a set of known set of K mutually orthogonal bipartite quantum states $\mathscr{S} \equiv \{|\psi_j\rangle \mid \langle\psi_i|\psi_j\rangle = \delta_{ij}\} \subset \mathbb{C}_A^{d_A} \otimes \mathbb{C}_B^{d_B}$ are distributed among spatially separated parties Alice and Bob without revealing the identity of the state. They have to identify the index i using LOCC.

In the next section, the seminal result of Jonathan Walgate, et. al. will be discussed which deals with the local distinguishability of any two pure, mutually orthogonal multipartite quantum states, regardless of their entanglement [175].

3.6 Distinguishability of any two orthogonal pure states

Theorem 1. *Any two orthogonal pure multipartite states, $|\Psi\rangle$ and $|\Phi\rangle$, can be exactly distinguished using local operations and classical communication (LOCC).*

We shall discuss the bipartite scenario for the sake of simplicity. They show that it is always possible via local operations to find a basis such that $|\Psi\rangle$ and $|\Phi\rangle$ can be represented as :

$$|\Psi\rangle = |1\rangle_A |\eta\rangle_B + \cdots + |l\rangle_A |\eta_l\rangle_B \tag{3.2}$$

and

$$|\Phi\rangle = |1\rangle_A |\eta_1^{\perp}\rangle_B + \cdots + |l\rangle_A |\eta_l^{\perp}\rangle_B \tag{3.3}$$

where $\{|i\rangle_A$ for i=1 to l$\}$ is some orthogonal basis set for Alice and $\{|\eta_1\rangle_B$ for i=1 to l$\}$ are unnormalized and such that $|\eta_i\rangle_B$ is orthogonal to $|\eta_i^{\perp}\rangle_B$ for each i. The next step for the discrimination task is obvious. Alice simply performs a measurement in the above $\{|i\rangle_A$ for i=1 to l$\}$ basis on her subsystem and communicates the obtained outcome i^*. Bob, depending on the communication, performs the trivial task of distinguishing between $|\eta_{i^*}\rangle_B$ and $|\eta_{i^*}^{\perp}\rangle_B$.

3.7 Distinguishability of a set of mutually orthogonal maximally entangled states

Recently, Hayashi and his collaborators established a necessary criterion for a set of mutually orthogonal multipartite states to be perfectly distinguished via LOCC [181]. Consequently, this criterion provides a sufficient condition for the states to be locally indistinguishable.

Theorem 2. *n mutually orthogonal maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$ cannot be perfectly distinguished through LOCC, whenever $n > d$.*

3.8 Local State Marking (LSM)

Definition 1. *[m-LSM] m number of states chosen randomly from a known set of pairwise orthogonal N-party quantum states $\mathscr{S} \equiv \left\{|\psi_j\rangle \mid \langle\psi_i|\psi_j\rangle = \delta_{ij}\right\} \subset \bigotimes_{i=1}^{N} \mathbb{C}_{A_i}^{d_i}$ are distributed among spatially separated parties without revealing the identity of each state. The m-LSM task is to perfectly identify/mark each of the states under the operational paradigm of LOCC.*

In Definition 1, m can take values from 1 to $|\mathscr{S}|$ and accordingly they constitute different discrimination tasks (see Fig.3.3). The task of 1-LSM is more popular as LSD which has been explored in great detail during the last two decades [174–181, 141–156]. The problem of LSD has also been studied with ensembles containing non-orthogonal states [11, 182]. Similarly, Definition 1 can also be generalized for such ensembles. In that case, the quantity of interest will be the difference between the maximum success probabilities of the corresponding marking task under global and local operations, respectively.

We will start the technical part of this article by establishing some generic results.

Lemma 1. *For a set of multipartite states $\mathscr{S}$, perfect $(|\mathscr{S}|-2)$-LSM always implies perfect LSM.*

Proof. Perfect $(|\mathscr{S}|-2)$-LSM of the set $\mathscr{S}$ implies that given arbitrary $(|\mathscr{S}|-2)$ states from the set, they can be marked locally. So we are left with two more states to identify locally. According to the standard result by Walgate *et al.* Theorem 1, any two multipartite pure orthogonal states can be distinguished locally [175], which proves our claim. □

While proof of Lemma 1 follows straightforwardly from the result of Walgate *et al.*, in the next we establish a rather nontrivial thesis.

Theorem 3. *For a set of multipartite states $\mathscr{S}$, perfect LSD (i.e. 1-LSM) always implies perfect LSM (i.e. $|\mathscr{S}|$-LSM).*

Proof. Let the set of states $\mathscr{S}_K \equiv \{|\psi_1\rangle, \cdots, |\psi_K\rangle\} \subset \bigotimes_{i=1}^{N} \mathbb{C}_{A_i}^{d_i} := \mathscr{H}$ be locally distinguishable. The problem of LSM for the set $\mathscr{S}_K$ can be reformulated as an LSD problem of the set of states $\mathscr{S}_{\mathscr{P}[\{K\}]} \equiv \left\{\mathscr{P}\left(\otimes_{i=1}^{K}|\psi_i\rangle\right)\right\} \subset \mathscr{H}^{\otimes K}$, where

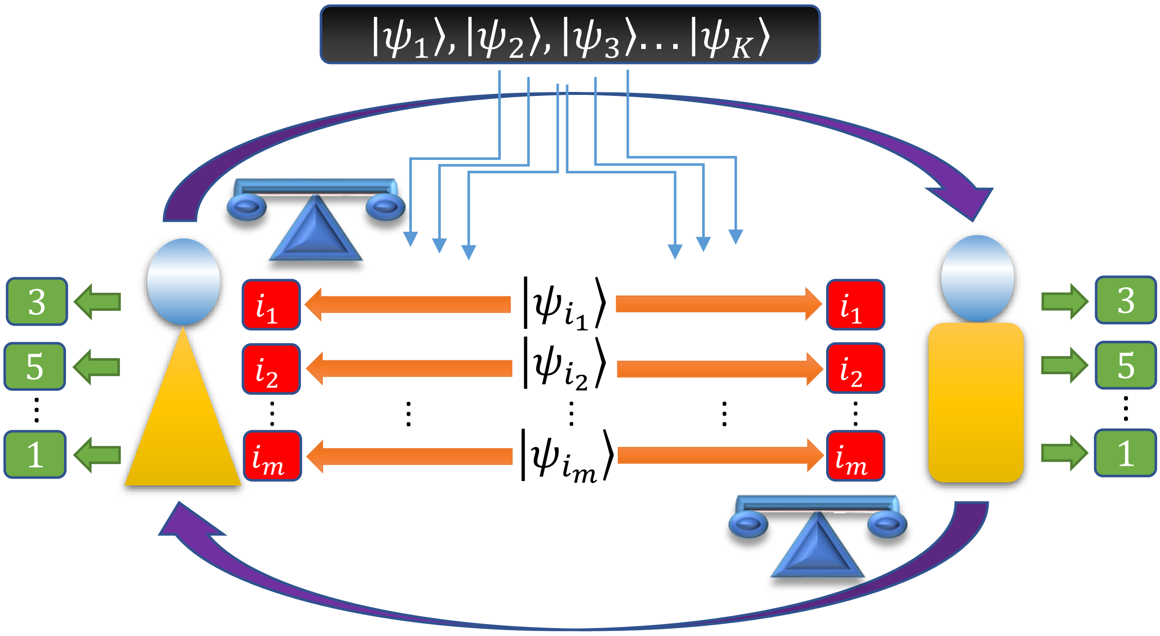

FIG. 3.3 The task of m-LSM is illustrated for the bipartite scenario. m states chosen randomly from a set of K states are distributed between spatially separated Alice and Bob without revealing the identities of the individual states. They have to identify the indices $i_1, \cdots, i_m$ using LOCC. In this particular example, the indices are identified to be $(i_1 = 3, i_2 = 5, \cdots, i_m = 1)$. The special case of $m = 1$ corresponds to the task of LSD.

$\left\{\mathscr{P}\left(\otimes_{i=1}^{K}|\psi_i\rangle\right)\right\}$ denotes the set of tensor product states generated through permutations of the indices $\{1, \cdots, K\}$. For instance, $\mathscr{S}_{\mathscr{P}[\{3\}]} := \left\{\mathscr{P}\left(\otimes_{i=1}^{3}|\psi_i\rangle\right)\right\} \equiv \{|\psi_1\psi_2\psi_3\rangle, |\psi_1\psi_3\psi_2\rangle, |\psi_2\psi_3\psi_1\rangle, |\psi_2\psi_1\psi_3\rangle, |\psi_3\psi_2\psi_1\rangle, |\psi_3\psi_1\psi_2\rangle\}$, where $|x\,y\,z\rangle := |x\rangle \otimes |y\rangle \otimes |z\rangle$. The states in $\mathscr{S}_{\mathscr{P}[\{K\}]}$ can be expressed group-wise as follows,

$$\mathscr{G}_l := |\psi_l\rangle \otimes \mathscr{S}_{\mathscr{P}[\{K\}\setminus l]} \equiv |\psi_l\rangle \otimes \left\{\mathscr{P}\left(\otimes_{i\neq l}|\psi_i\rangle\right)\right\},$$

where $l \in \{1, \cdots, K\}$. Clearly, the groups $\mathscr{G}_l$ make disjoint partitions of the set $\mathscr{S}_{\mathscr{P}[\{K\}]}$, *i.e.*, $\mathscr{S}_{\mathscr{P}[\{K\}]} \equiv \bigcup_{l=1}^{K}\mathscr{G}_l$ s.t. $\mathscr{G}_l \cap \mathscr{G}_{l'} = \emptyset$ whenever $l \neq l'$. Since the states in $\mathscr{S}_K$ is locally distinguishable, by local operations on the first part of the tensor product states in $\mathscr{S}_{\mathscr{P}[\{K\}]}$ we can know with certainty in which of the above groups the given state lies. If the group turns out to be $\mathscr{G}_{l^\star}$ (i.e., if the index l has been identified to be l^*), the given state $|\psi_{l^\star}\rangle \otimes (\cdots)$ evolves to $|\psi'_{l^\star}\rangle \otimes (\cdots)$ due to the LOCC protocol, where the term within the brackets remain unchanged and hence further LOCC protocols can be applied on them. The group of states

$\mathcal{G}_{l^\star} = |\psi'_{l^\star}\rangle \otimes \mathcal{S}_{\mathcal{P}[\{K\}\setminus l^\star]}$ can be further partitioned into disjoint subsets as,

$$\mathcal{G}_{l^\star} \equiv \bigcup \mathcal{G}_{l^\star,m} \text{ s.t. } \mathcal{G}_{l^\star,m} \cap \mathcal{G}_{l^\star,m'} = \emptyset \ \forall \ m \neq m',$$
$$\text{where } \mathcal{G}_{l^\star,m} := |\psi'_{l^\star}\rangle \otimes |\psi_m\rangle \otimes \mathcal{S}_{\mathcal{P}[\{K\}\setminus\{l^\star,m\}]},$$

and $m, m' \in \{1, \cdots, K\} \setminus l^\star$. Since any subset of a locally distinguishable set of states is also locally distinguishable, the identity of the index m can be known perfectly by applying some local protocol on the $|\psi_m\rangle$ part of the given state. As before, the remaining parts of the state will not change. We can continue this process till we completely determine the identity of the state in $\mathcal{S}_{\mathcal{P}[\{K\}]}$ which in turn marks the state in $\mathcal{S}_K$. This completes the proof. □

While Theorem 3 deals with the implications between two extreme cases, particularly establishing 1-LSM $\implies |\mathcal{S}|$-LSM, the following corollaries establish few more nontrivial implications among generic m-LSM tasks.

Corollary 1. *For a set of multipartite states $\mathcal{S}$, perfect m-LSM always implies perfect m'-LSM, where $1 \leq m \leq m'(:= nm) \leq |\mathcal{S}|$ with $n \in \mathbb{N}$.*

Proof. Given a set $\mathcal{S}_K \equiv \{|\psi_1\rangle, \cdots, |\psi_K\rangle\} \subset \bigotimes_{i=1}^N \mathbb{C}_{A_i}^{d_i}$ is m-LSM we are supposed to prove that it is m'-LSM, where $m' = nm$ with $n \in \mathbb{N}$. Intuitively, the proof goes as follows. Let $\mathcal{L}_m$ be the local protocol that successfully completes the m-LSM task for the set $\mathcal{S}_K$. For the m'-LSM task, we divide the set of m' states into n arbitrary disjoint sets each containing m states. Treating each of these n sets independently, we can mark them locally by following the protocol $\mathcal{L}_m$. Thus, by successively applying the protocol $\mathcal{L}_m$ we can construct the local protocol $\mathcal{L}_{m'}$ for the m'-LSM task .

We can also reformulate this as an LSD task as was done in Theorem **1**. We begin by noting that from the set $\mathcal{S}_K \equiv \{|\psi_1\rangle, \cdots, |\psi_K\rangle\} \subset \bigotimes_{i=1}^N \mathbb{C}_{A_i}^{d_i}$ one can choose m states in ${}^K C_m$ different ways. Let denote each such choice of states by the set $\mathcal{S}_m^j$ where $j \in \{1, \cdots, {}^K C_m\}$. Therefore, m-LSM problem of $\mathcal{S}_K$ can be reformulated as the LSD problem of the set of states

$$\mathcal{S}_{{}^K C_m \times m!} \equiv \bigcup_{j=1}^{{}^K C_m} \mathcal{S}^j_{\mathcal{P}[\{m\}]}$$
$$\text{s.t. } \mathcal{S}^j_{\mathcal{P}[\{m\}]} \bigcap \mathcal{S}^{j'}_{\mathcal{P}[\{m\}]} = \emptyset \text{ for } j \neq j',$$

where $\mathscr{S}^j_{\mathscr{P}[\{m\}]}$ is defined similarly as in Theorem 1. We are given that perfect m-LSM of the the set $\mathscr{S}_K$ is possible, *i.e.,* there exists a local protocol $\mathscr{L}_m$ that perfectly distinguishes the states in $\mathscr{S}_{K_{C_m \times m!}}$. While considering the m'-LSM problem, or equivalently, the LSD problem of the set $\mathscr{S}_{K_{C_{m'} \times m'!}}$, the states in $\mathscr{S}^j_{\mathscr{P}[\{m'\}]}$ can be expressed group-wise as $\mathscr{G}^j_{l_1,\ldots,l_m} := |\psi_{l_1},\ldots,\psi_{l_m}\rangle \otimes \mathscr{S}^j_{\mathscr{P}[\{m'\}\setminus\{l_1,\ldots,l_m\}]}$ for each value of j. Thus the groups $\mathscr{G}^j_{l_1,\ldots,l_m}$ make a disjoint partition of the the set $\mathscr{S}_{K_{C_{m'} \times m'!}}$. Since $\mathscr{S}_K$ is m-LSM, by performing local operations on the first m-parts of the tensor product states in $\mathscr{S}_{K_{C_{m'} \times m'!}}$ we can fix the indices $l_1,..,l_m$ of $\mathscr{G}^j_{l_1,\ldots,l_m}$. If $l_1,..,l_m$ is identified to be $l_1^*,..,l_m^*$ then we know with certainty that the given state lies in $\bigcup_j \mathscr{G}^j_{l_1^*,\ldots,l_m^*}$ and the given state is identified to be of the form $|\psi_{l_1^*},\ldots,\psi_{l_m^*}\rangle \otimes (\ldots)$ and evolves to $|\psi'_{l_1^*},\ldots,\psi'_{l_m^*}\rangle \otimes (\ldots)$ after the protocol has been performed, where the terms in the brackets remain unchanged and hence further protocols can be performed on that part. The groups $\mathscr{G}^j_{l_1^*,\ldots,l_m^*} = |\psi'_{l_1^*},\ldots,\psi'_{l_m^*}\rangle \otimes \mathscr{S}^j_{\mathscr{P}[\{m'\}\setminus\{l_1,\ldots,l_m\}]}$ can be further partitioned into disjoint subsets as $\mathscr{G}^j_{l_1^*,\ldots,l_m^*} = \bigcup_{t_1,\cdots,t_m} \mathscr{G}^j_{l_1^*,\ldots,l_m^*,t_1,\ldots,t_m}$ for each value of j, where $\mathscr{G}^j_{l_1^*,\ldots,l_m^*,t_1,\ldots,t_m} \equiv |\psi'_{l_1^*},\ldots,\psi'_{l_m^*}\rangle \otimes |\psi_{t_1},\ldots,\psi_{t_m}\rangle \otimes \mathscr{S}^j_{\mathscr{P}[\{m'\}\setminus\{l_1^*,\ldots,l_m^*,t_1,\ldots,t_m\}]}$. Since $\mathscr{S}_K$ is m-LSM, any subset of $\mathscr{S}_K$ is also m-LSM. Hence we can further fix the indices $t_1,..,t_m$ by performing local operations on the second m-parts of the tensor product states in $\bigcup_j \mathscr{G}^j_{l_1^*,\ldots,l_m^*}$. We continue this process n-times which will completely fix all the $nm = m'$ indices. This will also fix the index j since we have completely distinguished the state. This completes the proof. For the special case of $m = 1$, LSD (i.e., 1-LSM) implies perfect m-LSM with $1 \leq m \leq |\mathscr{S}|$. □

Corollary 2. *For a set of multipartite states $\mathscr{S}$ containing only product states, perfect m-LSM always implies perfect m'-LSM, where $1 \leq m \leq m' \leq |\mathscr{S}|$.*

Proof. It is sufficient to show that m-LSM implies $(m+1)$-LSM for any set $\mathscr{S}$ containing product states only. Given $(m+1)$-states to be marked, we begin by marking the first m-states by using the protocol for m-LSM. However, during this process, the first m-states are destroyed. But since we have determined the identity of the first m-states, we can locally create the original set of first m-states once again. It is to be noted that we can locally create any set of multipartite states whose identity is known if and only if the set contains product states only. We now run the protocol for m-LSM once again but this time on the last m-states. Thus we have identified all the $(m+1)$-states. This completes the proof. Reformulation of this proof in terms of the LSD problem is straightforward and follows similarly to the proof of Corollary 1. □

We note in passing that m-LSM does not trivially imply $(m-1)$-LSM for product states. In the m-LSM task, m states are accessible to the parties in order to mark their identities. However, for $(m-1)$-LSM, the number of accessible states reduces to $(m-1)$ and no trivial inferences can be drawn. Although we were unable to prove for product states, whether m-LSM implies (m-1)-LSM or not, if this really were the case, then the consequences would be very exciting. Using the contrapositive of the statement that m-LSM implies (m-1)-LSM, we would have thus given a protocol for constructing locally indistinguishable states in higher dimensions starting from states like Bennett's UPBs for which perfect LSD is not possible.

3.9 LSM and LSD are inequivalent

Our next result, however, establishes that the converse statement of Theorem 3 does not hold in general and we show this by providing an explicit example wherein given a set of entangled states that are known to be locally indistinguishable, the task of LSM is still possible, and that too with a substantial amount of surplus entanglement shared between the distant parties at the end of the protocol.

Theorem 4. *Perfect LSM of a given set of states $\mathscr{S}$ does not necessarily imply perfect LSD of $\mathscr{S}$.*

Proof. The proof is constructive. We provide a set of pairwise orthogonal states that can be perfectly marked under LOCC but do not allow perfect local distinguishability. To this aim consider the set of states $\mathscr{X}_4 \equiv \{|\chi_i\rangle\}_{i=1}^4 \subset \mathbb{C}_A^4 \otimes \mathbb{C}_B^4$ shared between Alice and Bob, where

$$\begin{aligned}
&|\chi_1\rangle := |\phi^+\rangle_{A_1B_1} \otimes |\phi^+\rangle_{A_2B_2}, \ |\chi_2\rangle := |\phi^-\rangle_{A_1B_1} \otimes |\phi^-\rangle_{A_2B_2}, \\
&|\chi_3\rangle := |\psi^+\rangle_{A_1B_1} \otimes |\phi^-\rangle_{A_2B_2}, \ |\chi_4\rangle := |\psi^-\rangle_{A_1B_1} \otimes |\phi^-\rangle_{A_2B_2}, \\
&\text{with} \ \ |\phi^\pm\rangle := \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \quad |\psi^\pm\rangle := \frac{|01\rangle \pm |10\rangle}{\sqrt{2}},
\end{aligned}$$

and A_1,A_2 subsystems are with Alice while B_1,B_2 are with Bob. The part of $|\chi_i\rangle$ indexed with A_1B_1 we will call the first part and the part with index A_2B_2 will be the second part. For LSM, Alice and Bob are provided the state $|\chi_p\rangle \otimes |\chi_q\rangle \otimes |\chi_r\rangle \otimes |\chi_s\rangle \in \left(\mathbb{C}_A^4 \otimes \mathbb{C}_B^4\right)^{\otimes 4}$, without specifying the indices $p,q,r,s \in \{1,\cdots,4\}$ and p,q,r,s are all distinct. Their collaborative aim is to identify the indices where the collaboration is restricted to LOCC. We shall now discuss the proof.

Now, local indistinguishability of the set $\mathscr{X}_4$ follows from the results of Yu *et al* [183]. There the authors have proved that states in $\mathscr{X}_4$ cannot be distinguished perfectly by any PPT-POVM, a larger class of operations that strictly contains all LOCC operations, as discussed in Section 3.4. Now we show that there exists a local strategy that marks the states exactly.

The set $\mathscr{X}_4$ can be thought of as the union of two disjoint sets of states

$$\mathscr{X}_4 = G_1 \cup G_2 \ \ \& \ \ G_1 \cap G_2 = \emptyset,$$
$$\text{where,} \ \ G_1 := \{|\chi_1\rangle, |\chi_2\rangle\}, \ \ G_2 := \{|\chi_3\rangle, |\chi_4\rangle\}.$$

The LSM task can be considered as identifying the indices $p,q,r,s \in \{1,\cdots,4\}$ in the state $|\Sigma\rangle := |\chi_p\rangle \otimes |\chi_q\rangle \otimes |\chi_r\rangle \otimes |\chi_s\rangle \in \left(\mathbb{C}^4_A \otimes \mathbb{C}^4_B\right)^{\otimes 4}$ locally, where p,q,r,s are distinct. Note that the state $|\Sigma\rangle$ is a composition (tensor product) of four different states and we will call $|\chi_p\rangle$ the first state, $|\chi_q\rangle$ the second state and so on (of course, the indices $p,q,\cdots$ are not known and the aim is to identify them locally). The local marking strategy of Alice and Bob goes as follows:

Step-1 Both Alice and Bob perform the Pauli-Z measurement on the first part of the first state (*i.e.,* the state $|\chi_p\rangle$). If they obtain correlated (C) outcomes, *i.e.,* If Alice and Bob both obtain the same outcome, then they conclude that $|\chi_p\rangle \in G_1$, whereas anti-correlated (AC) outcomes imply $|\chi_p\rangle \in G_2$. Depending on the results obtained in Step-1 they determine their protocol for the next step. For instance, if they obtain correlated outcomes then their protocol is discussed below.

Step-2 Knowing that $|\chi_p\rangle \in G_1$, both Alice and Bob perform Pauli-X measurement on the second part of $|\chi_p\rangle$. Correlated outcomes imply that the first state is $|\chi_1\rangle$ (*i.e.,* $p=1$), else it is $|\chi_2\rangle$ (*i.e.,* $p=2$). Accordingly, two different branches open up at the next step.

Step-3 :[Case-I] $p=1$ in Step-2 implies that the second part of all the states $|\chi_q\rangle, |\chi_r\rangle$ & $|\chi_s\rangle$ is $|\phi^-\rangle$. Using the second part of the second state (*i.e.,* $|\chi_q\rangle$) Alice and Bob follow the teleportation protocol (TP) to prepare the first part of $|\chi_q\rangle$ at Alice's laboratory. Alice now performs the Bell basis measurement (BM) on the first part of $|\chi_q\rangle$ and depending upon the measurement outcome marks the state exactly.

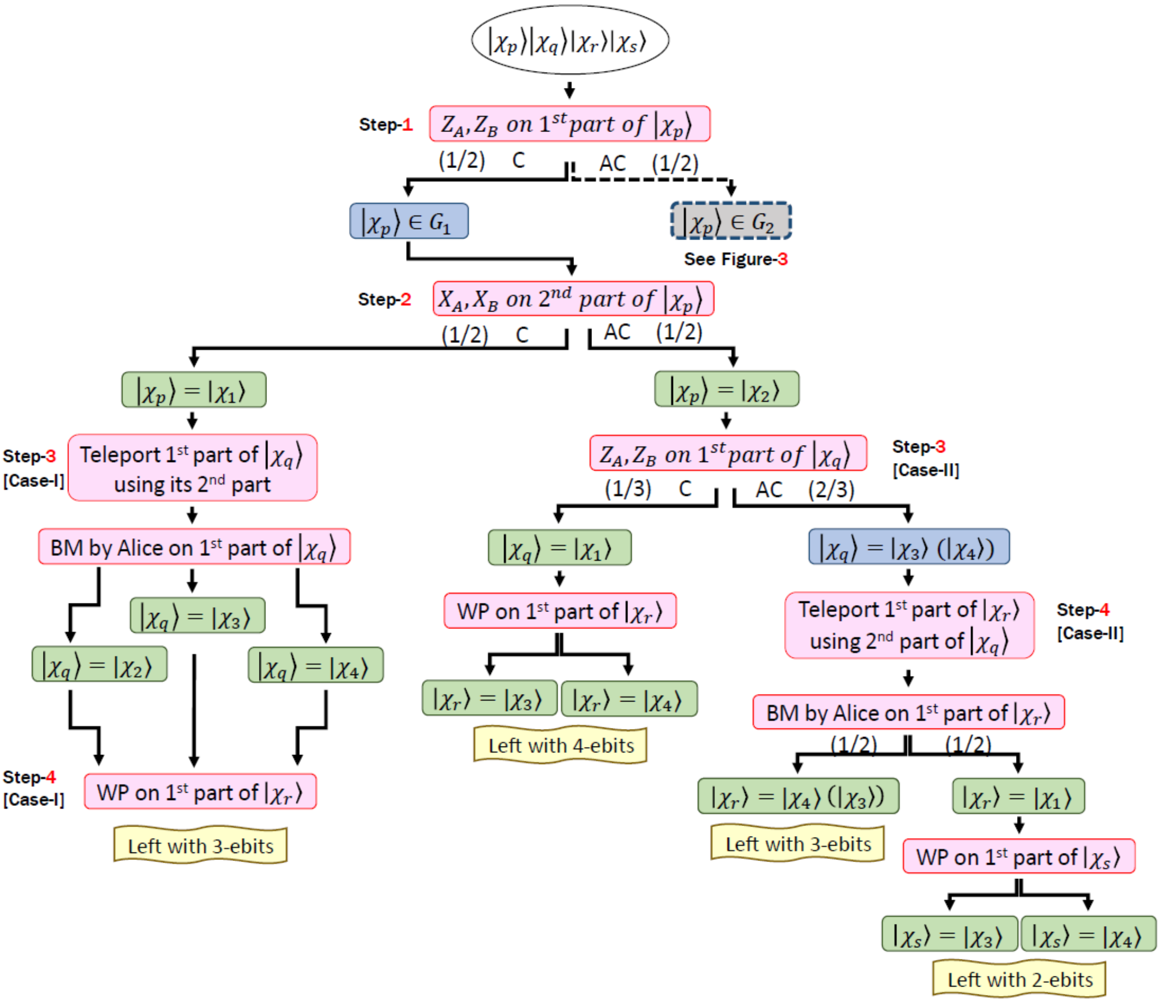

FIG. 3.4 Flow chart of the protocol if correlated outcomes are obtained in Step-1. The number written in each branch indicates the probability of occurrence of that branch. The average amount of entanglement left in this case is $\left[\frac{1}{2}\times 3+\frac{1}{2}\left\{\frac{1}{3}\times 4+\frac{2}{3}\left(\frac{1}{2}\times 3+\frac{1}{2}\times 2\right)\right\}\right]=3$ ebits.

Step-4:[Case-I] Since two states $|\chi_p\rangle$ and $|\chi_q\rangle$ are marked exactly (in this case $p=1$ and $q=2$ *or* 3 *or* 4), the result of Walgate *et al.* (Theorem 1) allows us to mark the state $|\chi_r\rangle$ by a local protocol on the first part of the state (In the flow charts of Figure 3.4 & 3.5 we will call it the Walgate Protocol and denote it as WP). The remaining state $|\chi_s\rangle$ is immediately marked as the set $\mathscr{X}_4$ is known. For the sake of completeness, we list the different possibilities and the corresponding Walgate Protocols:

- $p=1$ (in Step-2) and $q=2$ (in Step-3 [Case- I]): Both Alice and Bob perform the Pauli-X measurement on the first part of $|\chi_r\rangle$. Correlated outcomes imply $r=3$ and $s=4$. Anti-correlated outcomes imply $r=4$ and $s=3$.

- $p=1$ (in Step-2) and $q=3$ (in Step-3 [Case- I]): Both Alice and Bob perform the Pauli-Z measurement on the first part of $|\chi_r\rangle$. Correlated outcomes imply $r=2$ and $s=4$. Anti-correlated outcomes imply $r=4$ and $s=2$.

- $p=1$ (in Step-2) and $q=4$ (in Step-3 [Case- I]): Both Alice and Bob perform the Pauli-Z measurement on the first part of $|\chi_r\rangle$. Correlated outcomes imply $r=2$ and $s=3$. Anti-correlated outcomes imply $r=3$ and $s=2$.

Note that the entanglement of $|\chi_p\rangle$, $|\chi_q\rangle$, and the first part of $|\chi_r\rangle$ gets destroyed in the protocol, whereas the entanglement of $|\chi_s\rangle$ and the second part of $|\chi_r\rangle$ remains intact. So, whatever the outcome of BM at Step-3, the protocol ends with 3-ebit entanglement that can be used as a resource.

Step-3 :[Case-II] Let Step-2 yield the conclusion that $p=2$. Then, both Alice and Bob perform the Pauli-Z measurement on the first part of the second state (*i.e.,* the state $|\chi_q\rangle$).

- If correlated outcomes are obtained then $q=1$.

- If anti-correlated outcomes are obtained then $q=3$ or 4.

Step-4 :[Case-II] If correlated outcome is obtained in Step-3 [Case-II], then we have $p=2$ and $q=1$. Again, the result of Walgate *et al.* ensures that local marking of $|\chi_r\rangle$ is possible by a local protocol on the the first part of the state and accordingly the remaining state $|\chi_s\rangle$ is also marked. This leaves us with 4-ebit of entanglement at the end of the protocol – 1-ebit each in $|\chi_q\rangle$ and $|\chi_r\rangle$, and 2-ebit in $|\chi_s\rangle$.

If an anti-correlated outcome is obtained in Step-3 [Case-II] then Alice and Bob know that the second part of $|\chi_q\rangle$ is $|\phi^-\rangle$. Utilizing this $|\phi^-\rangle$ they teleport and prepare the first part of $|\chi_r\rangle$ at Alice's laboratory. Alice performs the Bell basis measurement (BM) on the first part of $|\chi_r\rangle$ and marks the state exactly.

- If $|\chi_r\rangle$ is identified as $|\chi_4\rangle$ then we have $p=2, q=3, r=4, s=1$. If $|\chi_r\rangle$ is identified as $|\chi_3\rangle$ then we have $p=2, q=4, r=3, s=1$. In both these cases we are left with 3-ebit of entanglement.

- If the state $|\chi_r\rangle$ is identified as $|\chi_1\rangle$, then we have $p=2$ and $r=1$. WP allows us to mark the state $|\chi_s\rangle$ by a local protocol on its first part. Therefore we have either $p=2, q=4, r=1, s=3$ or $p=2, q=3, r=1, s=4$. Both these cases leave us with 2-ebit of entanglement.

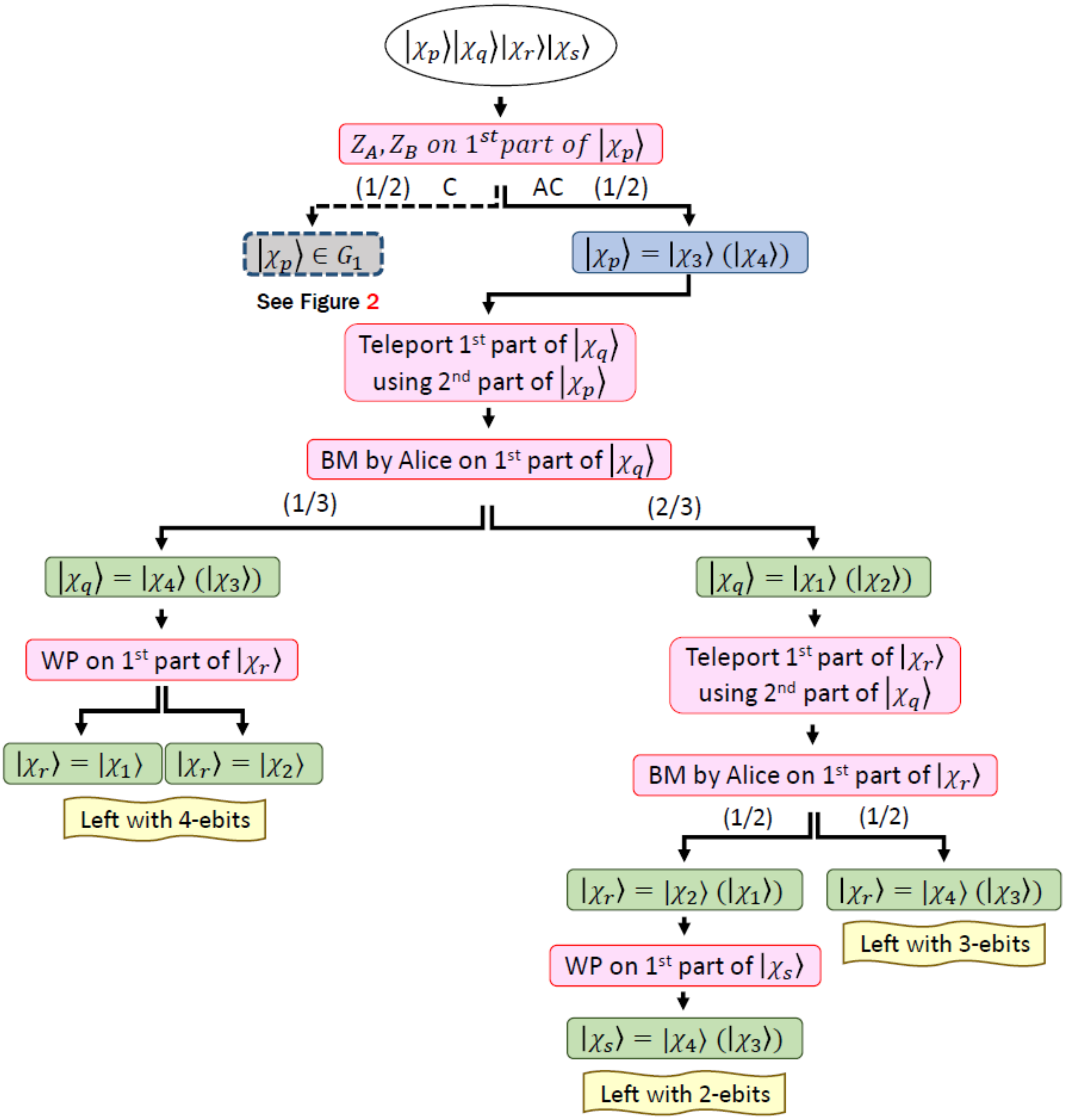

FIG. 3.5 Flow chart of the protocol if anti-correlated outcomes are obtained in Step-1. The average amount of entanglement left in this case is $\left[\frac{1}{3}\times 4+\frac{2}{3}\left\{\frac{1}{2}\times 2+\frac{1}{2}\times 3\right\}\right]=3$ ebits.

So far, we have discussed the protocol if we obtain correlated outcomes in Step-1. The protocol is summarized in the flow chart shown in Figure 3.4. However, to complete the proof we need to analyze the case if anti-correlated outcomes are obtained in Step-1. The corresponding flowchart is shown in Figure 3.5. From the flow charts, it straightforwardly follows that on an average 3-ebit $\left[\frac{1}{2}(3+3)\right]$ of entanglement is left at the end of the protocol.

□

It turns out that at the end of the local marking strategy described in Theorem 4 3-ebit of entanglement (on average) remains between Alice and Bob. However, the optimality of the protocol in terms of retaining entanglement remains an open problem.

3.10 Locally unmarkable set of states

So far we have considered sets that are locally markable. Our next result provides an example of a set of mutually orthogonal states that cannot be marked perfectly under LOCC. This set of states thus exhibits a form of nonlocality that is even stronger than local indistinguishability.

Proposition 1. *The two qubit Bell basis* $\mathscr{B}_4 \equiv \{|b_1\rangle := |\phi^+\rangle, |b_2\rangle := |\phi^-\rangle, |b_3\rangle :=$ $|\psi^+\rangle, |b_4\rangle$
$:= |\psi^-\rangle\} \subset \mathbb{C}^2 \otimes \mathbb{C}^2$ *is locally unmarkable.*

Proof. LSM of $\mathscr{B}_4$ is equivalent to LSD of the set $\mathscr{B}_{\mathscr{P}[\{4\}]}$ that contains 24 pairwise orthogonal maximally entangled states in $\mathbb{C}^{16} \otimes \mathbb{C}^{16}$. Therefore, the desired thesis follows from the fact that n pairwise orthogonal maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$ cannot be perfectly distinguished locally whenever $n > d$, as discussed in Theorem 2. □

Furthermore, in accordance with Lemma 1, the set $\mathscr{B}_4$ does not allow perfect 2-LSM and it also straightforwardly follows that perfect 3-LSM of $\mathscr{B}_4$ is impossible (in fact, for any set $\mathscr{S}$, $(|\mathscr{S}|-1)$-LSM always implies $|\mathscr{S}|$-LSM). A generalization of Proposition 1 follows arguably.

Proposition 2. *Consider any set of maximally entangled states*

$$\mathscr{B}_K(d) := \left\{|b_i\rangle \mid \langle b_i|b_j\rangle = \delta_{ij}\right\}_{i=1}^{K} \subset \mathbb{C}^d \otimes \mathbb{C}^d \tag{3.4}$$

The set is locally unmarkable whenever $K! > d^K$.

3.11 Entanglement assisted marking of states

We now move on to the possibility of entanglement-assisted marking of states that otherwise are locally unmarkable. It might happen that given δ-ebit of entanglement some LSM task can be performed exactly which is otherwise impossible to do locally, and moreover ε-ebit of entanglement is left at the end of the protocol. Such a protocol we will call (δ,ε) entanglement catalytic protocol and $(\delta-\varepsilon)$ quantifies the amount of entanglement consumed to accomplish the given LSM task.

Recall that given 1-ebit of entanglement as an additional resource, the two-qubit Bell basis can be distinguished perfectly. One of the parties teleports his/her part of the unknown Bell state to the other party who then performs the Bell basis measurement to identify the state. Furthermore, it is known that 1-ebit entanglement is the necessary resource required for perfect discrimination of the 2-qubit Bell basis [176]. Coming to the question of entanglement-assisted marking of the set $\mathscr{B}_4$, we obtain the following result.

Proposition 3. *There exists a* $(2,1)$ *entanglement catalytic perfect protocol for LSM of the set* $\mathscr{B}_4$.

Proof. LSM of the set $\mathscr{B}_4$ is equivalent to LSD of the set $\mathscr{B}_{\mathscr{P}[\{4\}]}$ containing states of the form $|b_p\rangle\otimes|b_q\rangle\otimes|b_r\rangle\otimes|b_s\rangle$ with $p,q,r,s\in\{1,\cdots,4\}$ & p,q,r,s are distinct. Let some supplier provide two EPR states for discriminating the set $\mathscr{B}_{\mathscr{P}[\{4\}]}$. Using the teleportation protocol Alice and Bob can know any of the two indices among p,q,r,s. Say they identify the indices p and q. Then the value of r has only two possibilities and the result of Walgate *et al.* ensures that this value can be known exactly under LOCC [175]. While determining the value of r, the entanglement of the state $|b_r\rangle$ gets destroyed. However, at the end of the mentioned protocol, entanglement of the state $|b_s\rangle$ remains intact and its identity is also known. Therefore, 1-ebit of entanglement can be returned back to the supplier. So the protocol consumes 1-ebit of entanglement in catalytic sense. $\square$

Once again we are not sure about optimality of the protocol in Proposition 3 in terms of resource consumption, and leave the question open here for further research. One can obtain a more exotic example of entanglement catalytic local marking phenomenon. To this aim we first prove the following result.

Proposition 4. *Any three Bell states of the two-qubit system is unmarkable under one-way LOCC.*

Proof. Consider a set of maximally entangled states $\{|\phi_k\rangle\}_{k=1}^{n}\subset\mathbb{C}^d\otimes\mathbb{C}^d$ that can be obtained from $|\phi_0(d)\rangle:=\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle$ by applying some unitary on one part of the system, *i.e.,* $|\phi_k\rangle=(U_k\otimes\mathbb{I})|\phi_0(d)\rangle$. According to a criterion, conjectured in [178] and subsequently derived in [184], the states can be discriminated under one-way LOCC *if and only if* there exists a $|\psi\rangle\in\mathbb{C}^d$, such that $\langle\psi_i|\,\psi_j\rangle=\delta_{ij},\forall i,j\in\{1,2,\cdots,n\}$, where $|\psi_k\rangle=U_k|\psi\rangle$. In our case, without loss of any generality we can consider $\mathscr{B}_3 \equiv \{|b_1\rangle := |\phi^+\rangle, |b_2\rangle := |\phi^-\rangle, |b_3\rangle = |\psi^+\rangle\}$, such that $\mathscr{B}_{\mathscr{P}[\{3\}]} \equiv \{|\phi_k\rangle\}_{k=1}^6 \subset \mathbb{C}^8 \otimes \mathbb{C}^8$, where

$$\begin{aligned}
|b_1b_2b_3\rangle &:= |\phi_1\rangle = (U_1 \otimes \mathbb{I}_8)|\phi_0(8)\rangle = ([\mathbb{I}_2 \otimes \sigma_z \otimes \sigma_x] \otimes \mathbb{I}_8)|\phi_0(8)\rangle,\\
|b_1b_3b_2\rangle &:= |\phi_2\rangle = (U_2 \otimes \mathbb{I}_8)|\phi_0(8)\rangle = ([\mathbb{I}_2 \otimes \sigma_x \otimes \sigma_z] \otimes \mathbb{I}_8)|\phi_0(8)\rangle,\\
|b_2b_3b_1\rangle &:= |\phi_3\rangle = (U_3 \otimes \mathbb{I}_8)|\phi_0(8)\rangle = ([\sigma_z \otimes \sigma_x \otimes \mathbb{I}_2] \otimes \mathbb{I}_8)|\phi_0(8)\rangle,\\
|b_2b_1b_3\rangle &:= |\phi_4\rangle = (U_4 \otimes \mathbb{I}_8)|\phi_0(8)\rangle = ([\sigma_z \otimes \mathbb{I}_2 \otimes \sigma_x] \otimes \mathbb{I}_8)|\phi_0(8)\rangle,\\
|b_3b_1b_2\rangle &:= |\phi_5\rangle = (U_5 \otimes \mathbb{I}_8)|\phi_0(8)\rangle = ([\sigma_x \otimes \mathbb{I}_2 \otimes \sigma_z] \otimes \mathbb{I}_8)|\phi_0(8)\rangle,\\
|b_3b_2b_1\rangle &:= |\phi_6\rangle = (U_6 \otimes \mathbb{I}_8)|\phi_0(8)\rangle = ([\sigma_x \otimes \sigma_z \otimes \mathbb{I}_2] \otimes \mathbb{I}_8)|\phi_0(8)\rangle.
\end{aligned}$$

Here $|\phi_0(8)\rangle := |\phi^+\rangle^{\otimes 3} \in \mathbb{C}^8 \otimes \mathbb{C}^8$. Now, consider an arbitrary quantum state $|\chi\rangle := \sum_{i=0}^7 a_i |i\rangle \in \mathbb{C}^8$, where $a_i \in \mathbb{C}$ & $\sum_{i=0}^7 |a_i|^2 = 1$. Thus the condition for distinguishability of the set $\mathscr{B}_{\mathscr{P}[\{3\}]}$ under one-way LOCC turns out to be $\langle\psi_i|\psi_j\rangle = \delta_{ij}$, where $|\psi_k\rangle := U_k|\chi\rangle$. It boils down to a numerical exercise to show that the aforesaid condition is not satisfied for any $|\chi\rangle \in \mathbb{C}^8$. □

While Proposition 4 proves impossibility of LSM of the set $\mathscr{B}_3$ under one-way LOCC, we have the following stronger result if we consider 2-LSM of the set.

Corollary 3. *Perfect 2-LSM of the set $\mathscr{B}_3$ is not possible even under two-way LOCC protocol.*

The proof follows from the fact that 6 pairwise maximally entangled states in $(\mathbb{C}^4)^{\otimes 2}$ are not locally distinguishable (using Theorem 2). Moving on to the question of entanglement-assisted discrimination of the set $\mathscr{B}_3$, it has been established that perfect discrimination requires 1-ebit entanglement [185]. Regarding entanglement-assisted marking of $\mathscr{B}_3$ we have the following result.

Proposition 5. *There exists a $(1,1)$ entanglement catalytic protocol for perfect LSM of the set $\mathscr{B}_3$.*

Proof. Let Alice and Bob have 1-ebit entanglement (received from some supplier) to distinguish the state $|b_p\rangle \otimes |b_q\rangle \otimes |b_r\rangle$, where $p,q,r \in \{1,2,3\}$ & p,q,r are distinct. Using the teleportation scheme they can identify one of the indices (say) p. Then, using the method of Walgate *et al.* [175], they identify the remaining two indices. At the end of this protocol 1-ebit entanglement remains with Alice and Bob which they can return to the supplier. So, in a catalytic sense, the protocol consumes 0-ebit of entanglement. □

Note that the protocol in Proposition 5 involves two-way CC. If the teleportation step is from Alice to Bob and thus requires CC from Alice to Bob, then the

Walgate step requires CC from Bob to Alice. The question remains open whether there exists some local protocol with two-way CC that perfectly marks the set $\mathscr{B}_3$ without involving entanglement even in the catalytic sense.

3.12 An information theoretic task

To further highlight the implication of the results from the previous section, a few comments are in order. Although both the problems of LSM and LSD stem from a common notion of state identification, the present work strives to point out a subtle difference between them. To elaborate on this difference one can consider the following three-party information-theoretic task.

Let us suppose three parties Alice, Bob and Charlie are spatially separated. Charlie shares quantum transmission lines with both Alice and Bob, but Alice and Bob are restricted to classical communication between themselves only. Charlie would like to communicate a classical message to both Alice and Bob. But to do that he is provided with an ensemble of n orthogonal bi-partite states of local dimension d which are not locally distinguishable. A justification for communicating in this way is to avoid the message being decoded by non-communicating eavesdroppers between Charlie-Alice and Charlie-Bob.

Now Charlie can provide Alice and Bob multiple copies of the unknown state from the ensemble, so that they can perform perfect LSD. Let us suppose k copies are necessary for perfect LSD. Thus Charlie could communicate to Alice and Bob $\log\, n$ bits by sending k qudits, i.e. $\frac{\log\, n}{k}$ bits per qudit.

Alternatively Charlie can provide Alice and Bob states from the ensemble corresponding to LSM task, i.e. an ensemble of size $\log\, n!$. The possibility of perfect LSM of this ensemble under LOCC will result in a communication of $\log\, n!$ bits by sending n qudits, i.e. $\frac{\log\, n!}{n}$ bits per qudit.

To compare the average communication per qudit, let us consider the ensemble in Theorem 4. The ensemble $\mathscr{X}_4$ of 4 orthogonal states with local dimension 4 is given to Charlie. This ensemble does not allow perfect LSD (according to Theorem 4) but 2 copies of the unknown state is sufficient for perfect LSD. So the average communication per ququad is $\frac{\log\, 4}{2} = 1$ bit. On the other hand, perfect LSM of this ensemble (as in Theorem 2) implies average communication per ququad to be $\frac{\log\, 4!}{4} = \frac{\log\, 24}{4} = \frac{3+\log\, 3}{4}$ bits which is greater than the average communication for the protocol based on multi-copy LSD. In this sense, LSM is more economical than the conventional multi-copy LSD.

3.13 Concluding Remarks

In summary, we have proposed a class of novel discrimination tasks, namely the m-LSM task, that goes beyond the much-explored task of local state discrimination. The present study unravels several curious and intricate features of the proposed task. For example, Proposition 4 is interesting from a different perspective. It is known that any set of $d+1$ mutually orthogonal $d\otimes d$ maximally entangled states is locally indistinguishable [181]. But the answer to the same question for smaller sets $(< d+1)$ is known only in a few cases [186]. Although the result of Walgate *et al.* ensures local distinguishability of any two maximally entangled states in $2\otimes 2$ and later Nathanson proved that any three mutually orthogonal $3\otimes 3$ maximally entangled states are locally distinguishable [187], the authors in [178, 183, 188] provide examples of 4 maximally entangled states in $4\otimes 4$ that are not local distinguishable. In Ref.[184] one can find an example of 4 maximally entangled states in $5\otimes 5$ as well as an example of 5 maximally entangled states in $6\otimes 6$ that cannot be perfectly distinguished under one-way LOCC. In a similar spirit, the set $\mathscr{B}_{\mathscr{P}[\{3\}]}$ constitutes an example of 6 maximally entangled states in $8\otimes 8$ that cannot be distinguished under one-way LOCC.

Lemma 1, Corollary 1-2, and Theorem 3-4 unveil some general features of local state marking task and Proposition 1-5 report some interesting consequences by considering specific set of states.

Chapter 4

Local Quantum Theory: Different Composition Models

4.1 The fourth Postulate of Quantum mechanics

The tensor product postulate of quantum mechanics also cited as the 'zeroth' axiom in literature [189], describes the Hilbert space of the joint system to be the tensor product of each of the subsystem's Hilbert spaces [190–192]. A recent study, however, logically derives this postulate from the state postulate and the measurement postulate rather than taking it as an independent one [120]. Nevertheless, within this tensor product structure, the unentangled Gleason's theorem assigns state spaces for the composite systems that include density operators (the quantum states) as a proper subset [42–44]. In fact, assuming individual systems' description to be quantum, several mathematical models are possible for the composite state and effect spaces that yield consistent outcome probability. Exploring these broader class of theories helps us to compare and contrast the information processing capabilities of quantum theory with other theories and gain new insights about the origin of such capabilities.

The framework of generalized probability theory (GPT) [27–31, 37] is well-suited to study these different composite models. We have discussed this extensively in Chapter 2, Section 2.3. Physical constraints, such as no-signaling and local tomography, limit the composite state spaces to be constrained within two extremes [38–41]– the minimal tensor product composition containing only separable states and the maximal tensor product composition containing beyond quantum states that are positive on product tests (POPT) and compatible with unentangled Gleason's theorem. The corresponding effect spaces are specified in accordance with the 'no-restriction' hypothesis [45] that includes all the mathematicall consistent effects in the theory.

A natural question is whether these different composite models can lead to stronger than quantum correlations that will in turn make them distinct from quantum state space and put an embargo on their physical existence. In this work, we ask and answer how the information processing capabilites of composite systems change when one uses different mathematical structures to describe composition. For the bipartite case a negative response comes through the work of Barnum *et al.* [47] which states that no such composition can produce any beyond quantum spacelike correlations in Bell type experimental scenario. While maximal composition involving more than two subsystems can yield stronger than quantum correlation in typical Bell scenario as shown by Acín *et al.* [193], recently in Ref. [194] it has been shown that even in bipartite case stronger than quantum correlations are possible if the typical classical input-classical output Bell scenario is generalized to quantum input-classical output semi-quantum scenario [195]. Although this quantum input scenario disallows all the compositions having beyond entangled states it requires trustworthy verifiers in producing some predetermined unentangled quantum inputs [194].

In a completely different approach, one of our recent works [196] demonstrated that bipartite minimal composition can yield correlations stronger than those allowed by quantum theory in a timelike scenario. Specifically, we showed that a communication game played between two timelike-separated players—a sender and a receiver in the sender's causal future—cannot be won perfectly using two elementary quantum systems (qubits) if the standard quantum composite state space is assumed. However, if the composition is instead taken to be the minimal one, the game becomes perfectly winnable. While minimal composition, which consists only of separable states, does not produce nonlocal correlations in a Bell-like scenario, the presence of beyond-quantum effects in this framework leads to beyond-quantum correlations in a timelike setting. This result may suggest that such effects are necessary to obtain beyond-quantum timelike correlations. However, in this chapter—based on our work [77]—we show that this intuition is, in fact, incorrect.

We organize the chapter as follows: in Section 4.2, we discuss the various notions of dimension in a theory. Then in Section 4.3, we briefly discuss the results of Barnum *et al.* and Acín *et al.* [47, 193] for the bipartite case. In Section 4.4, we show that maximal composition that allows only product effects but permits beyond quantum states can also yield beyond quantum correlations in timelike scenarios. Thus, while Barnum *et al.* result [47] shows that spacelike correlations are no good for establishing the beyond quantum nature of the bipartite maximal composition, our result establishes that timelike correlations do serve the purpose here. In Section 4.5, we discuss the underlying cause for the difference in the communication utilities of the two theories. We proceed to prove a no-go that although the maximal composition allows beyond quantum timelike correlations, the classical information carrying capacity of such models cannot be more than the corresponding quantum composite systems. In fact, we prove a generic result regarding the information capacity of composite systems in the GPT framework. Then in Section 4.6, we show that this gap can be increased further by considering more number of elementary systems. Finally in Section 4.7, we conclude this chapter.

4.2 Operational notions of dimension

The dimension of the vector space V in which the set Ω_S is embedded is a well-defined concept, but it does not carry any operational signature. However, the operationally motivated notion of dimension can be defined through the concept of state distinguishability. For the purpose of our work, in the following, we recall a few relevant definitions [197].

Definition 2 (Perfect distinguishability)**.** *Two states $\omega_1, \omega_2 \in \Omega_S$ are perfectly distinguishable whenever there exists some measurement $\mathscr{M} = \{e_1, e_2 \in \mathscr{E}_S \mid e_1 + e_2 = u\}$ such that $e_i(\omega_j) = \delta_{ij}$.*

For instance, two quantum states $|\psi\rangle, |\phi\rangle \in \mathbb{C}^d$ are perfectly distinguishable if and only if they are orthogonal, a fact which follows from the seminal no-cloning theorem [6]. On the other hand, in discrete classical probability theory the state spaces are simplices and any two extreme points are perfectly distinguishable [198].

Definition 3 (Operational Dimension)**.** *Operational dimension $\mathbb{O}(S)$ of a system S is the maximum cardinality of the set of states $\Omega_n := \{\omega_1, \cdots, \omega_n\} \subset \Omega_S$ such that all the states in Ω_n are perfectly distinguishable in a single measurement.*

For instance $\mathbb{O}(\mathbb{C}^d) = d$ although the the dimension of the vector space in which $\mathscr{D}(\mathbb{C}^d)$ is embedded is $d^2 - 1$. Operational dimension of a system quantifies its classical information carrying capacity [27, 199] (see also [200, 201]), *i.e.* sending a system with operational dimension $\mathbb{O}(S)$ through a noiseless channel a sender can sends $\log_2 \mathbb{O}(S)$-bits of classical information to a receiver.

Definition 4 (Information Dimension)**.** *The information dimension $\mathbb{I}(S)$ of a system S is the maximum cardinality of the set of states $\Omega_n := \{\omega_1, \cdots, \omega_n\} \subset \Omega_S$ such that all the states in Ω_n are pairwise perfectly distinguishable.*

Note that while defining $\mathbb{O}(S)$ a single measurement is allowed to distinguish the states in the set Ω_n. On the other hand, $\mathbb{I}(S)$ deals with the pairwise distinguishability and for different pairs of states $\{\omega_i, \omega_j\}$ in Ω_n, different measurements $\mathscr{M}_{ij}$ can be performed to distinguish the pairs. Therefore, it clearly follows that $\mathbb{I}(\star) \geq \mathbb{O}(\star)$ for an arbitrary GPT system, and accordingly one can define a quantity called dimension mismatch, $\Delta(\star) := \mathbb{I}(\star) - \mathbb{O}(\star)$. For classical and quantum systems it follows from simple arguments that both theses dimensions are equal. However, as shown in [197], for the hypothetical toy model of Box world ($\square$) the information dimension is strictly greater than the operational dimension. While $\mathbb{I}(\square) = 4$, one has that $\mathbb{O}(\square) = 2$.

4.3 POPT states and Bell correlations

As already mentioned, the state space of maximal composition strictly contains the quantum state space, *i.e.*, $\mathscr{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}) \subset \Omega_{\overline{\mathrm{SEP}}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$. In particular, an entanglement witness operator $W \notin \mathscr{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$, whereas $W \in \Omega_{\overline{\mathrm{SEP}}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$. Although the state space of $\overline{\mathrm{SEP}}$ theory is bigger than the quantum state space, the 'nonlocal strength' of the bipartite system $S^{AB}_{\overline{\mathrm{SEP}}}$ is no more than S^{AB}_{Q}. This follows from a generic result by Barnum *et al.* [47], where it is proved that any no-signaling bipartite input-output probability distribution $P(ab|xy)$ obtained from $S^{AB}_{\overline{\mathrm{SEP}}}$ can also be obtained from S^{AB}_{Q}; here a and b denote Alice's and Bob's output corresponding to their respective inputs x and y. For a state $W \in \Omega_{\overline{\mathrm{SEP}}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$ the correlation $P(ab|xy)$ is obtained as

$$
\begin{gathered}
P(ab|xy) = \mathrm{Tr}[W(\pi^a_x \otimes \pi^b_y)], \\
\pi^a_x \in \mathscr{P}(\mathbb{C}^{d_A}),\ \sum_a \pi^a_x = \mathbf{1}_{d_A}\ \&\ \pi^b_y \in \mathscr{P}(\mathbb{C}^{d_B}),\ \sum_b \pi^b_y = \mathbf{1}_{d_B}.
\end{gathered}
$$

As pointed out in [193], the result of Barnum *et al.* can be seen as follows. According to Choi–Jamiołkowski (CJ) isomorphism [202, 203], any $W \in \Omega_{\overline{\mathrm{SEP}}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B}) \setminus \mathscr{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ can be written as $[\mathscr{I} \otimes \Lambda](\phi^+)$, where Λ is a positive map, $\mathscr{I}$ is the identity map, and ϕ^+ is the projector on maximally entangled state. Furthermore, any such witness can also be written as $[\mathscr{I} \otimes \Lambda_{tp}](\psi)$, where Λ_{tp} is positive and trace-preserving and ψ is a projector onto a pure bipartite state [204]. Therefore, we have

$$\begin{aligned} P(ab|xy) &= \mathrm{Tr}[W(\pi_x^a \otimes \pi_y^b)] = \mathrm{Tr}[[\mathscr{I} \otimes \Lambda_{tp}](\psi)(\pi_x^a \otimes \pi_y^b)] \\ &= \mathrm{Tr}[\psi(\pi_x^a \otimes \Lambda_{tp}^\star[\pi_y^b])] = \mathrm{Tr}[\psi(\pi_x^a \otimes \tilde{\pi}_y^b)]. \end{aligned}$$

Here $\Lambda^\star$ is the adjoint map of Λ, and since the adjoint of a positive trace-preserving map is positive and unital, $\{\tilde{\pi}_y^b := \Lambda_{tp}^\star[\pi_y^b]\}_b$ forms a valid quantum measurement.

4.4 Revelation of beyond quantum correlation

We will now proceed to show that the system $S_{\overline{\mathrm{SEP}}}^{AB}$ can yield stronger than quantum correlation in the timelike domain. At this point, we would like to mention that the study of stronger than timelike correlation has been introduced in a recent paper by Dall'Arno *et al.* where the authors have proposed an interesting principle called No-Hypersignaling [35]. However, we will follow a bit different approach as studied in [196] and recall below a communication game introduced there.

4.4.1 Pairwise distinguishability game $\mathscr{P}_D^{[n]}$

The game involves two players (Alice and Bob) and a Referee. In each run of the game, the Referee provides a classical message η to Alice, randomly chosen from some set of messages $\mathscr{N}$, where $|\mathscr{N}| := n$. In the same run Bob is asked a question $\mathbb{Q}(\eta, \eta')$ – whether the message given to Alice is η or η', where $\eta' \neq \eta$. The winning condition demands Bob answer all questions correctly. Alice can help Bob by sending some information about the message she received. It is not hard to see that perfect winning demands Alice to encode the message on the states of some physical system that are pairwise distinguishable. With this game, we are now in a position to prove one of our main results.

4.4.2 Bipartite $\overline{\mathbf{SEP}}$ composition vs Quantum

Theorem 5. *The game $\mathscr{P}_D^{[8]}$ cannot be won if Alice uses the system $[\mathbb{C}^2, \mathbb{C}^2, \otimes_Q]$ to encode her message whereas $[\mathbb{C}^2, \mathbb{C}^2, \otimes_{\overline{SEP}}]$ system yields a perfect winning strategy.*

	Φ^+ / $\overline{\Phi^+}$	Φ^- / $\overline{\Phi^-}$	Ψ^+ / $\overline{\Psi^+}$	Ψ^- / $\overline{\Psi^-}$
Φ^+ / $\overline{\Phi^+}$	**NA**	$A^y \otimes A^y$	$\mathbf{1} \otimes \mathbf{1}$	$\mathbf{1} \otimes \mathbf{1}$
Φ^- / $\overline{\Phi^-}$	$A^y \otimes A^y$	**NA**	$\mathbf{1} \otimes \mathbf{1}$	$\mathbf{1} \otimes \mathbf{1}$
Ψ^+ / $\overline{\Psi^+}$	$\mathbf{1} \otimes \mathbf{1}$	$\mathbf{1} \otimes \mathbf{1}$	**NA**	$A^y \otimes A^y$
Ψ^- / $\overline{\Psi^-}$	$\mathbf{1} \otimes \mathbf{1}$	$\mathbf{1} \otimes \mathbf{1}$	$A^y \otimes A^y$	**NA**
$\overline{\Phi^+}$	$A^x \otimes A^x$	$A^y \otimes A^y$	$\mathbf{1} \otimes \mathbf{1}$	$\mathbf{1} \otimes \mathbf{1}$
$\overline{\Phi^-}$	$A^y \otimes A^y$	$A^x \otimes A^x$	$\mathbf{1} \otimes \mathbf{1}$	$\mathbf{1} \otimes \mathbf{1}$
$\overline{\Psi^+}$	$\mathbf{1} \otimes \mathbf{1}$	$\mathbf{1} \otimes \mathbf{1}$	$A^x \otimes A^x$	$A^y \otimes A^y$
$\overline{\Psi^-}$	$\mathbf{1} \otimes \mathbf{1}$	$\mathbf{1} \otimes \mathbf{1}$	$A^y \otimes A^y$	$A^x \otimes A^x$

FIG. 4.1 The unitaries required to construct the measurement $\mathscr{M}[U \otimes V]$ for pairwise distinguishability of the states in \$[8] are given. The states in the horizontal upper (lower) diagonal can be distinguished from the states in the vertical upper (lower) diagonal using the corresponding unitaries. For instance, the measurement to distinguish the pair $\{\Psi^+, \Psi^-\}$ as well as the pair $\{\overline{\Psi^+}, \overline{\Psi^-}\}$ is given by the entry in the third row and fourth column, *i.e.*, $\mathscr{M}[A^y \otimes A^y]$, whereas the pair $\{\overline{\Psi^+}, \Psi^+\}$ is distinguished by the measurement given in seventh row, third column, *i.e.*, $\mathscr{M}[A^x \otimes A^x]$. **NA** means that a state cannot be distinguished from itself.

Proof. Perfect winning of the game $\mathscr{P}_D^{[n]}$ requires Alice to communicate to Bob a physical system which has information dimension at least n. For the two-qubit system $[\mathbb{C}^2,\mathbb{C}^2,\bigotimes_Q]$, the information dimension is the same as its operational dimension which is 4, and therefore, $\mathscr{P}_D^{[8]}$ game cannot be won perfectly by communicating two qubits.

We now provide an explicit strategy to win the game $\mathscr{P}_D^{[8]}$ using the system $[\mathbb{C}^2,\mathbb{C}^2,\bigotimes_{\overline{\mathrm{SEP}}}]$. Let Alice use the set $\$[8] \equiv \left\{\Phi^{\pm},\Psi^{\pm},\overline{\Phi^{\pm}},\overline{\Psi^{\pm}}\right\} \subset \Omega_{\overline{\mathrm{SEP}}}(\mathbb{C}^2,\mathbb{C}^2)$ of eight different states to encode her messages; where $\chi := |\chi\rangle\langle\chi|$, $|\Phi^{\pm}\rangle := (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\Psi^{\pm}\rangle := (|01\rangle \pm |10\rangle)/\sqrt{2}$, and $\overline{\chi} := \mathscr{I}\otimes \mathrm{T}(\chi)$ with $\mathscr{I}$ denoting the identity map and T denoting the transposition map (in the computational basis). It remains to be shown that the states in $\$[8]$ are pairwise distinguishable with measurements constituted by the effects from the set $\mathscr{E}_{\overline{\mathrm{SEP}}}(\mathbb{C}^2,\mathbb{C}^2)$.

Consider the pair of states Φ^+ and Ψ^+, and the measurement

$$\mathscr{M} \equiv \begin{cases} E_{even} := |0\rangle\langle 0|\otimes|0\rangle\langle 0| + |1\rangle\langle 1|\otimes|1\rangle\langle 1|, \\ E_{odd} = \mathbf{1} - E_{even} := |0\rangle\langle 0|\otimes|1\rangle\langle 1| \\ \qquad\qquad\qquad + |1\rangle\langle 1|\otimes|0\rangle\langle 0|. \end{cases}$$

Clearly, $\mathscr{M}$ is a valid measurement on the system $[\mathbb{C}^2,\mathbb{C}^2,\bigotimes_{\overline{\mathrm{SEP}}}]$ as $E_{odd},E_{even} \in \mathscr{E}_{\overline{\mathrm{SEP}}}(\mathbb{C}^2,\mathbb{C}^2)$, where E_{even} is the projector of even number of up spin and E_{odd} is the projector of odd number of up spin. A straightforward calculation yields

$$\mathrm{Tr}(\Phi^+ E_{odd}) = 1, \quad \mathrm{Tr}(\Phi^+ E_{even}) = 0;$$
$$\mathrm{Tr}(\Psi^+ E_{odd}) = 0, \quad \mathrm{Tr}(\Psi^+ E_{even}) = 1.$$

Therefore, the measurement $\mathscr{M}$ perfectly distinguishes the states Φ^+ and Ψ^+. To show the same for any pair of states in $\$[8]$, let us denote as $\mathscr{M}[U\otimes V]$ the measurement obtained from $\mathscr{M}$ through the unitary rotation $U\otimes V$, *i.e.* $\mathscr{M}[U\otimes V] := \{U\otimes V E_{odd} U^{\dagger}\otimes V\dagger, U\otimes V E_{even} U^{\dagger}\otimes V\dagger\}$. As shown in Table 4.1, choosing U and V appropriately from the set $\left\{\mathbf{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}, A^x := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1\end{pmatrix}, A^y := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1\end{pmatrix}\right\}$ any pair of states in $\$[8]$ can be distinguished perfectly by the measurement $\mathscr{M}[U\otimes V]$. This completes the proof. $\square$

4.5 Dimension mismatch in $\overline{\text{SEP}}$ composition

Theorem 5 thus establishes that $\overline{\text{SEP}}$ composition of two elementary qubits can result in a correlation that can't be achieved with two qubits quantum composition. As an immediate corollary, we have a lower bound on the information dimension of the system $[\mathbb{C}^2, \mathbb{C}^2, \otimes_{\overline{\text{SEP}}}]$.

Corollary 4. *The information dimension of the system* $[\mathbb{C}^2, \mathbb{C}^2, \otimes_{\overline{SEP}}]$ *is at least* 8*, i.e.* $\mathbb{I}[\mathbb{C}^2, \mathbb{C}^2, \otimes_{\overline{SEP}}] \geq 8$.

At present we do not know whether the above bound is tight and leave this question open for future research. Rather, we proceed to find the operational dimension of the systems obtained through the $\overline{\text{SEP}}$ composition. To this aim, we first prove the following proposition.

Proposition 6. *Every POPT state* $W_{AB} \in \Omega_{\overline{SEP}}(\mathbb{C}^{d_A}, \mathbb{C}^{d_B})$ *can be written as* $(\mathscr{I}_A \otimes \Lambda_{R\to B})(\rho_{AR})$ *where* Λ *is a positive, unital map and* $\rho_{AR} \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_R}$ *is a pure quantum state independent of* W_{AB}.

Proof. We start by defining the following:[1]

$$\begin{aligned} W'_{AB} &:= W_{AB} + \mathbf{1}_A \otimes P_B^{\perp}; \quad P_B^{\perp} := \mathbf{1}_B - P_B; \\ P_B &:= \text{Projector onto the support of } W_B; \\ W_B &:= \mathrm{Tr}_A\left(W_{AB}\right); \;\; W'_B := \mathrm{Tr}_A\left(W'_{AB}\right). \end{aligned}$$

W'_{AB} is a POPT state (unnormalized) as for any separable effect $\pi_A \otimes \pi_B$ we have, $\mathrm{Tr}\left[(W'_{AB})(\pi_A \otimes \pi_B)\right] = \mathrm{Tr}\left[(W_{AB})(\pi_A \otimes \pi_B)\right] + \mathrm{Tr}\left(\pi_A\right)\mathrm{Tr}\left(P_B^{\perp}\pi_B\right) \geq 0$. Thus, W'_B is a full rank positive operator, and hence we can define:

$$W''_{AB} := \left[\mathbf{1}_A \otimes \left(W'_B\right)^{-1/2}\right] W'_{AB} \left[\mathbf{1}_A \otimes \left(W'_B\right)^{-1/2}\right],$$

$(W'_B)^{-1/2}$, being a positive operator, implies that W''_{AB} is a POPT: $\mathrm{Tr}\left[(W''_{AB})(\pi_A \otimes \pi_B)\right] = \mathrm{Tr}\left[W'_{AB}\left(\pi_A \otimes (W'_B)^{-1/2}\pi_B\,(W'_B)^{-1/2}\right)\right] \geq 0$.

Further, $\mathrm{Tr}_A\left(W''_{AB}\right) = \sum_i (W'_B)^{-1/2}\,\langle i|_A\, W'_{AB}\, |i\rangle_A\,(W'_B)^{-1/2} = (W'_B)^{-1/2}\, W'_B\,(W'_B)^{-1/2} = \mathbf{1}_B$.

Using CJ isomorphism we can write $W''_{AB} = \mathscr{I}_A \otimes \mathscr{U}_{S\to B}(|\chi^+\rangle_{AS}\langle\chi^+|)$, where $|\chi^+\rangle_{AB} := \sum_i |i\rangle_A\,|i\rangle_B$ is the unnormalized maximally entangled state and $\mathscr{U}_{S\to B}$

[1]The techniques used in the proof are motivated from [204].

is a positive map. More explicitly, the action of $\mathscr{U}_{S\to B}$ is given by, $\mathscr{U}_{S\to B}(M_S) = \mathrm{Tr}_S\left[(M_S^T \otimes \mathbf{1}_B)(W''_{SB})\right]$. $\mathscr{U}_{S\to B}$ is unital, since $\mathscr{U}_{S\to B}(\mathbf{1}_S) = \mathrm{Tr}_S(W''_{SB}) = \mathbf{1}_B$. Furthermore, it is easy to check that $W_{AB} = (\mathbf{1}_A \otimes V_B^\dagger) W''_{AB} (\mathbf{1}_A \otimes V_B)$, where $V_B := (W'_B)^{1/2} P_B$.

Let us now define a new completely positive, unital map

$$\mathscr{Y}_{BC\to B}(M_{BC}) := V_B^\dagger \langle 0|_C M |0\rangle_C V_B + V_B^{'\dagger} \langle 1|_C M |1\rangle_C V_B' \, ,$$

where V_B' is chosed so that it satisfies the condition $V_B^\dagger V_B + V_B^{'\dagger} V_B' = \mathbf{1}_B$ and $\mathscr{H}_C := \mathbb{C}^2$. The above map is the adjoint of the completely positive, trace-preserving map having the Kraus operators $\{V_B \otimes |0\rangle_C, V_B' \otimes |1\rangle_C\}$; and it has the property,

$$\begin{aligned} &\mathscr{I}_A \otimes \mathscr{Y}_{BC\to B}(M_{AB} \otimes |0\rangle_C \langle 0|) \\ &\qquad\qquad = (\mathbf{1}_A \otimes V_B^\dagger) M_{AB} (\mathbf{1}_A \otimes V_B). \end{aligned}$$

This further leads us to,

$$\begin{aligned} W_{AB} &= \left(\mathbf{1}_A \otimes V_B^\dagger\right) W''_{AB} \left(\mathbf{1}_A \otimes V_B\right) \\ &= \mathscr{I}_A \otimes \mathscr{Y}_{BC\to B}\left(W''_{AB} \otimes |0\rangle_C \langle 0|\right) \\ &= \mathscr{I}_A \otimes \mathscr{Y}_{BC\to B}\left[\left(\mathscr{I}_A \otimes \mathscr{U}_{S\to B}\right)\left(|\chi^+\rangle_{AS}\langle\chi^+|\right) \otimes |0\rangle_C \langle 0|\right] \\ &= \left(\mathscr{I}_A \otimes \mathscr{Y}_{BC\to B}\right) \circ \left(\mathscr{I}_A \otimes \mathscr{U}_{S\to B} \otimes \mathscr{I}_C\right)\left[|\chi^+\rangle_{AS}\langle\chi^+| \otimes |0\rangle_C \langle 0|\right] \\ &= \mathscr{I}_A \otimes \left(\mathscr{Y}_{BC\to B} \circ \mathscr{U}'_{SC\to BC}\right)\left[|\chi^+\rangle_{AS}\langle\chi^+| \otimes |0\rangle_C \langle 0|\right], \end{aligned}$$

where $\mathscr{U}'_{SC\to BC} := \mathscr{U}_{S\to B} \otimes \mathscr{I}_C$. Let $d_S := \dim(\mathscr{H}_S)$, $\Lambda_{SC\to B} := \frac{1}{d_S} \mathscr{Y}_{BC\to B} \circ \mathscr{U}'_{SC\to BC}$, $|\psi\rangle_{ASC} := \frac{1}{\sqrt{d_S}} |\chi^+\rangle_{AS} |0\rangle_C$, and $\mathscr{H}_R := \mathscr{H}_S \otimes \mathscr{H}_C$. Thus we have,

$$W_{AB} = (\mathscr{I}_A \otimes \Lambda_{R\to B})(|\psi\rangle_{AR}\langle\psi|),$$

where $\Lambda_{R\to B}$ is the composition of a completely positive unital map and a positive unital map; and therefore it is positive and unital. This completes the proof. □

We are now in a position to prove another important result of this work. The classical information carrying capacity of bipartite systems allowing maximal tensor product composition equals the classical capacity of the quantum composition.

Theorem 6. *The Operational Dimension of the system* $[\mathbb{C}^{d_A}, \mathbb{C}^{d_B}, \bigotimes_{\overline{SEP}}]$ *is* $d_A d_B$.

Proof. The proof is similar in spirit to Lemma 24 of Ref.[200]. However, while the assumption of 'transitivity' is used there, here we use the Proposition 6.

Let the Operational dimension of the system $[\mathbb{C}^{d_A}, \mathbb{C}^{d_B}, \bigotimes_{\overline{\text{SEP}}}]$ be N. N must be lower bounded by $d := d_A d_B$, as there exists d number of quantum states that can be perfectly distinguished by a single separable measurement. For instance, the set of pure states $\{|ij\rangle \mid i = 1, \cdots d_A \;\&\; j = 1, \cdots d_B\}$ can be distinguished by the separable measurement $\{|i\rangle\langle i| \otimes |j\rangle\langle j|\}_{i,j=1}^{d_A,d_B}$. As we have considered the operational dimension of the system $[\mathbb{C}^{d_A}, \mathbb{C}^{d_B}, \bigotimes_{\overline{\text{SEP}}}]$ to be N, there must exist N POPT states $\{W_1, \cdots, W_N\}$ and a separable measurement $\{E_1, \cdots, E_N \mid \sum_{i=1}^{N} E_i = \mathbf{1}_{AB}\}$ such that $Tr(E_i W_j) = \delta_{ij}$; $\forall i, j$. According to Proposition 6, $\forall\ j$, $W_j = (\mathscr{I} \otimes \Lambda_j)(\rho)$ for some positive, unital map $\Lambda_j : \mathscr{L}(\mathscr{H}_R) \to \mathscr{L}(\mathscr{H}_B)$ and pure state $\rho \in \mathscr{L}(\mathscr{H}_A \otimes \mathscr{H}_R)$. Denoting the projector on the orthogonal support of ρ as $P := \mathbf{1}_{AR} - \rho$, we have

$$
\begin{aligned}
d = Tr(\mathbf{1}_{AB}) = \sum_{i=1}^{N} Tr(E_i) &= \sum_{i=1}^{N} Tr[E_i(\mathscr{I} \otimes \Lambda_i)(\mathbf{1}_{AR})] \\
&= \sum_{i=1}^{N} Tr[E_i(\mathscr{I} \otimes \Lambda_i)(\rho + P)] \\
&= \sum_{i=1}^{N} Tr[E_i(\mathscr{I} \otimes \Lambda_i)(\rho)] + \sum_{i=1}^{N} Tr[E_i(\mathscr{I} \otimes \Lambda_i)(P)] \\
&= \sum_{i=1}^{N} Tr[E_i W_i] + \sum_{i=1}^{N} Tr[(\mathscr{I} \otimes \Lambda_i^*)(E_i) P],
\end{aligned}
$$

where Λ_i^* is the adjoint map of Λ_i and hence positive. Furthermore, $(\mathbb{1} \otimes \Lambda_i^*)(E_i)$ are positive operators since E_i's are separable. Therefore we have,

$$
d \geq \sum_{i=1}^{N} Tr[E_i W_i] = \sum_{i=1}^{N} \delta_{ii} = N.
$$

Since we know that $N \geq d$, therefore we conclude $N = d$. This completes the proof. □

While in Theorem 5 we have shown that the $\overline{\text{SEP}}$ composition of two elementary qubits can yield stronger timelike correlation than their quantum composition (*i.e.*, two-qubit), Theorem 6 establishes that such a composition is not strong enough to show super-additive feature of the information carrying capacity as the Information carrying capacity of a composition of two elementary systems with operational dimensions d_A and d_B, respectively will exhibit super-additive feature whenever its operational dimension $N > d_A d_B$, which accordingly results in $\log N > \log d_A + \log d_B$.. In this regard, a more generic result is presented in the next proposition.

Proposition 7. *The operational dimension of any bipartite composition (with normalized state space denoted as Ω_{AB}) of two elementary quantum systems $\mathbb{C}^{d_A}$ and $\mathbb{C}^{d_B}$ is d_Ad_B if $(\mathbf{1}_{AB} - W_{AB})$ lies within the unnormalized state cone $\forall\, W_{AB} \in \Omega_{AB}$.*

Proof. Let N be the operational dimension of the composite system. Then, there must exist a set containing N states $\{W_1, \cdots, W_N\}$ and measurement $\{E_1, \cdots, E_N \mid \sum_{i=1}^{N} E_i = \mathbf{1}_{AB}\}$ such that $Tr(E_iW_j) = \delta_{ij}$, $\forall\, i, j$. Manifestly it follows that $N \geq d := d_Ad_B$, since $\Omega_{\text{SEP}} \subseteq \Omega_{AB} \subseteq \Omega_{\overline{\text{SEP}}}$ and $\mathscr{E}_{\overline{\text{SEP}}} \subseteq \mathscr{E}_{AB} \subseteq \mathscr{E}_{\text{SEP}}$. As argued in the proof of Theorem 6, there always exists d_Ad_B number of product states that can be perfectly distinguished by a separable measurement. On the other hand,

$$\begin{aligned}\sum_{i=1}^{N} Tr(E_i(\mathbf{1} - W_i)) &= \sum_{i=1}^{N} Tr(E_i) - \sum_{i=1}^{N} Tr(E_iW_i)\\ &= d - \sum_{i=1}^{N} \delta_{ii} = d - N.\end{aligned}$$

Since $(\mathbf{1}_{AB} - W_{AB})$ is an unnormalised state by assumption, $d - N \geq 0$ or $d \geq N$, which completes the proof. $\square$

While Proposition 7 assumes elementary systems to be quantum it can however be further generalized within the GPT framework.

Proposition 8. *Let $\mathscr{S}_{AB} \equiv (\Omega_{AB}, \mathscr{E}_{AB})$ be a composite systems consisting two elementary systems $\mathscr{S}_A \equiv (\Omega_A, \mathscr{E}_A)$ and $\mathscr{S}_B \equiv (\Omega_B, \mathscr{E}_B)$ with operational dimensions N_A and N_B respectively. The operational dimension of $\mathscr{S}_{AB}$ is N_AN_B if $\exists\, \omega'_{AB} \in \Omega_{AB}$ such that $(N_AN_B\omega'_{AB} - \omega_{AB})$ is an unnormalized state $\forall\, \omega_{AB} \in \Omega_{AB}$.*

Proof. The operational dimension N_{AB} of the composite system $\mathscr{S}_{AB}$ is always greater than the product of the operational dimension of the elementary systems, *i.e.*, $N_{AB} \geq N_AN_B$. This simply follows from the fact that any valid composition includes the product states and product effects in its description. Now we have,

$$\begin{aligned}\sum_{i=1}^{N_{AB}} e_i(N_AN_B\omega' - \omega_i) &= N_AN_B \sum_{i=1}^{N_{AB}} e_i(\omega') - \sum_{i=1}^{N_{AB}} e_i(\omega_i)\\ &= N_AN_Bu(\omega') - \sum_{i=1}^{N_{AB}} \delta_{ii} = N_AN_B - N_{AB} \geq 0,\end{aligned}$$

since by assumption, $(N_A N_B \omega' - \omega_i)$ is an unnormalised state $\forall\ \omega_i$. Therefore, $N_{AB} \leq N_A N_B$, which completes the proof. □

Form Theorem 5 and Theorem 6 we can conclude that $\Delta[\mathbb{C}^2,\mathbb{C}^2,\bigotimes_{\overline{\mathrm{SEP}}}] \geq 4$, where Δ refers to the dimension mismatch of the theory. On the other hand, we can also conclude that the gap between the information dimensions of the systems $[\mathbb{C}^2,\mathbb{C}^2,\bigotimes_{\overline{\mathrm{SEP}}}]$ and $[\mathbb{C}^2,\mathbb{C}^2,\bigotimes_Q]$ is at least 4, *i.e.*,

$$\mathbb{I}\left[\mathbb{C}^2,\mathbb{C}^2,\otimes_{\overline{\mathrm{SEP}}}\right] - \mathbb{I}\left[\mathbb{C}^2,\mathbb{C}^2,\otimes_Q\right] \geq 4.$$

4.6 Increase in gap: the tripartite composition

Our next result shows that this gap can be increased further by considering more number of elementary systems.

Theorem 7. *The Information Dimension of the system* $[\mathbb{C}^2,\mathbb{C}^2,\mathbb{C}^2,\bigotimes_{\overline{SEP}}]$ *is at least* 24.

Proof. The proof is constructive and similar to the proof of Theorem 5. Consider the set of following 24 states

$$\begin{aligned}
\$[24] &:= \{\chi,\overline{\chi},\overline{\overline{\chi}}\} \subset \Omega_{\overline{\mathrm{SEP}}}[\mathbb{C}^2,\mathbb{C}^2,\mathbb{C}^2];\\
\overline{\chi} &:= \mathscr{I}\otimes \mathrm{T} \otimes \mathscr{I}(\chi);\\
\overline{\overline{\chi}} &:= \mathscr{I}\otimes \mathrm{T}\otimes \mathrm{T}(\chi);\\
|\chi\rangle \in \Bigg\{ |\Phi^{\pm}_{000}\rangle &:= \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle),\\
|\Phi^{\pm}_{001}\rangle &:= \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle),\\
|\Phi^{\pm}_{010}\rangle &:= \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle),\\
|\Phi^{\pm}_{011}\rangle &:= \frac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle)\Bigg\}.
\end{aligned}$$

We aim to show that the states in $[24] are pairwise distinguishable by fully separable measurements of the form

$$\mathscr{M} \equiv \begin{cases} E_{odd} := & |m\rangle\langle m| \otimes |n\rangle\langle n| \otimes |p\rangle\langle p| \\ & + |m\rangle\langle m| \otimes |n^\perp\rangle\langle n^\perp| \otimes |p^\perp\rangle\langle p^\perp| \\ & + |m^\perp\rangle\langle m^\perp| \otimes |n\rangle\langle n| \otimes |p^\perp\rangle\langle p^\perp| \\ & + |m^\perp\rangle\langle m^\perp| \otimes |n^\perp\rangle\langle n^\perp| \otimes |p\rangle\langle p|, \\ E_{even} = \mathbf{1} - E_{odd} \\ \quad := & |m\rangle\langle m| \otimes |n\rangle\langle n| \otimes |p^\perp\rangle\langle p^\perp| \\ & + |m\rangle\langle m| \otimes |n^\perp\rangle\langle n^\perp| \otimes |p\rangle\langle p| \\ & + |m^\perp\rangle\langle m^\perp| \otimes |n\rangle\langle n| \otimes |p\rangle\langle p| \\ & + |m^\perp\rangle\langle m^\perp| \otimes |n^\perp\rangle\langle n^\perp| \otimes |p^\perp\rangle\langle p^\perp| \end{cases}$$

where $|r\rangle, |r^\perp\rangle$ are 'up' and 'down' eigenstates of spin measurement $(\hat{r}\cdot\sigma)$ along the $\hat{r}$ direction, for $\hat{r} \in \{\hat{m}, \hat{n}, \hat{p}\}$. E_{odd} comprises of odd number of 'up spin' and E_{even} comprises of even number of 'up spin'. Clearly $\mathscr{M}$ is a an allowed measurement as $E_{odd}, E_{even} \in \mathscr{E}_{\overline{\text{SEP}}}(\mathbb{C}^2, \mathbb{C}^2, \mathbb{C}^2)$. The required m, n, and p to distinguish between different pairs of states are given on the first column of Table 4.2. For instance, the pair of states $\{\Phi^+_{000}, \Phi^-_{000}\}$ can be perfectly distinguished by choosing $(m,n,p) = (y,y,x)$. The measurement $\mathscr{M}_{\{\Phi^+_{000},\Phi^-_{000}\}} \equiv \{E_{odd}, E_{even}\}$ is given by,

$$\begin{aligned} E_{odd} := \; & |y\rangle\langle y| \otimes |y\rangle\langle y| \otimes |x\rangle\langle x| \\ & + |y\rangle\langle y| \otimes |y^\perp\rangle\langle y^\perp| \otimes |x^\perp\rangle\langle x^\perp| \\ & + |y^\perp\rangle\langle y^\perp| \otimes |y\rangle\langle y| \otimes |x^\perp\rangle\langle x^\perp| \\ & + |y^\perp\rangle\langle y^\perp| \otimes |y^\perp\rangle\langle y^\perp| \otimes |x\rangle\langle x|, \\ E_{even} = \; & 1 - E_{odd} \\ := \; & |y\rangle\langle y| \otimes |y\rangle\langle y| \otimes |x^\perp\rangle\langle x^\perp| \\ & + |y\rangle\langle y| \otimes |y^\perp\rangle\langle y^\perp| \otimes |x\rangle\langle x| \\ & + |y^\perp\rangle\langle y^\perp| \otimes |y\rangle\langle y| \otimes |x\rangle\langle x| \\ & + |y^\perp\rangle\langle y^\perp| \otimes |y^\perp\rangle\langle y^\perp| \otimes |x^\perp\rangle\langle x^\perp|. \end{aligned}$$

A straightforward calculation yields

$$\mathrm{Tr}(\Phi^-_{000} E_{odd}) = 1, \quad \mathrm{Tr}(\Phi^-_{000} E_{even}) = 0;$$
$$\mathrm{Tr}(\Phi^+_{000} E_{odd}) = 0, \quad \mathrm{Tr}(\Phi^+_{000} E_{even}) = 1.$$

Therefore, the measurement $\mathscr{M}_{\{\Phi^+_{000}, \Phi^-_{000}\}}$ perfectly distinguishes the states Φ^-_{000} and Φ^+_{000}. As we show in Table 4.2, any pair of states in $[24] can be distinguished perfectly by such a measurement. This completes the proof. □

Theorem 7 thus establishes that the $\mathscr{P}^{[24]}_D$ game can be won with three elementary qubits if the $\overline{\mathrm{SEP}}$ composition is considered among them, whereas if we consider quantum composition five elementary qubits are required.

Measu.	Odd no. 'up' spin	Even no. 'up' spin
(y,y,x)	$\Phi^-_{000}, \Phi^-_{001}, \Phi^+_{010}, \Phi^+_{011}$	$\Phi^+_{000}, \Phi^+_{001}, \Phi^-_{010}, \Phi^-_{011}$
	$\overline{\Phi^+_{000}}, \overline{\Phi^+_{001}}, \overline{\Phi^-_{010}}, \overline{\Phi^-_{011}}$	$\overline{\Phi^-_{000}}, \overline{\Phi^-_{001}}, \overline{\Phi^+_{010}}, \overline{\Phi^+_{011}}$
	$\overline{\overline{\Phi^+_{000}}}, \overline{\overline{\Phi^+_{001}}}, \overline{\overline{\Phi^-_{010}}}, \overline{\overline{\Phi^-_{011}}}$	$\overline{\overline{\Phi^-_{000}}}, \overline{\overline{\Phi^-_{001}}}, \overline{\overline{\Phi^+_{010}}}, \overline{\overline{\Phi^+_{011}}}$
(y,x,y)	$\Phi^-_{000}, \Phi^+_{001}, \Phi^-_{010}, \Phi^+_{011}$	$\Phi^+_{000}, \Phi^-_{001}, \Phi^+_{010}, \Phi^-_{011}$
	$\overline{\Phi^-_{000}}, \overline{\Phi^+_{001}}, \overline{\Phi^-_{010}}, \overline{\Phi^+_{011}}$	$\overline{\Phi^+_{000}}, \overline{\Phi^-_{001}}, \overline{\Phi^+_{010}}, \overline{\Phi^-_{011}}$
	$\overline{\overline{\Phi^+_{000}}}, \overline{\overline{\Phi^-_{001}}}, \overline{\overline{\Phi^+_{010}}}, \overline{\overline{\Phi^-_{011}}}$	$\overline{\overline{\Phi^-_{000}}}, \overline{\overline{\Phi^+_{001}}}, \overline{\overline{\Phi^-_{010}}}, \overline{\overline{\Phi^+_{011}}}$
(x,x,x)	$\Phi^+_{000}, \Phi^+_{001}, \Phi^+_{010}, \Phi^+_{011}$	$\Phi^-_{000}, \Phi^-_{001}, \Phi^-_{010}, \Phi^-_{011}$
	$\overline{\Phi^+_{000}}, \overline{\Phi^+_{001}}, \overline{\Phi^+_{010}}, \overline{\Phi^+_{011}}$	$\overline{\Phi^-_{000}}, \overline{\Phi^-_{001}}, \overline{\Phi^-_{010}}, \overline{\Phi^-_{011}}$
	$\overline{\overline{\Phi^+_{000}}}, \overline{\overline{\Phi^+_{001}}}, \overline{\overline{\Phi^+_{010}}}, \overline{\overline{\Phi^+_{011}}}$	$\overline{\overline{\Phi^-_{000}}}, \overline{\overline{\Phi^-_{001}}}, \overline{\overline{\Phi^-_{010}}}, \overline{\overline{\Phi^-_{011}}}$
(x,y,y)	$\Phi^-_{000}, \Phi^+_{001}, \Phi^+_{010}, \Phi^-_{011}$	$\Phi^+_{000}, \Phi^-_{001}, \Phi^-_{010}, \Phi^+_{011}$
	$\overline{\Phi^+_{000}}, \overline{\Phi^-_{001}}, \overline{\Phi^-_{010}}, \overline{\Phi^+_{011}}$	$\overline{\Phi^-_{000}}, \overline{\Phi^+_{001}}, \overline{\Phi^+_{010}}, \overline{\Phi^-_{011}}$
	$\overline{\overline{\Phi^-_{000}}}, \overline{\overline{\Phi^+_{001}}}, \overline{\overline{\Phi^+_{010}}}, \overline{\overline{\Phi^-_{011}}}$	$\overline{\overline{\Phi^+_{000}}}, \overline{\overline{\Phi^-_{001}}}, \overline{\overline{\Phi^-_{010}}}, \overline{\overline{\Phi^+_{011}}}$
(y,z,z)	$\Phi^+_{000}, \Phi^-_{000}, \Phi^+_{011}, \Phi^-_{011}$	$\Phi^+_{001}, \Phi^-_{001}, \Phi^+_{010}, \Phi^-_{010}$
	$\overline{\Phi^+_{000}}, \overline{\Phi^-_{000}}, \overline{\Phi^+_{011}}, \overline{\Phi^-_{011}}$	$\overline{\Phi^+_{001}}, \overline{\Phi^-_{001}}, \overline{\Phi^+_{010}}, \overline{\Phi^-_{010}}$
	$\overline{\overline{\Phi^+_{000}}}, \overline{\overline{\Phi^-_{000}}}, \overline{\overline{\Phi^+_{011}}}, \overline{\overline{\Phi^-_{011}}}$	$\overline{\overline{\Phi^+_{001}}}, \overline{\overline{\Phi^-_{001}}}, \overline{\overline{\Phi^+_{010}}}, \overline{\overline{\Phi^-_{010}}}$
(z,z,y)	$\Phi^+_{000}, \Phi^-_{000}, \Phi^+_{001}, \Phi^-_{011}$	$\Phi^+_{010}, \Phi^-_{010}, \Phi^+_{011}, \Phi^-_{011}$
	$\overline{\Phi^+_{000}}, \overline{\Phi^-_{000}}, \overline{\Phi^+_{001}}, \overline{\Phi^-_{001}}$	$\overline{\Phi^+_{010}}, \overline{\Phi^-_{010}}, \overline{\Phi^+_{011}}, \overline{\Phi^-_{011}}$
	$\overline{\overline{\Phi^+_{000}}}, \overline{\overline{\Phi^-_{000}}}, \overline{\overline{\Phi^+_{001}}}, \overline{\overline{\Phi^-_{001}}}$	$\overline{\overline{\Phi^+_{010}}}, \overline{\overline{\Phi^-_{010}}}, \overline{\overline{\Phi^+_{011}}}, \overline{\overline{\Phi^-_{011}}}$
(z,y,z)	$\Phi^+_{000}, \Phi^-_{000}, \Phi^+_{010}, \Phi^-_{010}$	$\Phi^+_{001}, \Phi^-_{001}, \Phi^+_{011}, \Phi^-_{011}$
	$\overline{\Phi^+_{000}}, \overline{\Phi^-_{000}}, \overline{\Phi^+_{010}}, \overline{\Phi^-_{010}}$	$\overline{\Phi^+_{001}}, \overline{\Phi^-_{001}}, \overline{\Phi^+_{011}}, \overline{\Phi^-_{011}}$
	$\overline{\overline{\Phi^+_{000}}}, \overline{\overline{\Phi^-_{000}}}, \overline{\overline{\Phi^+_{010}}}, \overline{\overline{\Phi^-_{010}}}$	$\overline{\overline{\Phi^+_{001}}}, \overline{\overline{\Phi^-_{001}}}, \overline{\overline{\Phi^+_{011}}}, \overline{\overline{\Phi^-_{011}}}$

FIG. 4.2 Pairwise distinguishablity of the set $[24]. Using a particular separable measurement given in the first column, any state on the odd no. 'up' spin (second) column can be distinguished from any state on the even no. 'up' spin (third) column. For instance, the pair $\{\overline{\overline{\Phi^+_{000}}}, \overline{\overline{\Phi^+_{001}}}\}$ (last row) is perfectly distinguishable via the separable measurement consisting of POVM elements given by $\mathscr{M} \equiv \{E_{odd}, E_{even}\}$, where E_{odd} and E_{even} are rank four projectors comprising odd number of spin-up and even number of spin-up outcomes respectively for the Pauli measurement $(\sigma_Z, \sigma_Y, \sigma_Z) \equiv (z,y,z)$.

4.7 Concluding Remarks

The need to understand quantum mechanics results in investigating theories other than itself which opens up a new avenue for research. Comparisons among the information processing capabilities in the various theories lead to newer insights about the underlying cause for such capabilities which led to the motivation for this paper. While Barnum, et al. in [47] have shown that in the space-like scenario, bipartite maximal tensor product structure of local quantum systems cannot generate beyond quantum correlations, the authors in [194] have shown that in a generalized Bell scenario every beyond quantum state can produce beyond quantum correlations. In this work, we have used a different approach wherein timelike scenarios are considered instead of the traditional spacelike Bell scenarios. We have provided concrete results that can be experimentally verified and used as principles to single out the quantum composition rule. While Corollary 4 and Theorem 6 establish that the phenomenon of dimension mismatch occurs in $\overline{SEP}$ composition, it has been shown [201, 196] that dimension mismatch occurs in SEP composition as well. A natural question then is to ask what other compositions can be ruled out using dimension mismatch. Another interesting direction to explore is by relaxing the assumption of quantum sub-systems. Propositions 7 and 8 provide some preliminary results in the GPT framework which may be useful in this regard. Our study forms an important piece of the quantum reconstruction program in which we seek to derive quantum theory from physical principles [27–29].

Chapter 5

Distillation and Discrimination of Post Classical Correlations

5.1 Motivation

One of the most celebrated non-classical aspects of quantum mechanics was pioneered by J. S. Bell in the year 1964 [84] (see also [85]). Bell's theorem mandates departure of quantum theory from the *locally causal* world view which subsequently has been confirmed in several milestone experiments led by Clauser, Aspect, Zeilinger, and others [205–214]. Unlike other non-classical features, such as entanglement and coherence, study of nonlocality can be conducted in a device independent setting where only the input-output statistics of the device matters and one does not need to know the inner design or working mechanisms of the device [215]. Along with foundational implications, Bell nonlocality has also been identified as the necessary resource for several important protocols [216–221, 61, 222–226], which, thus, makes the question of refinement or distillation of this resource practically indispensable. The study of nonlocality distillation has two major implications – (i) practical: where one aims to distill nonlocal correlations observed in the quantum world which can be then applied to make information flow networks efficient and secure, and (ii) foundational: where the goal is to identify post-quantum correlations, which, in turn, helps to understand the specialty of quantum theory among other possibilities allowed within the framework of generalized probabilistic theories. Interestingly, in Ref.[227], Forster *et al.* proposed a nonlocality distillation protocol that can extract nonlocality in stronger form starting with many copies of weakly nonlocal systems; this work has inspired several subsequent works consisting of interesting results on nonlocality distillation [228–240, 74, 75].

The research conducted so far on nonlocality distillation is mainly focused on distilling post quantum correlations [228–233, 235–240]. Only a few protocols are known that successfully distill some quantum correlations [227, 240]. The difficulty arises due to the top-down approach considered in earlier works where one starts with some parametric family of generic no-signaling (NS) correlations, and after obtaining a successful distillation protocol the motive is to check whether for some range of the parameter values the considered NS correlations allow quantum realization or not. For the simplest bipartite case, the well-known analytical criterion by Tsirelson-Landau-Masanes [241–243] and the Navascues-Pironio-Acin (NPA) criterion [244], and in general case a hierarchy of semi-definite programming conditions [245] can serve this purpose. Only in some fortunate cases sophisticated choices of the parametric class of NS correlations might lead to a desirable subset of quantum realizable correlations. However, the approach has severe pitfalls when more input-output scenarios are considered, as the recent mathematical breakthrough by W. Slofstra and the subsequent results establish that the set of quantum correlations is not topologically closed [246–248]. There are only a few results that report distillation of nonlocal correlations within quantum setup [227, 240], albeit the nonlocal strength of the distilled correlation is low. Therefore the aspects of analytical and quantitative study for distillation of quantum nonlocal correlations remain open.

In this chapter, which is based on one of our works [78], we now propose a generic framework for nonlocality distillation that overcomes limitations of the thus far proposed protocols. In contrast to the previously reported results, we intend to find out efficient distillation protocol(s) for quantum correlations. To this aim we consider the bottom-up approach. Instead of generic NS signaling correlations we start with weak nonlocal correlations which are quantum, and then try to obtain a nonlocality distillation protocol. The set of quantum correlations being closed under *wirings* [74, 75] assures the resulting distilled correlations to be quantum. Interestingly, we identify a simple protocol and come up with a generic approach that successfully distills nonlocality in a large class of weakly nonlocal quantum correlations. Towards this goal, first, we consider a variant of the nonlocality test proposed by Lucien Hardy [249], which we have discussed extensively in Chapter 2, Section 2.2.4. Success probability in Hardy's test qualifies as a measure of nonlocality for Hardy's correlations [250]. Given two copies of a quantum Hardy correlation, we show that there exists a simple

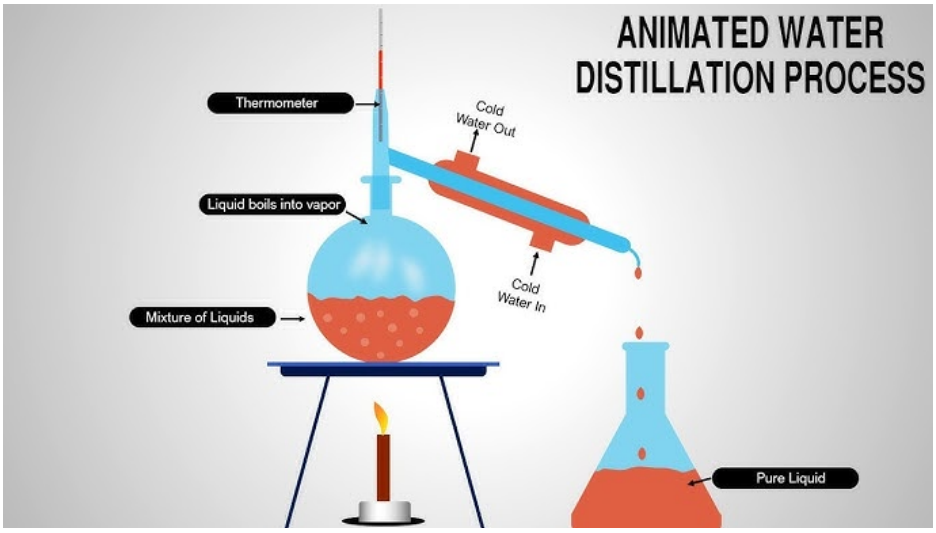

FIG. 5.1 Distillation of impure water

wiring that can distill Hardy nonlocality. We call this wiring logical OR-AND protocol, where OR ($\vee$) and AND ($\wedge$) functions on 2-bits z_1, z_2 are defined as $\vee(z_1, z_2) = \max\{z_1, z_2\}$ and $\wedge(z_1, z_2) = \min\{z_1, z_2\}$, respectively. The OR-AND protocol allows an immediate n-copy generalization (see Fig.5.2), which can provide a substantial distillation of Hardy's success with sufficiently large copies of initial correlations.

The chapter is organized as follows: in Section 5.2 we start by showing that the OR-AND protocol preserves the quantum Hardy structure and moreover it can distill the nonlocal strength of Hardy correlations. Further, we show in Section 5.3, that the OR-AND wiring when applied to a broader class of quantum correlations yields an interesting result: an arbitrarily small violation of the Clauser-Horne-Shimony-Holt (CHSH) [205] inequality can be amplified to a significantly higher degree. Finally, by applying our protocol we demonstrate in Section 5.4 that nonlocal correlations arbitrarily close to the extreme points of the set of local correlations are always distilled, which, in turn, establishes that set of distillable quantum as well as non-quantum correlations has non-zero measure in the full eight dimensions of the correlation space. In Section 5.5, we then move on to study the distillation of post-quantum correlations and show that OR-AND protocol becomes efficient there too. In particular, we find correlations whose post-quantum signature is established through OR-AND distillation, while the known information principles, such as nontrivial communication complexity [70] and information causality [251, 252], fail to serve the purpose. In

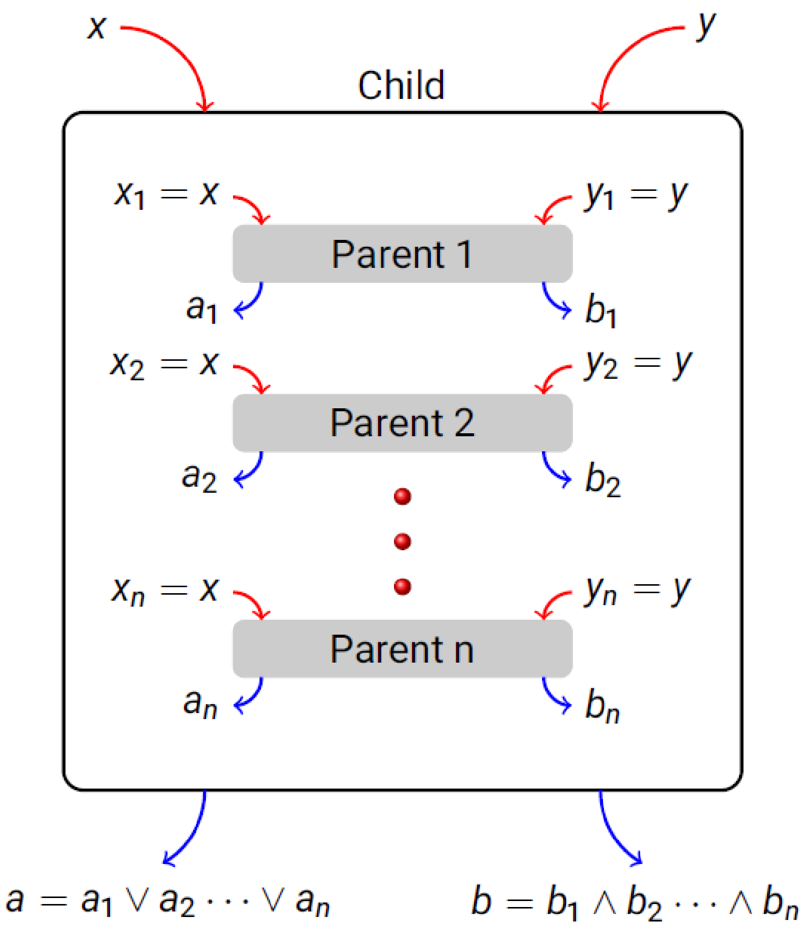

FIG. 5.2 Multi-copy OR-AND wiring. Given n-number of parent correlations $\{\mathrm{P}_{NS}[i]\}_{i=1}^{n} \subset \mathbb{NS}$, the OR-AND wiring produce a child correlation $\mathrm{P}_{NS}^{(n)} \in \mathbb{NS}$. The outcome a on Alice's side for the child box is obtained as, $a = a_1 \vee \cdots \vee a_n = \max\{a_1, \cdots, a_n\}$ for the input $x_1 = \cdots = x_n = x$, where x_i and a_i are the input and output of the i^{th} parent. On the Bob's side, $y_1 = \cdots = y_n = y$ and $b = b_1 \wedge \cdots \wedge b_n = \min\{b_1, \cdots, b_n\}$.

the end, in Section 5.6, we conclude this chapter by discussing the novelty of the approach followed here in comparison to the existing methods on nonlocality distillation.

5.2 OR-AND wiring and the structure of quantum Hardy correlations

Theorem 8. *The OR-AND wiring preserves the structure of quantum Hardy correlations and can efficiently distill the strength of success probability in Hardy's test of nonlocality.*

Proof. Within the considered CHSH symmetry [*i.e.*, Eq.(2.8)], any NS correlation can be represented as a convex mixture of the nonlocal vertex along with 8 local vertices. A quantum Hardy correlation demands nonzero weights for exactly 5 different local vertices along with the nonlocal vertex [239]. This, in turn, ensures that the correlation matrix has precisely 3 zero elements corresponding to probabilities taking the value zero in Hardy's test. It turns out that, then any quantum Hardy correlation H_Q, can be represented as

$$\mathrm{H}_Q = c_0 \mathrm{P}_{NL} + \sum_{i=1}^{5} c_i \mathrm{P}_{L_i}; \;\; c_i > 0 \; \forall \, i, \;\; \text{and} \; \sum_{i=0}^{5} c_i = 1, \tag{5.1}$$

with success in Hardy's test $p_{\text{Hardy}} = \frac{c_0}{2}$. With little algebra, it can be shown that OR-AND wiring applied to two copies of H_Q results in a correlation

$$\begin{aligned}\mathrm{H}_Q^{(2)} =& 2\left(\left(\frac{c_0}{2}+c_1\right)^2 - c_1^2\right)\mathrm{P}_{NL} + c_1^2 \mathrm{P}_{L_1} + \left(c_0\left(1-\frac{c_0}{2}\right) + 2c_2\left(1-\frac{c_2}{2}\right) - c_0\left(c_1+c_2\right)\right)\mathrm{P}_{L_2} \\ &+ c_3\left(2-c_0-c_3-2c_2\right)\mathrm{P}_{L_3} + c_4\left(c_0+2c_1+c_4\right)\mathrm{P}_{L_4} + c_5\left(c_0+2c_1+2c_4+c_5\right)\mathrm{P}_{L_5}.\end{aligned} \tag{5.2}$$

Eq.(5.2) is clearly in the form Eq.(5.1) (i.e., both are convex mixtures of same set of one nonlocal and five local boxes) and therefore the correlation resulting from wiring is a Hardy nonlocal correlation, establishing that OR-AND protocol preserves Hardy structure of quantum Hardy correlations.

Thus on applying the OR-AND wiring to 2 copies of (parents) H_Q one obtains a resulting (child) Hardy correlation $\mathrm{H}_Q^{(2)}$ with nonlocality strength $p_{\text{Hardy}}^{(2)} = (\frac{c_0}{2}+c_1)^2 - c_1^2$. It is also clear from the expression that 2-copy OR-AND wiring distills nonlocality whenever $\frac{c_0}{2} + 2c_1 > 1$. Similarly, on applying OR-AND protocol to n copies of H_Q we obtain a (child) Hardy correlation $\mathrm{H}_Q^{(n)}$ with nonlocality strength $p_{\text{Hardy}}^{(n)} = (\frac{c_0}{2}+c_1)^n - c_1^n$. The protocol serves the purpose of an effective n copy distillation as long as $p_{\text{Hardy}}^{(k)} > p_{\text{Hardy}}^{(k-1)}$, for all $k \in \{2,3,...,n\}$. □

5.2.1 Distillation of arbitrarily weak quantum Hardy correlation

Let us consider the class of quantum correlations

$$\tilde{\mathrm{H}}_Q(\lambda) := \lambda \mathrm{H}_Q^{\max} + (1-\lambda)\mathrm{P}_{L_1}, \;\; \lambda \in (0,1], \tag{5.3}$$

for which the Hardy success probability $p_{\text{Hardy}}(\lambda) = \lambda k_1 = \frac{\lambda}{2}(5\sqrt{5} - 11)$. Then, on applying the OR-AND protocol to two copies of (parent) $\tilde{\text{H}}_Q(\lambda)$ yields the child $\tilde{\text{H}}_Q^{(2)}(\lambda)$ with Hardy success probability $p^{(2)}_{\text{Hardy}}(\lambda) = [\lambda(k_1 + 2k_2) + 2(1-\lambda)]\lambda k_1$. Then it follows that $p^{(2)}_{\text{Hardy}}(\lambda) > p_{\text{Hardy}}(\lambda)$ for $\lambda \in (0, \phi^{-1})$, where ϕ is the golden ratio, *i.e.*, $\phi = \frac{1+\sqrt{5}}{2}$.

We will show now that on considering sufficiently large copies (n) of very weakly nonlocal correlations $\tilde{\text{H}}_Q$ Eq. (5.3) with $p_{\text{Hardy}}(\lambda) \to 0$, we find that the OR-AND wiring results in a Hardy correlation with a considerably large nonlocal strength $p^{(n)}_{\text{Hardy}} = 0.041$.We further show that arbitrarily weak quantum Hardy correlation can be distilled up to 0.0433.

To see this, let us turn to the distillability of quantum Hardy correlations under multi copy OR-AND wiring. In general, here we consider a two parameter family of quantum Hardy correlations which also includes the maximum quantum Hardy correlation used in Theorem 8. The family of such correlations is as

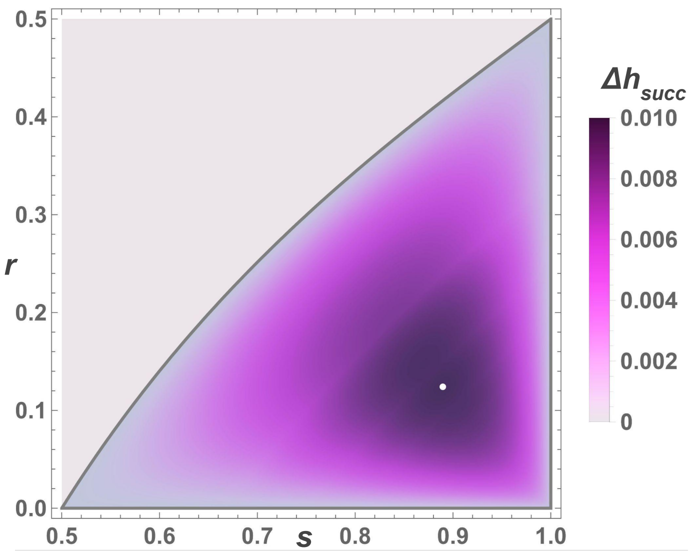

FIG. 5.3 The variation of distillation gap with r and s. The coloured region satisfies Eq.(5.9) and the distillation gap of an (r,s) point is mapped by the color as shown in the color bar. The white point denotes the correlation with maximal distillation gap.

follows,

$$
\mathrm{H}_{\mathrm{NS}}^{(r,s)} \equiv
\begin{array}{c}
xy/ab \\ 00 \\ 01 \\ 10 \\ 11
\end{array}
\begin{array}{c}
\begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\
\begin{pmatrix}
\frac{(1-r)r(1-s)s}{1-rs} & \frac{(1-r)^2 s}{1-rs} & (1-r)(1-s) & r \\
0 & (1-r)s & \frac{1-s}{1-rs} & \frac{(1-r)rs^2}{1-rs} \\
0 & s & \frac{(1-r)(1-s)}{1-rs} & \frac{r(1-s)^2}{1-rs} \\
\frac{r(1-s)s}{1-rs} & \frac{(1-r)s}{1-rs} & 1-s & 0
\end{pmatrix}
\end{array}
\tag{5.4}
$$

where, $r,s \in [0,1]$. The measurements performed by Alice and Bob are given by

$$\text{Alice's measurements}: \ \{x_0 \equiv \{|0\rangle\langle 0|, |1\rangle\langle 1|\}, \quad x_1 \equiv \{|u_0\rangle\langle u_0|, |u_1\rangle\langle u_1|\}\}, \tag{5.5a}$$

$$\text{Bob's measurements}: \ \{y_0 = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}, \quad y_1 = \{|v_0\rangle\langle v_0|, |v_1\rangle\langle v_1|\}\}, \tag{5.5b}$$

where, the first term in the brackets corresponds to the outcome 0 and second term the outcome 1, and

$$|u_0\rangle := \mathbf{C}_\alpha|0\rangle + e^{\iota\phi}\mathbf{S}_\alpha|1\rangle, \quad |u_1\rangle := -\mathbf{S}_\alpha|0\rangle + e^{\iota\phi}\mathbf{C}_\alpha|1\rangle, \tag{5.6}$$

$$|v_0\rangle := \mathbf{C}_\beta|0\rangle + e^{\iota\xi}\mathbf{S}_\beta|1\rangle, \quad |v_1\rangle := -\mathbf{S}_\beta|0\rangle + e^{\iota\xi}\mathbf{C}_\beta|1\rangle, \tag{5.7}$$

$$\text{with } \ \mathbf{C}_z := \cos(z/2), \ \ \mathbf{S}_z := \sin(z/2) \ \text{ and } \ \alpha,\beta \in [0,\pi] \ \ \&\ \phi,\xi \in [0,2\pi).$$

The two-qubit state on which the measurements are performed, yielding the correlation (5.4), is given by

$$|\psi\rangle_{_{Hardy}} := \frac{|u_0 v_0\rangle + \mathbf{W}_\alpha\,|u_1 v_0\rangle + \mathbf{W}_\beta\,|u_0 v_1\rangle}{\sqrt{1+\mathbf{W}_\alpha^2+\mathbf{W}_\beta^2}}; \quad \mathbf{W}_z := \cot(z/2) \tag{5.8}$$

where $r := 1 - \mathbf{S}_\alpha^2\mathbf{S}_\beta^2$ and $s := r^{-1}\mathbf{C}_\alpha^2$ [95]. It can be verified that maximal Hardy nonlocality is achieved when $r = s = \frac{1}{2}\left(\sqrt{5}-1\right)$, resulting in Eq.(2.9) which we have discussed in Chapter 2, Section 2.2.4. Correlation $\mathrm{H}_{\mathrm{NS}}^{(r,s)}$ can be distilled using OR-AND protocol *if and only if*

$$r^2(s+s^2) - r(s^2+2s) + (2s-1) > 0. \tag{5.9}$$

Furthermore, it turns out that the region of distillability remains the same for the n-copy wiring. One can take a step further, and quantify the distillability of these correlations under the n-copy OR-AND protocol using distillation gap, defined as $\Delta h_{\text{succ}} := p_{\text{Hardy}}^{(N^{\text{opt}})} - p_{\text{Hardy}}$, where N^{opt} is the optimal number of copies obtained from Proposition 1. The resulting variation of distillation gap with r and s is shown in Fig.5.3. The colored region in the density plot satisfies Eq.(5.9) and the distillation gap of a point is mapped by the color as indicated by the color bar. The white point in the graph denotes the optimal distillation of approximately 0.0101896, obtained when 4 copies of the quantum correlation $\mathrm{H}_{\text{NS}}^{(r,s)}$ identified by $r \approx 0.1241$ and $s \approx 0.8896$ is used.

Interestingly, a much higher distillation gap can be obtained when one considers convex mixtures of the correlations given in Eq.(5.4) and P_{L_1}. More strikingly, high amount of nonlocality can be distilled from mixtures with vanishingly small contribution from quantum Hardy correlations. For example, consider the correlation from Eq.(5.3) given by,

$$\tilde{\mathrm{H}}_Q(\lambda) := \lambda \mathrm{H}_Q^{\max} + (1-\lambda)\mathrm{P}_L^{[1]}, \;\; \lambda \in (0,1].$$

The Hardy success of this correlation is $p_{\text{Hardy}}(\lambda) = \lambda k_1 = \frac{\lambda}{2}(5\sqrt{5}-11)$. Now, after using the n-copy OR-AND protocol, the resulting Hardy success is given by

$$p_{\text{Hardy}}^{(n)}(\lambda) = (c_0/2 + c_1)^n - c_1^n = \left(\left(\sqrt{5}-3\right)\lambda + 1\right)^n - \left(\frac{\sqrt{5}}{2}\left(\sqrt{5}-3\right)\lambda + 1\right)^n.$$

Now, assuming very small λ and Taylor expanding around $\lambda = 0$, it turns out that the leading order term in the expression for optimal number of copies (see Proposition 1) is of the order λ^{-1}. Hence, for very small values of λ, we can ignore the floor function arising in N^{opt}. Thus, we have the following for $p_{\text{Hardy}}^{(\mathrm{N}^{opt})}$ in the small λ limit,

$$\begin{aligned} p_{\text{Hardy}}^{(\mathrm{N}^{opt})}(\lambda) &= 4^{(2+\sqrt{5})}\, 5^{(-\frac{5}{2}-\sqrt{5})}\left(\sqrt{5}-2\right) - 4^{(1+\sqrt{5})}\, 5^{(-2-\sqrt{5})}\left(\sqrt{5}-3\right)\log\left(\frac{5}{4}\right)\lambda + O\left(\lambda^2\right) \\ &\approx 0.0410237 + 0.0165601\lambda + O\left(\lambda^2\right) \end{aligned} \tag{5.10}$$

Eq.(5.10) tells that even as λ approaches 0, corresponding to vanishingly small initial nonlocality, the optimal use of the n-copy OR-AND can distill a high nonlocality of approximately 0.0410237. In fact, this increases linearly with λ.

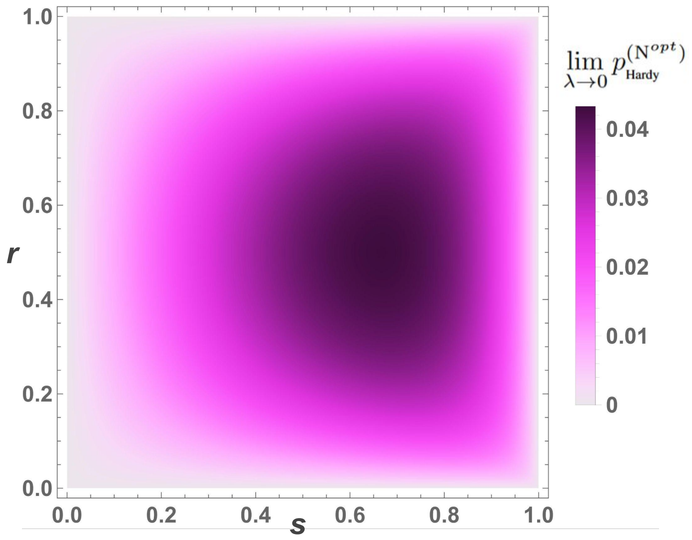

FIG. 5.4 The variation of distilled Hardy success in the $\lambda \to 0$ with r and s. The Hardy success of an (r,s) point is mapped by the color as shown in the color bar.

In the above, we have considered the mixture of optimal quantum Hardy correlation $\mathrm{H}_Q^{\max}$ with P_{L_1}. We can consider the same scenario for arbitrary $\mathrm{H}_Q^{(r,s)}$. Then again, in the small λ limit, one can follow similar steps to arrive at the following expression for the optimal Hardy success in the limit of vanishing λ,

$$\lim_{\lambda\to 0} p_{\text{Hardy}}^{(\mathrm{N}^{opt})}(r,s,\lambda) = \frac{(1-r)r(1-s)s\left(\frac{1-s+(1-r)rs}{1-s+(1-r)rs^2}\right)^{\left(1-\frac{1}{(1-r)rs}-\frac{1}{1-s}\right)}}{1-s+(1-r)rs}. \tag{5.11}$$

A density plot of Eq.(5.11) is shown in Fig.5.4, where the distilled Hardy success of the point (r,s) is indicated by the color of the point. Moreover, one can find the optimal value of Eq.(5.11) to be approximately 0.0433049, attained when $r = \frac{1}{2}$ and $s = \frac{2}{3}$. This is interesting, since it means that the mixture of a weakly nonlocal Hardy correlation with local noise can distill more nonlocality than a mixture with the optimal quantum nonlocal Hardy correlation and the same local noise. This again reveals the nontrivial structure of nonlocality distillation. Finally, note that despite the ability of the OR-AND protocol to distill high Hardy success from a mixture of $\mathrm{H}_Q^{(r,s)}$ and P_{L_1}, one can numerically verify that the distilled success of this mixture is never greater than the distilled success of $\mathrm{H}_Q^{(r,s)}$ itself.

While applying multi-copy OR-AND protocol it turns out that the optimal distillation of Hardy's success is obtained with a threshold number of initial boxes, and the success gets decreased if more number of initial boxes are considered. Our next proposition provides an exact expression for the optimal number of initial Hardy correlation required for maximal distillation.

Proposition 9. *A no-signaling Hardy correlation of the form of Eq.*(6.1) *yields Hardy success* $p^{(n)}_{Hardy} = (\frac{c_0}{2}+c_1)^n - c_1^n$*, when its* n*-copy is wired under OR-AND protocol. The optimal value of distilled Hardy success is given by* $p^{opt}_{Hardy} = \max\{p^{(\mathrm{N})}_{Hardy},\ p^{(\mathrm{N}+1)}_{Hardy}\}$*, where*

$$\mathrm{N} := \left\lfloor \log\left(\frac{\log c_1}{\log\frac{c_0}{2}+c_1}\right)/\log\left(\frac{\frac{c_0}{2}+c_1}{c_1}\right)\right\rfloor. \tag{5.12}$$

Proof. Condition for n copy distillation demands that at least two copy distillation must be successful, i.e., $\mathrm{n}\geq 2$. This imposes the condition $c_1 > \frac{1}{2}-\frac{c_0}{2}$ (along with other conditions $c_0\geq 0$, $c_1\geq 0$, and $c_0+c_1\leq 1$ on the coefficients c_0 and c_1 of the respective boxes P_{NL} and P_{L_1}). Let us consider a continues and smooth function $f(x)=\left(\frac{c_0}{2}+c_1\right)^x-(c_1)^x$ obtained by substituting the number of copies n with a continuous variable $x\in[1,\infty)$ in the expression for Hardy's success probability $p^n_{\text{Hardy}} = (\frac{c_0}{2}+c_1)^n - c_1^n$. The derivative $\frac{df(x)}{dx}$ takes the value zero at exactly one point given by

$$x^* = \log\left(\frac{\log c_1}{\log\frac{c_0}{2}+c_1}\right)/\log\left(\frac{\frac{c_0}{2}+c_1}{c_1}\right). \tag{5.13}$$

Then, one can conclude that the critical point x^* is the point of global maxima of $f(x)$ because due to at least two copy distillation condition $f(x)$ must be an increasing function in the beginning, then it achieves the global maxima at x^* and starts decreasing when $x>x^*$. Let us define $\mathrm{N}=\lfloor x^*\rfloor$, then since $f(x^*)\geq f(x)$ for all $x\in[1,\infty)$ it easily follows that the optimal value of distilled Hardy success is given by $p^{opt}_{\text{Hardy}} = \max\{p^{(\mathrm{N})}_{\text{Hardy}},\ p^{(\mathrm{N}+1)}_{\text{Hardy}}\}$. The optimal number of copies of initial boxes yielding maximum distillation of Hardy success, i.e., N^{opt} is either N or $\mathrm{N}+1$; the one which gives maximum Hardy success. This completes the proof. □

5.3 Distillation of CHSH nonlocal quantum correlations

Here, we consider quantum nonlocal correlation, not necessarily in Hardy form, to establish an even higher Tsirelson gain through the OR-AND wiring. Since a correlation with Hardy success p_{Hardy} yields CHSH value $2+4p_{\text{Hardy}}$ [250], in order to measure the efficacy of distillation let us define the *Tsirelson gain in percentage* as follows,

$$\Delta\mathscr{T} := \frac{1}{2(\sqrt{2}-1)}(\mathscr{B}_{\text{Child}} - \mathscr{B}_{\text{Parent}}) \times 100\%. \tag{5.14}$$

Manifestly, the gain will be 100% when by wiring a nonlocal correlation with arbitrary small CHSH violation, the distilled correlation achieves Tsirelson's bound – the maximum CHSH value in NS [253]. We then obtain that under the OR-AND wiring a quantum Hardy correlation can yield Tsirelson gain at most 20.9%.

Theorem 9. *Starting with a quantum correlation with arbitrarily small CHSH nonlocality OR-AND wiring can yield Tsirelson gain up to* ($\approx$) 39.75%*.*

Proof. Consider a one parameter family of quantum correlations given by

$$\tilde{\mathrm{B}}_Q(\lambda) := \lambda \mathrm{B}_Q^{\max} + (1-\lambda)\mathrm{P}_{L_1}, \;\; \lambda \in (0,1], \;\; \text{where,} \tag{5.15}$$
$$\mathrm{B}_Q^{\max} := (\sqrt{2}-1)\mathrm{P}_{NL} + \frac{1}{4}\left(1 - \frac{1}{\sqrt{2}}\right)\sum_{i=1}^{8} \mathrm{P}_{L_i}.$$

Note that the correlation $\mathrm{B}_Q^{\max}$ saturates the Tsirelson's bound in NS. Manifestly, $\tilde{\mathrm{B}}_Q(\lambda)$ yields CHSH value $\mathscr{B}(\lambda) = 2 + (2\sqrt{2}-2)\lambda$. After 2-copy OR-AND wiring the resulting correlation $\tilde{\mathrm{B}}_Q^{(2)}(\lambda)$ attains CHSH value $\mathscr{B}^{(2)}(\lambda) = 2 + 2(2\sqrt{2}-2)\lambda + (11/4 - 3\sqrt{2})\lambda^2$. Distillation is successful whenever $\lambda < \frac{8}{167}(13-\sqrt{2}) \approx 0.555$. While appropriate choice of λ yields maximal Tsirelson gain ($\approx$) 13.9% with 2-copy distillation of the correlation $\tilde{\mathrm{B}}_Q(\lambda)$, multi-copy OR-AND wirings can yield a maximal gain ($\approx$) 39.75% and is obtained via distillation of parent correlation with arbitrary small value of λ. □

In the proof to Theorem 9, we have showed that a mixture containing P_{L_1} and arbitrarily small amount of $\mathrm{B}_Q^{\max}$ can be distilled using the OR-AND protocol. Now, we numerically show that by using the optimal number of copies, we can distill to a high CHSH value of 2.32.

For this, first note that, given an arbitrary correlation $\mathrm{P} \equiv \{p(ab|xy)\}$ the resulting correlation after n-copy OR-AND protocol is given by,

$$p^{(n)}(00|xy) = (p(00|xy) + p(01|xy))^n - p(01|xy)^n, \tag{5.16a}$$

$$p^{(n)}(01|xy) = p(01|xy)^n, \tag{5.16b}$$

$$p^{(n)}(11|xy) = (p(11|xy) + p(01|xy))^n - p(01|xy)^n, \tag{5.16c}$$

$$p^{(n)}(10|xy) = 1 - p^{(n)}(00|xy) - p^{(n)}(01|xy) - p^{(n)}(11|xy). \tag{5.16d}$$

Eq.(5.16) can be easily verified using mathematical induction starting from the 2-copy OR-AND protocol. Using Eq.(5.16), we arrive at the following expression for the distilled CHSH value ($\mathscr{B}^n(\lambda)$) of the correlation $\tilde{\mathrm{B}}_Q(\lambda)$ using the n-copy OR-AND protocol:

$$\mathscr{B}^{(n)}(\lambda) = 2 - 8\left(1 - \frac{\lambda}{2}\right)^n + 12\left(1 - \frac{1}{8}\left(6 - \sqrt{2}\right)\lambda\right)^n - 4\left(1 - \frac{1}{8}\left(6 + \sqrt{2}\right)\lambda\right)^n. \tag{5.17}$$

Eq.(5.17) can now be used to estimate the maximum CHSH value that can be distilled in the $\lambda \to 0$ limit. However, this scenario is more difficult compared to the proof in Section 5.2.1 since we do not have an analytical expression for the optimal number of copies for maximal distillation of the CHSH value.

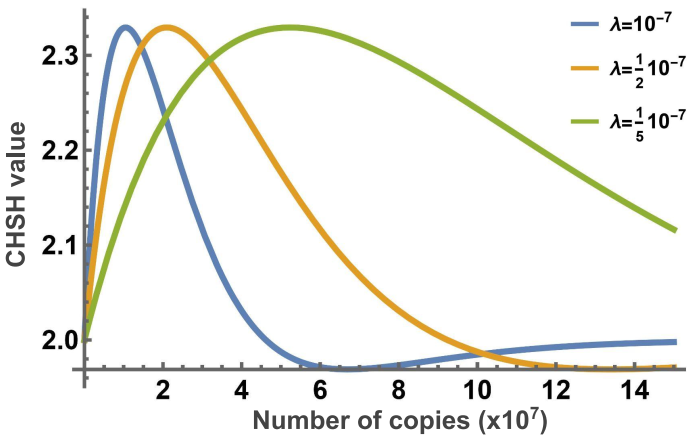

FIG. 5.5 The distilled CHSH value of the correlation $\tilde{\mathrm{B}}_Q(\lambda)$ is plotted as a function of the number of copies for different values of λ. The figure shows that optimal distilled CHSH value is around 2.32928 for the different values of small λ considered, yielding the Tsirelson gain, $\Delta\mathscr{T} \approx \frac{0.32928}{2\sqrt{2}-2} \times 100\% \approx 39.748\%$

.

Let us start by considering a small value of $\lambda = 10^{-7}$ and studying the variation of the distilled CHSH value with the number of copies (see Fig.5.5). As seen from Fig.5.5, the distilled value for $\lambda = 10^{-7}$ initially increases with the number of copies, reaches a maximum of 2.32928 for 1.04739×10^{7} copies and then decays to the classical value of 2. Note that the CHSH value drops below 2 before eventually saturating at 2. Moreover, Fig.5.5 shows that peak value does not change significantly as λ is reduced to $\lambda = \frac{1}{2}10^{-7}$ or $\frac{1}{5}10^{-7}$ and that overall behaviour is similar upto some re-scaling.

This suggests that the optimal number of copies is inversely proportional to λ, in the small λ limit. This motivates an ansatz for the optimal number of copies $N^{\text{opt}} = \frac{\alpha}{\lambda}$, for α unknown. Since the derivative for $\mathscr{B}^{(n)}(\lambda)$ with n vanishes at the optimal number of copies, solving $\lim_{\lambda\to 0} \frac{d\mathscr{B}^{(n)}(\lambda)}{dn}\Big|_{\frac{\alpha}{\lambda}} = 0$ can be used to find α. This can in turn be done using Taylor expansion, yielding the value of $\alpha = 1.047391$. One can further numerically show that this ansatz is robust in the sense that for $\lambda < 10^{-5}$, $\frac{d\mathscr{B}^{(n)}(\lambda)}{dn}\Big|_{\frac{\alpha}{\lambda}} < 10^{-11}$. Thus, using this ansatz, we can obtain the following expression for $\mathscr{B}^{(N^{\text{opt}})}(\lambda)$ when $\lambda < 10^{-5}$:

$$\mathscr{B}^{(N_{\text{opt}})}(\lambda) \approx 2.32928 + 0.169161\lambda + O(\lambda^2). \tag{5.18}$$

This proves the claim that as $\lambda \to 0$, the AND-OR protocol can distill a large nonlocality of approximately 2.32928.

Theorem 9 has many interesting implications for information processing tasks, wherein higher CHSH violation is desirable for higher performance of the protocols. For instance, the amount of certifiable randomness as obtained in [219] monotonically scales with the degree of violation of CHSH inequality. On the other hand, the authors in [223] come up with a conflicting interest Bayesian game where the payoff in correlated equilibrium strategy increases linearly with the amount of CHSH violation (see also [224]). More recently, the authors in [225] proposed a communication task where pre-shared entanglement between sender and receiver is shown to enhance the communication utility of a perfect classical communication channel. As it turns out payoff of this task is also a linear function of the value of CHSH expression [226].

5.4 Distillable No-Signaling Correlations: Subsets of Non-Zero Measures

By now, an observant reader might have already noticed that the local box P_{L_1} plays crucial role in the proof of Theorem 8 and Theorem 9. We will now use this observation to prove a generic result as formalized in the following theorem.

Theorem 10. *CHSH nonlocality of any no-singling correlation of the form* $\tilde{C}(\lambda) = \lambda C + (1-\lambda)P_{L_1}$, *where* $0 < \lambda \leq 1$ *and* $C \in \text{ConvexHull}\,\{P_{NL}, P_{L_i} \mid i \in \{1,\cdots,8\}\}$ *can be distilled through OR-AND wiring by choosing the values of* λ *sufficiently small. Furthermore,* 2*-copy OR-AND distillation is successful for all the* $\tilde{C}(\lambda)$ *correlation boxes whenever* $\lambda < \frac{2}{3}c_0$*; where* c_0 *is the* P_{NL} *fraction in* C.

Proof. Given two correlations $\chi_1, \chi_2 \in \mathbb{NS}$, let $\mathscr{W}[\chi_1,\chi_2]$ denotes the resulting correlation obtained under OR-AND wiring, where $\mathscr{W}[\chi,\chi] \equiv \chi^{(2)}$. We, therefore, have

$$\tilde{C}^{(2)}(\lambda) = \lambda^2 C^{(2)} + \lambda(1-\lambda)\{\mathscr{W}[C,P_{L_1}] + \mathscr{W}[P_{L_1},C]\} \\ + (1-\lambda)^2 \mathscr{W}[P_{L_1},P_{L_1}].$$

A straightforward calculation yields, $\mathscr{W}[C,P_{L_1}] = C = \mathscr{W}[P_{L_1},C]$, that further result in

$$\tilde{C}^{(2)}(\lambda) = \lambda^2 C^{(2)} + 2\lambda(1-\lambda)C + (1-\lambda)^2 P_{L_1}.$$

While CHSH value of the box P_{L_1} is 2, let the CHSH value of the boxes C and $C^{(2)}$ be denoted as $\mathscr{K}$ (>2) and $\mathscr{K}^{(2)}$ respectively. Then, the CHSH value of the correlations $\tilde{C}(\lambda)$ and $\tilde{C}^{(2)}(\lambda)$ can be expressed as,

$$\mathscr{B}(\lambda) = \lambda\ \mathscr{K} + 2\ (1-\lambda),$$
$$\mathscr{B}^{(2)}(\lambda) = \lambda^2\ \mathscr{K}^{(2)} + 2\ \lambda\ (1-\lambda)\mathscr{K} + 2\ (1-\lambda)^2.$$

A successful distillation demands $\mathscr{B}^{(2)}(\lambda) > \mathscr{B}(\lambda)$, implying $(\mathscr{K}-2) + (\mathscr{K}^{(2)} - 2\mathscr{K}+2)\lambda > 0$, which can be guaranteed by choosing the values for λ accordingly. This completes first part of the proof. A bit more calculation yields the quantitative bound $\lambda < \frac{2}{3}c_0$, on the radius of the eight-dimensional ball centered at point P_{L_1} assuring 2-copy OR-AND distillation such that any nonlocal no-signaling correlation, be it quantum or post-quantum, chosen from a nonzero-measure sector of the ball can be distilled (in the full eight dimensions).

Given two correlations $\chi_1 \equiv \{p_1(ab|xy\}$ and $\chi_2 \equiv \{p_2(ab|xy\}$ in $\mathbb{NS}$, the resulting correlation obtained through OR-AND wiring is denoted as $\mathscr{W}[\chi_1,\chi_2] \equiv \{p(ab|xy\}$. The input-output joint probabilities for the resulting correlation reads as

$$p(00|xy) = \sum_{b_1 \wedge b_2 = 0} p_1(0b_1|xy)p_2(0b_2|xy); \tag{5.19a}$$

$$p(01|xy) = p_1(01|xy)p_2(01|xy); \tag{5.19b}$$

$$p(11|xy) = \sum_{a_1 \vee a_2 = 1} p_1(a_1 1|xy)p_2(a_2 1|xy); \tag{5.19c}$$

$$p(10|xy) = 1 - p(00|xy) - p(01|xy) - p(11|xy); \tag{5.19d}$$

for all $x,y \in \{0,1\}$. Now, let us consider two correlation $\mathrm{C} \equiv \{c(ab|xy)\} \in \mathbb{NS}$ and $\mathrm{P}_{L_1} = \{p_{L_1}(ab|xy) = \delta_{a,0}\ \delta_{b,1}\}$. We denote $\mathscr{W}[\mathrm{C},\mathrm{P}_{L_1}] \equiv \{p_{\mathrm{C,L_1}}(ab|xy)\}$, then on substituting the probabilities of the local box P_{L_1}, above stated relations for two OR-AND wired boxes reduce to:

$$p_{\mathrm{C,L_1}}(00|xy) = c(00|xy); \tag{5.20a}$$

$$p_{\mathrm{C,L_1}}(01|xy) = c(01|xy); \tag{5.20b}$$

$$p_{\mathrm{C,L_1}}(10|xy) = c(10|xy); \tag{5.20c}$$

$$p_{\mathrm{C,L_1}}(11|xy) = c(11|xy); \tag{5.20d}$$

for all $x,y \in \{0,1\}$. Therefore, $\mathscr{W}[\mathrm{C},\mathrm{P}_{L_1}] = \mathrm{C}$. Similarly, by substituting the probabilities of the P_{L_1} box it also easily follows that $\mathscr{W}[\mathrm{P}_{L_1},\mathrm{C}] = \mathrm{C}$, and $\mathscr{W}[\mathrm{P}_{L_1},\mathrm{P}_{L_1}] = \mathrm{P}_{L_1}$.

Further, for obtaining a quantitative bound on the the radius of the eight-dimensional ball centered at P_{L_1} within which any nonlocal correlation, in a sector of nonzero-measure, allows 2-copy OR-AND distillation, we write the correlation C in terms of the coefficients of the PR-box and eight local boxes, then

$$\mathrm{C} = c_0\mathrm{P}_{NL} + \sum_{i=1}^{8} c_i\mathrm{P}_{L_i}. \tag{5.21}$$

Now on calculating, the respective Bell-CHSH values $\mathscr{K}$ and $\mathscr{K}^{(2)}$ of respective correlations C and $\mathrm{C}^{(2)}$ we find that

$$\mathscr{K} = 2(1+c_0), \tag{5.22}$$

$$\mathscr{K}^{(2)} = 2+c_0^2+4c_0(c_1+2c_4)+8c_4(c_1+c_2+c_3+c_5+c_6-1)+8c_4^2-8c_5c_7. \tag{5.23}$$

In the above we have used the normalization condition $\sum_{i=0}^{8} c_i = 1$ to eliminate the coefficient c_8. Then the condition for two copy distillation can be written as follows:

$$\begin{aligned} & (\mathscr{K}-2)+(\mathscr{K}^{(2)}-2\mathscr{K}+2)\,\lambda > 0 \\ \implies\ & 2\,c_0+\left\{c_0^2+4c_0(c_1+2c_4-1)+8\left(c_4(c_1+c_2+c_3+c_5+c_6-1)+c_4^2-c_5c_7\right)\right\}\lambda > 0 \\ \equiv\ & 2\,c_0+f(c_0,c_1,c_2,c_3,c_4,c_5,c_6,c_7)\,\lambda > 0. \end{aligned} \tag{5.24}$$

Since $2c_0+\min\{f(c_0,c_1,...,c_7)\}>0 \implies 2c_0+f(c_0,c_1,...,c_7)>0$, two copy distillation is possible if $2c_0+\min\{f(c_0,c_1,...,c_7)\}>0$. Further, $\min\{f(c_0,c_1,...,c_7)\}=-3$ and it is achieved at $c_0=1$ and $c_1=c_2=c_3=c_4=c_5=c_6=c_7=0$. Therefore, we obtain that for any *NS* correlation $\tilde{\mathrm{C}}(\lambda)$, two copy distillation is successful if

$$2c_0-3\lambda>0 \Rightarrow \lambda<\frac{2}{3}\,c_0. \tag{5.25}$$

Thus we also have an analytical expression for the radius of the ball centered at P_{L_1} such that any nonlocal no-signaling correlation $\tilde{\mathrm{C}}(\lambda)$, be it quantum or post-quantum, chosen from a nonzero-measure sector of the ball can be distilled (in full eight dimensions). □

Theorem 10 has profound topological implication. It establishes that the sets of no-signalling, as well as quantum correlations allowing nonlocality distillation, have non-zero measure in the full eight-dimensional correlation space. Furthermore, it should be mentioned that the correlation box P_{L_1} appearing in Theorem 10 is not any special local deterministic box: the result holds also for all the remaining 15 local deterministic boxes on suitable relabeling of the OR-AND wiring.

While the studies in nonlocality distillation of quantum correlations are mostly limited to the 2-2-2 Bell scenario, Theorem 10 opens up an avenue to study the same in a general N-M-K scenario that involves N spatially separated parties each performing M different measurements with K outcomes. It is not hard to find the extreme local boxes in such a general scenario. Now if for such an extreme box P_L we obtain a wiring W such that $\mathrm{W}[P_L,\mathrm{X}] = X = \mathrm{W}[\mathrm{X},P_L]$ for any N-M-K no-signaling correlation X, then it results in a generalization of Theorem 10 in the N-M-K scenario. This consequently will imply that quantum correlations allowing nonlocality distillation have non-zero measure even in this general scenario.

5.5 Detection of Post-Quantum Correlations

We now proceed to show that OR-AND wiring has an important proviso in ruling out (unphysical) post-quantum correlations. Several techniques are there to establish post-quantumness of a given correlations. For instance, isotropic no-signaling correlations yielding CHSH value more than $4\sqrt{2/3}$ violate the principle of nontrivial communication complexity [70] (see also [71–73]), thus demarcating such correlations as unphysical. Furthermore, any NS correlating with CHSH value more than Tsirelson bound violates the principle of information causality [251, 252]. It has also been shown that a correlation might not violate these principles by its own, but after distillation the resulting correlation violates such a principle, which, in turn, establish unphysicality of the original correlation [228] (see also [240]).

Interestingly, the OR-AND wiring becomes useful to establish post-quantum nature of a correlation. Let us consider the following NS correlation

$$\mathrm{H}_{NS} = 0.1\ \mathrm{P}_{NL} + 0.85\ \mathrm{P}_{L_1} + 0.01\ \mathrm{P}_{L_2} + 0.01\ \mathrm{P}_{L_3} + 0.02\ \mathrm{P}_{L_4} + 0.01\ \mathrm{P}_{L_5}, \tag{5.26}$$

$$= \begin{array}{c} xy/ab \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} 0.05 & 0.85 & 0.01 & 0.09 \\ 0 & 0.90 & 0.08 & 0.02 \\ 0 & 0.93 & 0.06 & 0.01 \\ 0.01 & 0.92 & 0.07 & 0 \end{pmatrix} \end{array} \tag{5.27}$$

which exhibits Hardy's nonlocality with success probability $p_{\mathrm{Hardy}} = 0.05$. While its Hardy success is 0.05, after OR-AND distillation the Hardy success gets increased. The optimal distillation is achieved for 8-copy parent correlation and the resulting child correlation reads as

$$\mathrm{H}_{NS}^{(8)} = 0.31594\mathrm{P}_{NL} + 0.27249\ \mathrm{P}_{L_1} + 0.23246\ \mathrm{P}_{L_2} + 0.04999\ \mathrm{P}_{L_3} + 0.08275\ \mathrm{P}_{L_4} + 0.0436\ \mathrm{P}_{L_5}, \tag{5.28}$$

$$= \begin{array}{c} xy/ab \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} 0.157977 & 0.272491 & 0.232454 & 0.337078 \\ 0 & 0.430467 & 0.486781 & 0.0827517 \\ 0 & 0.559582 & 0.390431 & 0.0499871 \\ 0.0463629 & 0.513219 & 0.440418 & 0 \end{pmatrix} \end{array} \tag{5.29}$$

Child correlation $\mathrm{H}_{NS}^{(8)}$ having the Hardy success 0.157977, which is greater that optimal quantum bound $(5\sqrt{5}-11)/2 \approx 0.09$, this fact then establishes the post-quantum nature of the parent correlation H_{NS}. As it turns out the correlation H_{NS} neither violates known necessary condition for respecting the principal of nontrivial communication complexity nor for the principle of information causality. However, the considered example violates the macroscopic locality principle [254]. That being said, we do point out that checking membership to the NPA hierarchy can become computationally expensive, particularly at higher orders of the hierarchy, while the distillation criteria is far more tractable.

Importantly, several other known post-quantum tests fail to detect post-quantumness of the correlation H_{NS}. For instance, correlations having CHSH value more than $4\sqrt{2/3} \approx 3.26599$ violate nontrivial communication complexity [70]. However, for the correlations H_{NS} and $\mathrm{H}_{NS}^{(8)}$ the CHSH values turns out to be 2.2 and 2.63088, respectively, which are strictly less than the aforesaid threshold value 3.26599.

The authors in [251] have obtained a sufficient criterion for violation of the information causality principle. For the CHSH symmetry considered in this work, the condition reads as

$$\mathscr{I} := E_1^2 + E_2^2 > 1, \ \text{ where } \ E_i := 2\mathscr{P}_i - 1, \ \text{ with}$$

$$\mathscr{P}_1 := \frac{1}{2}[p(a\oplus b = 0|00) + p(a\oplus b = 1|10)], \ \ \mathscr{P}_2 := \frac{1}{2}[p(a\oplus b = 1|01) + p(a\oplus b = 1|11)]$$

For the correlations H_{NS} and $\mathrm{H}_{NS}^{(8)}$ the values that $\mathscr{I}$ attain are respectively 0.9578 and 0.9565. Therefore information causality remains silent about the post-quantum nature of these boxes.

However, it may be noted that correlation given in Eq.(5.26) falls outside the first level of the NPA-hierarchy [245]. This easily proves the post-quantumness of the correlation under consideration, and moreover, implies that the correlation violates the principle of macroscopic locality [254].

That being said, we do point out that checking membership to the different levels of NPA hierarchy can become computationally expensive, particularly at higher levels of the hierarchy, while the distillation criteria can be far more computationally tractable. For instance, let us consider the correlation:

$$\mathrm{H}'_{NS} = \begin{array}{c c} xy/ab & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{pmatrix} 0.0773 & 0.0256 & 0.5599 & 0.3372 \\ 0 & 0.1029 & 0.7804 & 0.1167 \\ 0 & 0.3374 & 0.6372 & 0.0254 \\ 0.1178 & 0.2196 & 0.6626 & 0 \end{pmatrix} \end{array} . \tag{5.30}$$

One may easily verify that correlation given in Eq.(5.30) is post-quantum by observing that after 2-copy distillation using OR-AND protocol, the Hardy success goes up to 0.0925 (a value beyond the maximum possible success probaility in quantum mechanics). On the other hand, for the considered correlation, tests like known necessary conditions for violating non-trivial computational complexity and information causality principle fails to detect its post-quantumness. However, unlike the first example, on considering NPA criteria, a membership test into the second tier of the NPA hierarchy is required to establish the post-quantumness of this correlation. Along similar lines, one may imagine post-quantum correlations like Eq.(5.30) that lies at further deeper levels of the NPA-hierarchy, while its post-quantumness may be conveniently detected via efficient nonlocality distillation protocols.

5.6 Concluding Remarks

Distillation, the process of extracting a desirable substance in pure form from a source of impure mixture through heating and other means, has an ancient history. Quite interestingly, during recent past, the idea finds novel applications in quantum information theory, where one aims to obtain fewer number of higher resourceful states starting with larger number of lesser resourceful states under free operations [255]. Some canonical examples are: (i) for our present study, the resource theory of Bell-nonlocal boxes [256, 257], or (ii) the well known protocols for quantum entanglement distillation, where many copies of mixed entangled states are distilled into pure form under local quantum operations and classical communications [258].

In summary, we have established a generic approach for distillation of nonlocal correlations arising in quantum mechanics. This problem is of utmost importance as Bell nonlocal correlations are ubiquitous in device-independent protocols – more the nonlocality more the utility. Interestingly, we come up with an elegant protocol, the OR-AND wiring, that distills nonlocality in quantum correlations with high efficiency. In the simplest bipartite scenario, in stark distinction with the results reported prior to our work [227–240, 74, 75], our protocol establishes that, within the set of full eight-dimensional correlation space, the distillable quantum as well as no-signaling nonlocal correlations form subsets of non-zero measures; i.e., sector of open balls of a specified radius centered at local deterministic correlations (Theorem 10). Moreover, by considering correlations arbitrarily close to local deterministic points, applying our protocol, with optimal number of copies, one can distill nonlocality by a significant amount both for the quantum as well as post-quantum non-signaling correlations. Finally, we also demonstrate the efficacy of the considered distillation protocol in detecting post-quantum correlations.

Chapter 6

Summary and Further Outlook

Let us now summarize the main results of this thesis. We have studied the significance of various discrimination tasks and their implications in different quantum information processing scenarios. We introduced the task of local state marking (LSM) in Section 3.8, a novel variant of the local state discrimination task (LSD). In Section 3.9, we show how these two tasks are inequivalent. In Section 3.10, we present examples of a set of mutually orthogonal bipartite states that cannot even be marked locally. Hence, this results in a stronger form of quantum nonlocality in the LOCC paradigm than what we already know. Then in Section 3.11, we go on to explore the possibility of entanglement-assisted marking of states that otherwise are locally unmarkable. The advantage of LSM becomes apparent in comparison to multi-copy LSD in an information-theoretic task which we discuss in Section 3.12. Thereafter, in Section 4.4, we show that the maximal tensor product theory, also known as the $\overline{\text{SEP}}$ theory, one of the many theories concerning the composition of local quantum systems, does indeed show beyond quantum correlation even concerning bipartite local quantum systems. We were able to show this using a game that is based on a pairwise distinguishability task. From there, we go on to prove that $\overline{\text{SEP}}$ theory shows dimension mismatch, which we discuss in Section 4.5. We then demonstrate in Section 4.6 that the gap between the information dimensions of a system composed of three-qubit subsystems under the $\overline{\text{SEP}}$ composition rule and those under the quantum composition rule is even larger than in the bipartite case with two-qubit subsystems. This establishes that the gap in the communication utilities of quantum theory and the $\overline{\text{SEP}}$ theory increases further once we increase the cardinality of the pairwise distinguishability game to 24. Thereafter, we move to the context of Bell nonlocality. Bell inequalities discriminate a classical correlation from a post-classical one. However, the degree of nonlocality can vary from one correlation to the other. The nonlocality of a correlation is a resource in information-processing tasks. Hence we move on to the study of distillation of the nonlocality in correlations. In Section 5.2, we give a distillation protocol for Bell correlations which can preserve the structure of Hardy correlations as well as distill their strength of nonlocality. In Section 5.3, we demonstrate that applying the OR-AND wiring to a wider range of quantum correlations produces a notable outcome: an arbitrarily small violation of the Clauser-Horne-Shimony-Holt (CHSH) [205] inequality can be amplified to a significantly higher degree. Subsequently, in Section 5.4 using our protocol we show that nonlocal correlations, which are arbitrarily close to the boundary of local correlations, can consistently be distilled. This finding implies that the sets of distillable quantum and non-quantum correlations occupy a non-zero measure in the full eight-dimensional correlation space. Moving to post-quantum scenarios in Section 5.5, we examine how the OR-AND protocol operates effectively in this context as well. Specifically, we identify correlations that display post-quantum behavior when distilled through the OR-AND process, even when principles such as nontrivial communication complexity [70] or information causality [251, 252] fail to detect the post-quantum nature.

The present thesis leaves open several important questions and possibilities for further study. In the following we summarize some of those and mention some of the relevant issues.

1. It is important to resolve the question of optimal resource consumption for local state marking task with and without catalysts as mentioned in discussions after Theorem 4 and in Section 3.11, respectively. Furthermore, all the ensembles considered in the present work consist of bipartite entangled states. Except for Corollary 2, the present work does not provide much insight into the local state marking of ensembles containing only product states. Does there exist such a product ensemble that cannot be marked locally? If yes, would it imply a stronger notion of *nonlocality without entanglement* [174]? In the recent past, this phenomenon of *nonlocality without entanglement* has been studied in the generalized probabilistic theory framework [154]. It might be interesting to extend the study of LSM in this framework.
   In the same spirit of multipartite LSD [181], exploring LSM for multipartite systems might unveil new features of LOCC as well as of multipartite

entanglement. Finally, local indistinguishability has also been shown to have practical implications in cryptographic primitives such as data hiding and secret sharing. It would be quite interesting to find such novel applications for the LSM task introduced here.

2. In Section 4.5, Corollary 4 and Theorem 6 establish that the phenomenon of dimension mismatch occurs in $\overline{SEP}$ composition, it has been shown [201, 196] that dimension mismatch occurs in SEP composition as well. A natural question then is to ask what other compositions can be ruled out using dimension mismatch. Another interesting direction to explore is by relaxing the assumption of quantum sub-systems. Propositions 7 and 8 provide some preliminary results in the GPT framework which may be useful in this regard.

3. In Section 5.2, we gave the OR-AND wiring protocol which preserves the structure of quantum Hardy correlations and can efficiently distill the strength of success probability in Hardy's test of nonlocality. As for the future, it would be interesting to explore the full potential of our generic framework proposed here in distilling quantum nonlocal correlations. In particular, obtaining some bound on the relative volume of the quantum correlations in the correlation space that can be distilled under OR-AND wiring would be interesting. Furthermore, a generalization of this protocol for higher input-output as well as in multiparty scenarios might be of great use.

References

[1] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, July 1948.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, Feb. 1978.

[3] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[4] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing. , 10-12 december 1984, .," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore*, pp. 175–179, 1984.

[5] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, p. 78–88, Jan. 1983.

[6] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, p. 802–803, Oct. 1982.

[7] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on einstein-podolsky-rosen states," *Physical Review Letters*, vol. 69, no. 20, p. 2881, 1992.

[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical Review Letters*, vol. 70, no. 13, p. 1895, 1993.

[9] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.

[10] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Reviews of modern physics*, vol. 86, no. 2, p. 419, 2014.

[11] A. Peres and W. K. Wootters, "Optimal detection of quantum information," *Phys. Rev. Lett.*, vol. 66, pp. 1119–1122, Mar 1991.

[12] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, "Quantum nonlocality without entanglement," *Phys. Rev. A*, vol. 59, pp. 1070–1091, Feb 1999.

[13] D. DiVincenzo, D. Leung, and B. Terhal, "Quantum data hiding," *IEEE Transactions on Information Theory*, vol. 48, no. 3, pp. 580–598, 2002.

[14] W. Matthews, S. Wehner, and A. Winter, "Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding," *Communications in Mathematical Physics*, vol. 291, no. 3, pp. 813–843, 2009.

[15] D. Markham and B. C. Sanders, "Graph states for quantum secret sharing," *Phys. Rev. A*, vol. 78, p. 042309, Oct 2008.

[16] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical Review Letters*, vol. 83, no. 3, p. 648, 1999.

[17] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, pp. 1829–1834, Mar 1999.

[18] R. Rahaman and M. G. Parker, "Quantum scheme for secret sharing based on local distinguishability," *Phys. Rev. A*, vol. 91, p. 022330, Feb 2015.

[19] J. Wang, L. Li, H. Peng, and Y. Yang, "Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states," *Phys. Rev. A*, vol. 95, p. 022320, Feb 2017.

[20] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical Review Letters*, vol. 67, no. 6, p. 661, 1991.

[21] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, p. 3121, 1992.

[22] C. H. Bennett and G. Brassard, "Quantum cryptography," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, 1984.

[23] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, "Everything you always wanted to know about locc (but were afraid to ask)," *Communications in Mathematical Physics*, vol. 328, no. 1, pp. 303–326, 2014.

[24] G. Ludwig, "Attempt of an axiomatic foundation of quantum mechanics and more general theories, ii," *Communications in Mathematical Physics*, vol. 4, p. 331–348, Oct. 1967.

[25] E. B. Davies and J. T. Lewis, "An operational approach to quantum probability," *Communications in Mathematical Physics*, vol. 17, p. 239–260, Sept. 1970.

[26] B. Mielnik, "Generalized quantum mechanics," *Communications In Mathematical Physics*, vol. 37, p. 221–256, Sept. 1974.

[27] L. Hardy, "Quantum theory from five reasonable axioms," *arXiv preprint quant-ph/0101012*, 2001.

[28] J. Barrett, "Information processing in generalized probabilistic theories," *Phys. Rev. A*, vol. 75, p. 032304, Mar 2007.

[29] G. Chiribella, G. M. D'Ariano, and P. Perinotti, "Informational derivation of quantum theory," *Phys. Rev. A*, vol. 84, p. 012311, Jul 2011.

[30] H. Barnum and A. Wilce, "Information processing in convex operational theories," *Electronic Notes in Theoretical Computer Science*, vol. 270, no. 1, pp. 3–15, 2011. Proceedings of the Joint 5th International Workshop on Quantum Physics and Logic and 4th Workshop on Developments in Computational Models (QPL/DCM 2008).

[31] L. Masanes and M. P. Müller, "A derivation of quantum theory from physical requirements," *New Journal of Physics*, vol. 13, p. 063001, jun 2011.

[32] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, "Generalized no-broadcasting theorem," *Phys. Rev. Lett.*, vol. 99, p. 240501, Dec 2007.

[33] M. P. Müller and C. Ududec, "Structure of reversible computation determines the self-duality of quantum theory," *Phys. Rev. Lett.*, vol. 108, p. 130401, Mar 2012.

[34] M. Kleinmann, T. J. Osborne, V. B. Scholz, and A. H. Werner, "Typical local measurements in generalized probabilistic theories: emergence of quantum bipartite correlations," *Phys. Rev. Lett.*, vol. 110, p. 040403, Jan. 2013.

[35] M. Dall'Arno, S. Brandsen, A. Tosini, F. Buscemi, and V. Vedral, "No-hypersignaling principle," *Phys. Rev. Lett.*, vol. 119, p. 020401, Jul 2017.

[36] Y. Yoshida, H. Arai, and M. Hayashi, "Perfect discrimination in approximate quantum theory of general probabilistic theories," *Phys. Rev. Lett.*, vol. 125, p. 150402, Oct. 2020.

[37] M. Plávala, "General probabilistic theories: An introduction," *Physics Reports*, vol. 1033, pp. 1–64, 2023. General probabilistic theories: An introduction.

[38] I. Namioka and R. Phelps, "Tensor products of compact convex sets," *Pacific Journal of Mathematics*, vol. 31, p. 469–480, Nov. 1969.

[39] G. P. Barker, "Monotone norms and tensor products," *Linear and Multilinear Algebra*, vol. 4, p. 191–199, Jan. 1976.

[40] G. P. Barker, "Theory of cones," *Linear Algebra and its Applications*, vol. 39, p. 263–291, Aug. 1981.

[41] G. Aubrun, L. Lami, C. Palazuelos, and M. Plávala, "Entangleability of cones," *Geometric and Functional Analysis*, vol. 31, p. 181–205, Apr. 2021.

[42] M. Kläy, C. Randall, and D. Foulis, "Tensor products and probability weights," *International Journal of Theoretical Physics*, vol. 26, p. 199–219, Mar. 1987.

[43] N. R. Wallach, "An unentangled gleason's theorem," 2000.

[44] H. Barnum, C. A. Fuchs, J. M. Renes, and A. Wilce, "Influence-free states on compound quantum systems," 2005.

[45] G. Chiribella, G. M. D'Ariano, and P. Perinotti, "Probabilistic theories with purification," *Phys. Rev. A*, vol. 81, p. 062348, Jun 2010.

[46] A. Acín, R. Augusiak, D. Cavalcanti, C. Hadley, J. K. Korbicz, M. Lewenstein, L. Masanes, and M. Piani, "Unified framework for correlations in terms of local quantum observables," *Phys. Rev. Lett.*, vol. 104, p. 140404, Apr 2010.

[47] H. Barnum, S. Beigi, S. Boixo, M. B. Elliott, and S. Wehner, "Local quantum measurement and no-signaling imply quantum correlations," *Phys. Rev. Lett.*, vol. 104, p. 140401, Apr 2010.

[48] P. Janotta, C. Gogolin, J. Barrett, and N. Brunner, "Limits on nonlocal correlations from the structure of the local state space," *New Journal of Physics*, vol. 13, p. 063024, jun 2011.

[49] S. Popescu and D. Rohrlich, "Quantum nonlocality as an axiom," *Foundations of Physics*, vol. 24, p. 379–385, Mar. 1994.

[50] S. Popescu, "Nonlocality beyond quantum mechanics," *Nat. Phys.*, vol. 10, p. 264–270, Apr. 2014.

[51] L. Masanes, S. Pironio, and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices," *Nature communications*, vol. 2, no. 1, pp. 1–7, 2011.

[52] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, *et al.*, "Random numbers certified by bell's theorem," *Nature*, vol. 464, no. 7291, pp. 1021–1024, 2010.

[53] A. Acín, S. Massar, and S. Pironio, "Randomness versus nonlocality and entanglement," *Phys. Rev. Lett.*, vol. 108, p. 100402, Mar 2012.

[54] J. Barrett, A. Kent, and S. Pironio, "Maximally nonlocal and monogamous quantum correlations," *Phys. Rev. Lett.*, vol. 97, p. 170409, Oct 2006.

[55] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, "Full security of quantum key distribution from no-signaling constraints," *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4973–4986, 2014.

[56] J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution," *Phys. Rev. Lett.*, vol. 95, p. 010503, Jun 2005.

[57] R. Colbeck and R. Renner, "Hidden variable models for quantum theory cannot have any local part," *Phys. Rev. Lett.*, vol. 101, p. 050403, Aug 2008.

[58] R. Colbeck and R. Renner, "No extension of quantum theory can have improved predictive power," *Nature Communications*, vol. 2, no. 1, pp. 1–5, 2011.

[59] T. Franz, F. Furrer, and R. F. Werner, "Extremal quantum correlations and cryptographic security," *Phys. Rev. Lett.*, vol. 106, p. 250502, Jun 2011.

[60] C. Dhara, G. Prettico, and A. Acín, "Maximal quantum randomness in bell tests," *Phys. Rev. A*, vol. 88, p. 052116, Nov 2013.

[61] A. Chaturvedi and M. Banik, "Measurement-device–independent randomness from local entangled states," *EPL (Europhysics Letters)*, vol. 112, p. 30003, Nov. 2015.

[62] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, "Limit on nonlocality in any world in which communication complexity is not trivial," *Phys. Rev. Lett.*, vol. 96, p. 250401, Jun 2006.

[63] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, "Nonlocal correlations as an information-theoretic resource," *Phys. Rev. A*, vol. 71, p. 022101, Feb 2005.

[64] J. Barrett, "Information processing in generalized probabilistic theories," *Phys. Rev. A*, vol. 75, p. 032304, Mar 2007.

[65] W. Van Dam, "Implausible consequences of superstrong nonlocality," *Natural Computing*, vol. 12, no. 1, pp. 9–12, 2013.

[66] A. J. Short, S. Popescu, and N. Gisin, "Entanglement swapping for generalized nonlocal correlations," *Phys. Rev. A*, vol. 73, p. 012101, Jan 2006.

[67] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical Review Letters*, vol. 23, no. 15, p. 880, 1969.

[68] L. Hardy, "Quantum mechanics, local realistic theories, and lorentz-invariant realistic theories," *Physical Review Letters*, vol. 68, no. 20, p. 2981, 1992.

[69] L. Hardy, "Nonlocality for two particles without inequalities for almost all entangled states," *Physical Review Letters*, vol. 71, no. 11, p. 1665, 1993.

[70] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, "Limit on nonlocality in any world in which communication complexity is not trivial," *Physical Review Letters*, vol. 96, June 2006.

[71] W. van Dam, "Implausible consequences of superstrong nonlocality, [see also arXiv:quant-ph/0501159]," *Natural Computing*, vol. 12, p. 9–12, Nov. 2012.

[72] G. Brassard, "Is information the key?," *Nature Physics*, vol. 1, p. 2–4, Oct. 2005.

[73] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, “Nonlocality and communication complexity,” *Reviews of Modern Physics*, vol. 82, p. 665–698, Mar. 2010.

[74] J. Allcock, N. Brunner, N. Linden, S. Popescu, P. Skrzypczyk, and T. Vértesi, “Closed sets of nonlocal correlations,” *Physical Review A*, vol. 80, Dec. 2009.

[75] B. Lang, T. Vértesi, and M. Navascués, “Closed sets of correlations: answers from the zoo,” *Journal of Physics A: Mathematical and Theoretical*, vol. 47, p. 424029, Oct. 2014.

[76] S. Sen, E. P. Lobo, S. G. Naik, R. K. Patra, T. Gupta, S. B. Ghosh, S. Saha, M. Alimuddin, T. Guha, S. S. Bhattacharya, and M. Banik, “Local quantum state marking,” *Phys. Rev. A*, vol. 105, p. 032407, Mar 2022.

[77] S. Sen, E. P. Lobo, R. K. Patra, S. G. Naik, A. Das Bhowmik, M. Alimuddin, and M. Banik, “Timelike correlations and quantum tensor product structure,” *Phys. Rev. A*, vol. 106, p. 062406, Dec 2022.

[78] S. G. Naik, G. L. Sidhardh, S. Sen, A. Roy, A. Rai, and M. Banik, “Distilling nonlocality in quantum correlations,” *Phys. Rev. Lett.*, vol. 130, p. 220201, Jun 2023.

[79] M. A. Nielsen and I. Chuang, “Quantum computation and quantum information,” 2002.

[80] M. Neumark, “On a representation of additive operator set functions,” in *CR (Doklady) Acad. Sci. URSS (NS)*, vol. 41, pp. 359–361, 1943.

[81] L. Hardy and W. K. Wootters, “Limited holism and real-vector-space quantum theory,” *Foundations of Physics*, vol. 42, pp. 454–473, 2012.

[82] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?,” *Physical review*, vol. 47, no. 10, p. 777, 1935.

[83] D. Bohm, “Quantum theory prentice-hall,” *Englewood Cliffs, NJ*, 1951.

[84] J. S. Bell, “On the einstein podolsky rosen paradox,” *Physics Physique Fizika*, vol. 1, pp. 195–200, Nov 1964.

[85] J. S. Bell, “On the problem of hidden variables in quantum mechanics,” *Reviews of Modern Physics*, vol. 38, p. 447–452, July 1966.

[86] N. Gisin, “Bell’s inequality holds for all non-product states,” *Physics Letters A*, vol. 154, no. 5-6, pp. 201–202, 1991.

[87] B. S. Cirel’son, “Quantum generalizations of bell’s inequality,” *Letters in Mathematical Physics*, vol. 4, no. 2, pp. 93–100, 1980.

[88] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani, “Geometry of the set of quantum correlations,” *Physical Review A*, vol. 97, Feb. 2018.

[89] A. Rai, C. Duarte, S. Brito, and R. Chaves, "Geometry of the quantum set on no-signaling faces," *Physical Review A*, vol. 99, Mar. 2019.

[90] S. Goldstein, "Nonlocality without inequalities for almost all entangled states for two particles," *Phys. Rev. Lett.*, vol. 72, pp. 1951–1951, Mar 1994.

[91] S. K. Choudhary and P. Agrawal, "The hardy's nonlocality argument," *International Journal of Quantum Information*, vol. 14, no. 06, p. 1640035, 2016.

[92] G. Kar, "Hardy's nonlocality for mixed states," *Physics Letters A*, vol. 228, no. 3, pp. 119–120, 1997.

[93] R. Rabelo, L. Y. Zhi, and V. Scarani, "Device-independent bounds for hardy's experiment," *Physical Review Letters*, vol. 109, Oct. 2012.

[94] K. P. Seshadreesan and S. Ghosh, "Constancy of maximal nonlocal probability in hardy's nonlocality test for bipartite quantum systems," *Journal of Physics A: Mathematical and Theoretical*, vol. 44, p. 315305, July 2011.

[95] A. Rai, M. Pivoluska, S. Sasmal, M. Banik, S. Ghosh, and M. Plesch, "Self-testing quantum states via nonmaximal violation in hardy's test of nonlocality," *Physical Review A*, vol. 105, May 2022.

[96] R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication," *Physical Review A*, vol. 56, no. 2, p. 1201, 1997.

[97] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, "Nonlocality and communication complexity," *Rev. Mod. Phys.*, vol. 82, pp. 665–698, Mar 2010.

[98] N. Herbert, "Cryptographic approach to hidden variables," *American Journal of Physics*, vol. 43, no. 4, pp. 315–316, 1975.

[99] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992.

[100] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," 1998.

[101] A. Acín, N. Gisin, and L. Masanes, "From bell's theorem to secure quantum key distribution," *Phys. Rev. Lett.*, vol. 97, p. 120405, Sep 2006.

[102] J. Barrett, R. Colbeck, and A. Kent, "Unconditionally secure device-independent quantum key distribution with only two devices," *Phys. Rev. A*, vol. 86, p. 062326, Dec 2012.

[103] R. Colbeck, "Quantum and relativistic protocols for secure multi-party computation (phd thesis)," *arXiv preprint arxiv:0911.3814*, 2007.

[104] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices," *Journal of Physics A: Mathematical and Theoretical*, vol. 44, no. 9, p. 095305, 2011.

[105] S. Pironio and S. Massar, "Security of practical private randomness generation," *Phys. Rev. A*, vol. 87, p. 012336, Jan 2013.

[106] U. Vazirani and T. Vidick, "Stoc'12 proceedings of the 44th symposium on theory of computing," 2012.

[107] S. Fehr, R. Gelles, and C. Schaffner, "Security and composability of randomness expansion from bell inequalities," *Phys. Rev. A*, vol. 87, p. 012335, Jan 2013.

[108] M. J. Hall, "Imprecise measurements and non-locality in quantum mechanics," *Physics Letters A*, vol. 125, no. 2-3, pp. 89–91, 1987.

[109] N. Gisin, "Quantum cloning without signaling," *Physics Letters A*, vol. 242, no. 1-2, pp. 1–3, 1998.

[110] A. K. Pati and S. L. Braunstein, "Quantum deleting and signalling," *Physics Letters A*, vol. 315, no. 3-4, pp. 208–212, 2003.

[111] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[112] L. Hardy and D. D. Song, "No signalling and probabilistic quantum cloning," *Physics Letters A*, vol. 259, no. 5, pp. 331–333, 1999.

[113] M. Banik, "Measurement incompatibility and Schrödinger-Einstein-Podolsky-Rosen steering in a class of probabilistic theories," *Journal of Mathematical Physics*, vol. 56, p. 052101, 05 2015.

[114] M. Banik, S. Saha, T. Guha, S. Agrawal, S. S. Bhattacharya, A. Roy, and A. S. Majumdar, "Constraining the state space in any physical theory with the principle of information symmetry," *Phys. Rev. A*, vol. 100, p. 060101, Dec 2019.

[115] S. S. Bhattacharya, S. Saha, T. Guha, and M. Banik, "Nonlocality without entanglement: Quantum theory and beyond," *Phys. Rev. Res.*, vol. 2, p. 012068, Mar 2020.

[116] S. Saha, S. S. Bhattacharya, T. Guha, S. Halder, and M. Banik, "Advantage of quantum theory over nonclassical models of communication," *Annalen der Physik*, vol. 532, no. 12, p. 2000334, 2020.

[117] S. Saha, T. Guha, S. S. Bhattacharya, and M. Banik, "Quantum theory is exclusive: a distributed computing setup," *arXiv:2012.05781*, 2021.

[118] M. K, T. Muruganandan, S. G. Naik, T. Guha, M. Banik, and S. Saha, "Bipartite polygon models: entanglement classes and their nonlocal behaviour," *arXiv:2205.05415*, 2022.

[119] M. Krumm, H. Barnum, J. Barrett, and M. P. Müller, "Thermodynamics and the structure of quantum theory," *New Journal of Physics*, vol. 19, p. 043025, apr 2017.

[120] G. Carcassi, L. Maccone, and C. A. Aidala, “Four postulates of quantum mechanics are three,” *Phys. Rev. Lett.*, vol. 126, p. 110402, Mar 2021.

[121] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[122] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without bell’s theorem,” *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992.

[123] C. H. Bennett and S. J. Wiesner, “Communication via one- and two-particle operators on einstein-podolsky-rosen states,” *Phys. Rev. Lett.*, vol. 69, pp. 2881–2884, Nov 1992.

[124] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels,” *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar 1993.

[125] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, “Noncommuting mixed states cannot be broadcast,” *Phys. Rev. Lett.*, vol. 76, pp. 2818–2821, Apr 1996.

[126] M. Banik, S. Saha, T. Guha, S. Agrawal, S. S. Bhattacharya, A. Roy, and A. S. Majumdar, “Constraining the state space in any physical theory with the principle of information symmetry,” *Phys. Rev. A*, vol. 100, p. 060101, Dec 2019.

[127] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, “Distinguishability of bell states,” *Phys. Rev. Lett.*, vol. 87, p. 277902, Dec 2001.

[128] J. Walgate and L. Hardy, “Nonlocality, asymmetry, and distinguishing bipartite states,” *Phys. Rev. Lett.*, vol. 89, p. 147901, Sep 2002.

[129] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, “Local distinguishability of multipartite orthogonal quantum states,” *Phys. Rev. Lett.*, vol. 85, pp. 4972–4975, Dec 2000.

[130] M. Horodecki, P. Horodecki, and J. Oppenheim, “Reversible transformations from pure to mixed states and the unique measure of information,” *Physical Review A*, vol. 67, no. 6, p. 062104, 2003.

[131] H. Fan, “Distinguishability and indistinguishability by local operations and classical communication,” *Phys. Rev. Lett.*, vol. 92, p. 177905, Apr 2004.

[132] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, “Distinguishability of maximally entangled states,” *Phys. Rev. A*, vol. 70, p. 022304, Aug 2004.

[133] M. Nathanson, “Distinguishing bipartitite orthogonal states using LOCC: Best and worst cases,” *Journal of Mathematical Physics*, vol. 46, p. 062103, jun 2005.

[134] E. Chitambar, R. Duan, and M.-H. Hsieh, "When do local operations and classical communication suffice for two-qubit state discrimination?," *IEEE Transactions on Information Theory*, vol. 60, no. 3, pp. 1549–1561, 2014.

[135] M. Banik, T. Guha, M. Alimuddin, G. Kar, S. Halder, and S. S. Bhattacharya, "Multicopy adaptive local discrimination: Strongest possible two-qubit nonlocal bases," *Phys. Rev. Lett.*, vol. 126, p. 210505, May 2021.

[136] R. Duan, Y. Feng, Y. Xin, and M. Ying, "Distinguishability of quantum states by separable operations," *IEEE Transactions on Information Theory*, vol. 55, no. 3, pp. 1320–1330, 2009.

[137] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu, "Limitations on separable measurements by convex optimization," *IEEE Transactions on Information Theory*, vol. 61, no. 6, pp. 3593–3604, 2015.

[138] S. M. Cohen, "Class of unambiguous state discrimination problems achievable by separable measurements but impossible by local operations and classical communication," *Physical Review A*, vol. 91, no. 1, p. 012321, 2015.

[139] N. Yu, R. Duan, and M. Ying, "Four locally indistinguishable ququad-ququad orthogonal maximally entangled states," *Phys. Rev. Lett.*, vol. 109, p. 020506, Jul 2012.

[140] N. Yu, R. Duan, and M. Ying, "Distinguishability of quantum states by positive operator-valued measures with positive partial transpose," *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2069–2079, 2014.

[141] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, "Unextendible product bases and bound entanglement," *Phys. Rev. Lett.*, vol. 82, pp. 5385–5388, Jun 1999.

[142] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, "Unextendible product bases, uncompletable product bases and bound entanglement," *Commun. Math. Phys.*, vol. 238, pp. 379–410, July 2003.

[143] J. Niset and N. J. Cerf, "Multipartite nonlocality without entanglement in many dimensions," *Phys. Rev. A*, vol. 74, p. 052103, Nov 2006.

[144] R. Duan, Y. Feng, Z. Ji, and M. Ying, "Distinguishing arbitrary multipartite basis unambiguously using local operations and classical communication," *Phys. Rev. Lett.*, vol. 98, p. 230502, Jun 2007.

[145] J. Calsamiglia, J. I. de Vicente, R. Muñoz Tapia, and E. Bagan, "Local discrimination of mixed states," *Phys. Rev. Lett.*, vol. 105, p. 080504, Aug 2010.

[146] S. Bandyopadhyay, "More nonlocality with less purity," *Phys. Rev. Lett.*, vol. 106, p. 210402, May 2011.

[147] E. Chitambar, R. Duan, and M.-H. Hsieh, "When do local operations and classical communication suffice for two-qubit state discrimination?," *IEEE Transactions on Information Theory*, vol. 60, no. 3, pp. 1549–1561, 2014.

[148] S. Halder, "Several nonlocal sets of multipartite pure orthogonal product states," *Phys. Rev. A*, vol. 98, p. 022303, Aug 2018.

[149] M. Demianowicz and R. Augusiak, "From unextendible product bases to genuinely entangled subspaces," *Phys. Rev. A*, vol. 98, p. 012313, Jul 2018.

[150] S. Halder, M. Banik, S. Agrawal, and S. Bandyopadhyay, "Strong quantum nonlocality without entanglement," *Phys. Rev. Lett.*, vol. 122, p. 040403, Feb 2019.

[151] S. Halder, M. Banik, and S. Ghosh, "Family of bound entangled states on the boundary of the peres set," *Phys. Rev. A*, vol. 99, p. 062329, Jun 2019.

[152] S. Agrawal, S. Halder, and M. Banik, "Genuinely entangled subspace with all-encompassing distillable entanglement across every bipartition," *Phys. Rev. A*, vol. 99, p. 032335, Mar 2019.

[153] S. Rout, A. G. Maity, A. Mukherjee, S. Halder, and M. Banik, "Genuinely nonlocal product bases: Classification and entanglement-assisted discrimination," *Phys. Rev. A*, vol. 100, p. 032321, Sep 2019.

[154] S. S. Bhattacharya, S. Saha, T. Guha, and M. Banik, "Nonlocality without entanglement: Quantum theory and beyond," *Phys. Rev. Res.*, vol. 2, p. 012068, Mar 2020.

[155] M. Banik, T. Guha, M. Alimuddin, G. Kar, S. Halder, and S. S. Bhattacharya, "Multicopy adaptive local discrimination: Strongest possible two-qubit nonlocal bases," *Phys. Rev. Lett.*, vol. 126, p. 210505, May 2021.

[156] S. Rout, A. G. Maity, A. Mukherjee, S. Halder, and M. Banik, "Multiparty orthogonal product states with minimal genuine nonlocality," *Phys. Rev. A*, vol. 104, p. 052433, Nov 2021.

[157] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, "Hiding bits in bell states," *Phys. Rev. Lett.*, vol. 86, pp. 5807–5810, Jun 2001.

[158] T. Eggeling and R. F. Werner, "Hiding classical data in multipartite quantum states," *Phys. Rev. Lett.*, vol. 89, p. 097905, Aug 2002.

[159] W. Matthews, S. Wehner, and A. Winter, "Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding," *Commun. Math. Phys.*, vol. 291, pp. 813–843, Nov. 2009.

[160] C. W. Helstrom, "Quantum detection and estimation theory," *J. Stat. Phys.*, vol. 1, no. 2, pp. 231–252, 1969.

[161] A. S. Holevo, “Statistical decision theory for quantum systems,” *J. Multivar. Anal.*, vol. 3, pp. 337–394, Dec. 1973.

[162] H. Yuen, R. Kennedy, and M. Lax, “Optimum testing of multiple hypotheses in quantum detection theory,” *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 125–134, 1975.

[163] G. Chiribella, G. M. D’Ariano, and P. Perinotti, “Quantum circuit architecture,” *Phys. Rev. Lett.*, vol. 101, p. 060401, Aug 2008.

[164] M. Piani and J. Watrous, “All entangled states are useful for channel discrimination,” *Phys. Rev. Lett.*, vol. 102, p. 250501, Jun 2009.

[165] G. Chiribella, “Perfect discrimination of no-signalling channels via quantum superposition of causal structures,” *Phys. Rev. A*, vol. 86, p. 040301, Oct 2012.

[166] C. Hirche, “Quantum Network Discrimination,” *Quantum*, vol. 7, p. 1064, July 2023.

[167] S. Pirandola, R. Laurenza, C. Lupo, and J. L. Pereira, “Fundamental limits to quantum channel discrimination,” *Npj Quantum Inf.*, vol. 5, June 2019.

[168] R. Takagi, B. Regula, K. Bu, Z.-W. Liu, and G. Adesso, “Operational advantage of quantum resources in subchannel discrimination,” *Phys. Rev. Lett.*, vol. 122, p. 140402, Apr 2019.

[169] R. Takagi and B. Regula, “General resource theories in quantum mechanics and beyond: Operational characterization via discrimination tasks,” *Phys. Rev. X*, vol. 9, p. 031053, Sep 2019.

[170] G. Chiribella, M. Banik, S. S. Bhattacharya, T. Guha, M. Alimuddin, A. Roy, S. Saha, S. Agrawal, and G. Kar, “Indefinite causal order enables perfect quantum communication with zero capacity channels,” *New J. Phys.*, vol. 23, p. 033039, Mar. 2021.

[171] S. S. Bhattacharya, A. G. Maity, T. Guha, G. Chiribella, and M. Banik, “Random-receiver quantum communication,” *PRX Quantum*, vol. 2, p. 020350, Jun 2021.

[172] N. Yu, R. Duan, and M. Ying, “Distinguishability of quantum states by positive operator-valued measures with positive partial transpose,” *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2069–2079, 2014.

[173] R. Duan, Y. Feng, Y. Xin, and M. Ying, “Distinguishability of quantum states by separable operations,” *IEEE Transactions on Information Theory*, vol. 55, no. 3, pp. 1320–1330, 2009.

[174] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, “Quantum nonlocality without entanglement,” *Phys. Rev. A*, vol. 59, pp. 1070–1091, Feb 1999.

[175] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, "Local distinguishability of multipartite orthogonal quantum states," *Phys. Rev. Lett.*, vol. 85, pp. 4972–4975, Dec 2000.

[176] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, "Distinguishability of bell states," *Phys. Rev. Lett.*, vol. 87, p. 277902, Dec 2001.

[177] J. Walgate and L. Hardy, "Nonlocality, asymmetry, and distinguishing bipartite states," *Phys. Rev. Lett.*, vol. 89, p. 147901, Sep 2002.

[178] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, "Distinguishability of maximally entangled states," *Phys. Rev. A*, vol. 70, p. 022304, Aug 2004.

[179] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, "Local indistinguishability: More nonlocality with less entanglement," *Phys. Rev. Lett.*, vol. 90, p. 047902, Jan 2003.

[180] J. Watrous, "Bipartite subspaces having no bases distinguishable by local operations and classical communication," *Phys. Rev. Lett.*, vol. 95, p. 080505, Aug 2005.

[181] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani, "Bounds on multipartite entangled orthogonal state discrimination using local operations and classical communication," *Phys. Rev. Lett.*, vol. 96, p. 040501, Feb 2006.

[182] E. Chitambar and M.-H. Hsieh, "Revisiting the optimal detection of quantum information," *Phys. Rev. A*, vol. 88, p. 020302, Aug 2013.

[183] N. Yu, R. Duan, and M. Ying, "Four locally indistinguishable ququad-ququad orthogonal maximally entangled states," *Phys. Rev. Lett.*, vol. 109, p. 020506, Jul 2012.

[184] S. Bandyopadhyay, S. Ghosh, and G. Kar, "LOCC distinguishability of unilaterally transformable quantum states," *New J. Phys.*, vol. 13, p. 123013, Dec. 2011.

[185] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu, "Limitations on separable measurements by convex optimization," *IEEE Transactions on Information Theory*, vol. 61, no. 6, pp. 3593–3604, 2015.

[186] A. Cosentino and V. Russo, "Small sets of locally indistinguishable orthogonal maximally entangled states," arXiv:1307.3232v2 [quant-ph], 2014.

[187] M. Nathanson, "Distinguishing bipartitite orthogonal states using LOCC: Best and worst cases," *J. Math. Phys.*, vol. 46, p. 062103, June 2005.

[188] T. Singal, R. Rahaman, S. Ghosh, and G. Kar, "Necessary condition for local distinguishability of maximally entangled states: Beyond orthogonality preservation," *Phys. Rev. A*, vol. 96, p. 042314, Oct 2017.

[189] W. H. Zurek, "Quantum darwinism," *Nature Physics*, vol. 5, p. 181–188, Mar. 2009.

[190] J. von Neumann, *Mathematical Foundations of Quantum Mechanics: New Edition*. Princeton University Press, Mar. 2018.

[191] P. A. M. Dirac, *The Principles of Quantum Mechanics*. Oxford: Clarendon, 1958.

[192] J. M. Jauch, *Foundations of quantum mechanics*. A-W series in advanced physics, Reading, Mass.: Addison-Wesley Pub. Co, 1968.

[193] A. Acín, R. Augusiak, D. Cavalcanti, C. Hadley, J. K. Korbicz, M. Lewenstein, L. Masanes, and M. Piani, "Unified framework for correlations in terms of local quantum observables," *Phys. Rev. Lett.*, vol. 104, p. 140404, Apr 2010.

[194] E. P. Lobo, S. G. Naik, S. Sen, R. K. Patra, M. Banik, and M. Alimuddin, "Certifying beyond quantumness of locally quantum no-signaling theories through a quantum-input bell test," *Phys. Rev. A*, vol. 106, p. L040201, Oct 2022.

[195] F. Buscemi, "All entangled quantum states are nonlocal," *Phys. Rev. Lett.*, vol. 108, p. 200401, May 2012.

[196] S. G. Naik, E. P. Lobo, S. Sen, R. K. Patra, M. Alimuddin, T. Guha, S. S. Bhattacharya, and M. Banik, "Composition of multipartite quantum systems: Perspective from timelike paradigm," *Phys. Rev. Lett.*, vol. 128, p. 140401, Apr 2022.

[197] N. Brunner, M. Kaplan, A. Leverrier, and P. Skrzypczyk, "Dimension of physical systems, information processing, and thermodynamics," *New Journal of Physics*, vol. 16, p. 123050, Dec. 2014.

[198] A. Wilce, "Quantum Logic and Probability Theory," in *The Stanford Encyclopedia of Philosophy* (E. N. Zalta and U. Nodelman, eds.), Metaphysics Research Lab, Stanford University, Summer 2024 ed., 2024.

[199] W. K. Wootters, "Quantum mechanics without probability amplitudes," *Foundations of Physics*, vol. 16, p. 391–405, Apr. 1986.

[200] M. P. Müller, O. C. O. Dahlsten, and V. Vedral, "Unifying typical entanglement and coin tossing: on randomization in probabilistic theories," *Communications in Mathematical Physics*, vol. 316, p. 441–487, Oct. 2012.

[201] H. Arai, Y. Yoshida, and M. Hayashi, "Perfect discrimination of non-orthogonal separable pure states on bipartite system in general probabilistic theory," *Journal of Physics A: Mathematical and Theoretical*, vol. 52, p. 465304, Oct. 2019.

[202] M.-D. Choi, "Completely positive linear maps on complex matrices," *Linear Algebra and its Applications*, vol. 10, p. 285–290, June 1975.

[203] A. Jamiołkowski, “Linear transformations which preserve trace and positive semidefiniteness of operators,” *Reports on Mathematical Physics*, vol. 3, p. 275–278, Dec. 1972.

[204] M. Horodecki, P. Horodecki, and R. Horodecki, “Separability of mixed quantum states: Linear contractions and permutation criteria,” *Open Systems &; Information Dynamics*, vol. 13, p. 103–111, Mar. 2006.

[205] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories,” *Physical Review Letters*, vol. 23, p. 880–884, Oct. 1969.

[206] S. J. Freedman and J. F. Clauser, “Experimental test of local hidden-variable theories,” *Physical Review Letters*, vol. 28, p. 938–941, Apr. 1972.

[207] A. Aspect, “Proposed experiment to test the nonseparability of quantum mechanics,” *Physical Review D*, vol. 14, p. 1944–1951, Oct. 1976.

[208] A. Aspect, P. Grangier, and G. Roger, “Experimental tests of realistic local theories via bell’s theorem,” *Physical Review Letters*, vol. 47, p. 460–463, Aug. 1981.

[209] A. Aspect, P. Grangier, and G. Roger, “Experimental realization of einstein-podolsky-rosen-bohmgedankenexperiment: A new violation of bell’s inequalities,” *Physical Review Letters*, vol. 49, p. 91–94, July 1982.

[210] A. Aspect, J. Dalibard, and G. Roger, “Experimental test of bell’s inequalities using time- varying analyzers,” *Physical Review Letters*, vol. 49, p. 1804–1807, Dec. 1982.

[211] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, “““event-ready-detectors”” bell experiment via entanglement swapping,” *Physical Review Letters*, vol. 71, p. 4287–4290, Dec. 1993.

[212] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, “Experimental entanglement swapping: Entangling photons that never interacted,” *Physical Review Letters*, vol. 80, p. 3891–3894, May 1998.

[213] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, “Violation of bell’s inequality under strict einstein locality conditions,” *Physical Review Letters*, vol. 81, p. 5039–5043, Dec. 1998.

[214] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, “Observation of three-photon greenberger-horne-zeilinger entanglement,” *Physical Review Letters*, vol. 82, p. 1345–1349, Feb. 1999.

[215] V. Scarani, “The device-independent outlook on quantum physics (lecture notes on the power of bell’s theorem)see also arXiv:1303.3081 [quant-ph]],” 2013.

[216] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Physical Review Letters*, vol. 67, p. 661–663, Aug. 1991.

[217] J. Barrett, L. Hardy, and A. Kent, “No signaling and quantum key distribution,” *Physical Review Letters*, vol. 95, June 2005.

[218] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, “Device-independent quantum key distribution secure against collective attacks,” *New Journal of Physics*, vol. 11, p. 045021, Apr. 2009.

[219] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, “Random numbers certified by bell’s theorem,” *Nature*, vol. 464, p. 1021–1024, Apr. 2010.

[220] R. Colbeck and A. Kent, “Private randomness expansion with untrusted devices,” *Journal of Physics A: Mathematical and Theoretical*, vol. 44, p. 095305, Feb. 2011.

[221] R. Colbeck and R. Renner, “Free randomness can be amplified,” *Nature Physics*, vol. 8, p. 450–453, May 2012.

[222] A. Mukherjee, A. Roy, S. S. Bhattacharya, S. Das, M. R. Gazi, and M. Banik, “Hardy’s test as a device-independent dimension witness,” *Physical Review A*, vol. 92, Aug. 2015.

[223] A. Pappa, N. Kumar, T. Lawson, M. Santha, S. Zhang, E. Diamanti, and I. Kerenidis, “Nonlocality and conflicting interest games,” *Physical Review Letters*, vol. 114, Jan. 2015.

[224] A. Roy, A. Mukherjee, T. Guha, S. Ghosh, S. S. Bhattacharya, and M. Banik, “Nonlocal correlations: Fair and unfair strategies in bayesian games,” *Physical Review A*, vol. 94, Sept. 2016.

[225] P. E. Frenkel and M. Weiner, “On entanglement assistance to a noiseless classical channel,” *Quantum*, vol. 6, p. 662, Mar. 2022.

[226] R. K. Patra, S. G. Naik, E. P. Lobo, S. Sen, T. Guha, S. S. Bhattacharya, M. Alimuddin, and M. Banik, “Classical analogue of quantum superdense coding and communication advantage of a single quantum system,” *Quantum*, vol. 8, p. 1315, Apr. 2024.

[227] M. Forster, S. Winkler, and S. Wolf, “Distilling nonlocality,” *Physical Review Letters*, vol. 102, Mar. 2009.

[228] N. Brunner and P. Skrzypczyk, “Nonlocality distillation and postquantum theories with trivial communication complexity,” *Physical Review Letters*, vol. 102, Apr. 2009.

[229] A. J. Short, “No deterministic purification for two copies of a noisy entangled state,” *Physical Review Letters*, vol. 102, May 2009.

[230] N. Brunner, D. Cavalcanti, A. Salles, and P. Skrzypczyk, “Bound nonlocality and activation,” *Physical Review Letters*, vol. 106, Jan. 2011.

[231] M. Forster, “Bounds for nonlocality distillation protocols,” *Physical Review A*, vol. 83, June 2011.

[232] P. Høyer and J. Rashid, “Optimal protocols for nonlocality distillation,” *Physical Review A*, vol. 82, Oct. 2010.

[233] J. Rashid, “Limits and consequesnces of nonlocality distillation,” 2012.

[234] P. HØYER and J. RASHID, “Quantum nonlocal boxes exhibit stronger distillability,” *Modern Physics Letters A*, vol. 28, p. 1330012, June 2013.

[235] H. Ebbe and S. Wolf, “Multi-user non-locality amplification,” *IEEE Transactions on Information Theory*, vol. 60, p. 1159–1167, Feb. 2014.

[236] J. Tuziemski and K. Horodecki, “On the non-locality of tripartite non-signaling boxes emerging from wirings,” 2014.

[237] S. Beigi and A. Gohari, “Monotone measures for non-local correlations,” *IEEE Transactions on Information Theory*, vol. 61, p. 5185–5208, Sept. 2015.

[238] G. Brassard, B. Salwey, and S. Wolf, “Non-locality distillation as cryptographic game,” in *2015 IEEE Information Theory Workshop (ITW)*, IEEE, Apr. 2015.

[239] S. G. A. Brito, M. G. M. Moreno, A. Rai, and R. Chaves, “Nonlocality distillation and quantum voids,” *Physical Review A*, vol. 100, July 2019.

[240] G. Eftaxias, M. Weilenmann, and R. Colbeck, “Advantages of multicopy nonlocality distillation and its application to minimizing communication complexity,” *Phys. Rev. Lett.*, vol. 130, p. 100201, Mar 2023.

[241] B. S. Tsirel'son, “Quantum analogues of the bell inequalities. the case of two spatially separated domains,” *Journal of Soviet Mathematics*, vol. 36, p. 557–570, Feb. 1987.

[242] L. J. Landau, “Empirical two-point correlation functions,” *Foundations of Physics*, vol. 18, p. 449–460, Apr. 1988.

[243] L. Masanes, “Necessary and sufficient condition for quantum-generated correlations,” 2003.

[244] M. Navascués, S. Pironio, and A. Acín, “Bounding the set of quantum correlations,” *Physical Review Letters*, vol. 98, Jan. 2007.

[245] M. Navascués, S. Pironio, and A. Acín, “A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations,” *New Journal of Physics*, vol. 10, p. 073013, July 2008.

[246] W. Slofstra, “Tsirelson's problem and an embedding theorem for groups arising from non-local games,” *Journal of the American Mathematical Society*, vol. 33, p. 1–56, Sept. 2019.

[247] W. SLOFSTRA, "The set of quantum correlations is not closed," *Forum of Mathematics, Pi*, vol. 7, 2019.

[248] K. Dykema, V. I. Paulsen, and J. Prakash, "Non-closure of the set of quantum correlations via graphs," *Communications in Mathematical Physics*, vol. 365, p. 1125–1142, Jan. 2019.

[249] L. Hardy, "Nonlocality for two particles without inequalities for almost all entangled states," *Physical Review Letters*, vol. 71, p. 1665–1668, Sept. 1993.

[250] J. L. Cereceda *Foundations of Physics Letters*, vol. 13, no. 5, p. 427–442, 2000.

[251] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, "Information causality as a physical principle," *Nature*, vol. 461, pp. 1101–1104, Oct 2009.

[252] N. Miklin and M. Pawłowski, "Information causality without concatenation," *Physical Review Letters*, vol. 126, June 2021.

[253] B. S. Cirel'son, "Quantum generalizations of bell's inequality," *Letters in Mathematical Physics*, vol. 4, p. 93–100, Mar. 1980.

[254] M. Navascués and H. Wunderlich, "A glance beyond the quantum model," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 466, p. 881–890, Nov. 2009.

[255] E. Chitambar and G. Gour, "Quantum resource theories," *Reviews of Modern Physics*, vol. 91, Apr. 2019.

[256] J. I. de Vicente, "On nonlocality as a resource theory and nonlocality measures," *Journal of Physics A: Mathematical and Theoretical*, vol. 47, p. 424017, Oct. 2014.

[257] E. Wolfe, D. Schmid, A. B. Sainz, R. Kunjwal, and R. W. Spekkens, "Quantifying bell: the resource theory of nonclassicality of common-cause boxes," *Quantum*, vol. 4, p. 280, June 2020.

[258] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical Review Letters*, vol. 76, p. 722–725, Jan. 1996.