universität wien

DISSERTATION

Titel der Dissertation

Generic Probabilistic Theories– Reconstruction of quantum theory

Verfasser

Borivoje Dakić

angestrebter akademischer Grad

Doktor der Naturwissenschaften

Wien, im Juli 2011

Studienkennzahl laut Studienblatt: A 091 411

Dissertationsgebiet laut Studienblatt: Physik

Betreuer: ao. Univ.-Prof. Časlav Brukner

Contents

Abstract

This thesis is a collection of projects done under supervision of Prof. Časlav Brukner. It is divided into two main chapters. First part is based on the instrumental approach to quantum mechanics with the main objective to identify and mark the exclusive features of quantum theory in a broad class of probabilistic theories. The second part investigates the non-classical features of quantum mechanics including quantum statistics, quantum correlations and quantum simulations.

It is fair to say that we still lack intuitive clear and broadly accepted physical principles that are a groundbasis of quantum theory. This shortfall is the main reason for today's coexistence of various interpretations of quantum theory, some of which even use mutually exclusive concepts. One of the main objectives in the first chapter was to specify theories that describe systems with fundamentally *limited information content* and therefore necessarily give a probabilistic description. With "limited information content of the system" we understand a fundamental restriction on how much information about the state preparation can be decoded in the measurement. What was found is the whole hierarchy of theories that share this property with quantum and classical probability theory. The two theories separate from the full class of the probabilistic theories by adopting additional assumptions: *locality* and *reversibility*. With the "locality" principle we assume that a global state of a composite system can be learned trough the statistics of individual systems, whereas the "reversibility" principle states that any two pure state can be connected by a reversible transformation. Finally, quantum theory is separated by the requirement that the set of reversible transformations is *continuous*. In addition, one of the basic quantum concepts, the complementarity principle was investigated through so- called *mutually unbiased bases* relating them to the known mathematical problem of orthogonal Latin squares.

A plausible classical description of quantum statistics requires counterintuitive concepts such as "quantum non-locality" and "contextuality". The part of the second chapter deals with another question, i.e. the "cost" in terms of resources for a plausible classical description. It was found that classical simulation of quantum statistics requires a *polynomial number of classical resources* (hidden-variables) in terms of number of measurement settings. Furthermore, the model confirms, in a proper limit, the known result that quantum mechanics is indeed the most optimal description of itself.

Quantum correlations are responsible for "quantum non-locality", as well as com-

putational speedups and quantum information processing. There are examples of quantum information tasks that do not necessarily require entanglement. Therefore it is fair to say that "quantumness" of the correlations is not equivalent to entanglement. The part of the second chapter deals with the question of "non-classicality" of quantum correlations, captured by *quantum discord*. The main result gives an experimentally friendly *necessary and sufficient condition* for non-zero quantum discord. Furthermore the analysis of the resources in a mixed-state quantum computation scenario is provided and shows that the role of quantum discord in quantum information processing still remains unclear.

Finally, the part of the last chapter investigates *quantum simulations*, both theoretically and experimentally. Quantum simulators provide a platform to mimic the dynamics of another quantum system that is infeasible for simulations on a classical computer. What is presented is the framework for the experimental realization of a *small-size photonic quantum simulator* that is capable of simulating a frustrated spin tetramer. The full dynamics and simulation of the ground state adiabatic evolution is achieved by employing entangled photon pairs, tunable quantum gates and measurement induced nonlinearities.

Zusammenfassung

Diese Dissertation besteht aus einer Sammlung von Projekten, welche unter der Betreuung von Prof. Časlav Brukner durchgeführt wurden. Die Arbeit gliedert sich in zwei Hauptteile. Der erste Teil widmet sich dem operativen Zugang zu der Quantenmechanik. Die Hauptaufgabe besteht hierbei darin, die exklusiven Eigenschaften der Quantenmechanik in einer größeren Klasse probabilistischer Theorien zu identifizieren. Der zweite Teil beschäftigt sich mit der typischen Charakteristik der Quantenphysik, wie der Quantenstatistik, den Quantenkorellationen und Quantensimulationen.

Man kann sicherlich sagen, dass wir derzeit noch keine der Intuition zugänglichen, und allgemein akzeptierte physikalische Prinzipien haben, welche die Grundlage der Quantemechanik darstellen. Der Mangel solcher Prinzipien ist die Hauptursache für die derzeitige Koexistenz von vielen Interpretationen der Quantenmechanik, die von Konzepten Gebrauch machen, welche sich gegenseitig ausschließen. Eine Hauptaufgabe des ersten Kapitel besteht in der Spezifizierung von Theorien mit grundsätzlich beschränkten Informationsgehalt, welche aufgrund dieser Tatsache eine probabilistische Beschreibung besitzen. Unter dem "beschränkten Informationsgehalt eines Systems", verstehen wir eine grundsätzliche Beschränkung der Information welche durch eine Messung über die Preparation eines Zustandes gewonnen werden kann. Ein Ergebnis dieses Kapitels ist die Charakterisierung der gesamten Hierarchie der Theorien, welchen diese Eigenschaft gemein sind. Auf den unteren Stufen dieser Hierarchie sind die klassische, wie auch die quantenmechanische Wahrscheinlichkeitstheorie enthalten. Um die Quantentheorie und klassische Theorie von der ganzen Klasse der Wahrscheinlichkeitstheorien zu unterscheiden, wurden zusätzliche Annahmen getroffen. Diese Annahmen sind *Lokalität* und *Umkehrbarkeit*. Unter dem Prinzip der *Lokalität* verstehen wir, dass der Gesamtzustand eines Systems durch die Statistik der individuellen Untersysteme rekonstruiert werden kann. Das Prinzip der *Umkehrbarkeit* drückt aus, dass zwei reine Zustände immer durch eine umkehrbare Transformation auseinander hervorgehen. Darüber hinaus, wurde ein weiteres fundamentales Prinzip der Quantenmechanik, das *Komplementaritätsprinzip*, mittels "mutually unbiased bases" untersucht. Es wurde eine Verbindung zu dem bekannten mathematischen Problem der orthogonalen lateinischen Quadraten hergestellt.

Eine plausible klassische Beschreibung der Quantenstatistik benötigt nicht eingängige Konzepte wie die quantenmechanische "Nicht-lokalität" und "Kontextualität". Der zweite Teil dieser Dissertation widmet sich einer weiteren Frage, der Frage nach dem

“Kostenaufwand” im Sinne der beschreibenden Ressourcen welche eine plausible klassische Beschreibung der Quantenstatistik zulassen. Es wurde gezeigt, dass die klassische Simulation der Quantenstatistik nur eine polynomiale Anzahl an Ressourcen, so genannte verborgene Variablen, für die Verschiedenen Messeinstellungen benötigt. Darüber hinaus bestätigt dieses Simulationsmodell auch, dass in einem vernünftigen Limes, die optimale Beschreibung der Quantenstatistik die Quantenmechanik selbst ist.

Quantenkorrelationen sind für die quantenmechanische Nicht-lokalität verantwortlich, wie auch für den “computational speedup” in der Quanten Informationsverarbeitung. Es gibt Beispiele von Quanteninformationsprotokollen, die mit Sicherheit kein Verschränkung nutzen aber dennoch von quantenmechanischen Korrelationen Gebrauch machen. Es ist daher nicht möglich die Korrelationen in ihrer allgemeinen Form mit der Verschränkung gleich zu setzen. Das zweite Kapitel behandelt die Frage der nicht-klassischen Eigenschaften der Quantenkorrelationen welche durch den “quantum discord” beschrieben werden. Das Hauptergebnis ist eine experimentell einfach zugängliche, hinreichend wie auch notwendige, Bedingung für nicht-verschwindenden quantum discord. Darüber hinaus stellen wir eine Analyse der Ressourcen in “mixed-state quantum computation” vor, welche zeigt, dass die Rolle des “quantum discord” in der Quanteninformationsverarbeitung weiterhin unklar ist.

Schließlich widmet sich das letzte Kapitel dieses Teils der Untersuchung von Quantensimulationen, sowohl theoretisch als auch experimentell. Quantensimulatoren können verwendet werden um die Zeitenwicklung eines bestimmten quantenmechanischen system darzustellen, eine Aufgabe, die für klassische Computer sehr schwierig ist. Es wird ein kleiner photonischer Quantensimulator vorgestellt, der in der Lage ist ein frustriertes Spin Tetramer zu simulieren. Die Simulation macht von verschränkten Photonpaaren, verstellbaren Quantengattern und durch Messung induzierten Nichtlinearitäten Gebrauch.

Acknowledgments

I owe special thanks to my supervisor Prof. Časlav Brukner for his support and encouragement during my PhD studies. Many thanks to the TAC (Thesis Advisory Committee) members Prof. Frank Verstraete and Prof. Alan Aspuru-Guzik. I would like to thank whole Vienna Quantum Foundations and Quantum Information Theory Group for excellent (not only scientific) discussions. Many thanks to my colleagues and collaborators Xiaosong Ma, Philip Walther, Tomasz Paterek and Vlatko Vedral for already longstanding and plentiful collaboration. I owe special thanks to Prof. Markus Arndt, CoQuS administrative stuff and Austrian Science Foundation (FWF) for leading, organizing and supporting CoQuS doctoral program.

I acknowledge support by the FWF project CoQuS (No. W1210-N16), the FWF Project No. P19570-N16, the European Commission Project QAP (No. 015846), Foundational Questions Institute (FQXi), and Q-ESSENCE Project (No. 248095).

List of Publications

Articles in refereed journals:

1. B. Dakić and Č. Brukner, *Quantum Theory and Beyond: Is Entanglement Special?* In Deep Beauty: Understanding the Quantum World Through Mathematical Innovation, edited by H. Halvorson, Cambridge University Press, 2011.

2. T. Paterek, B. Dakić, and Č. Brukner, *Reply to "Comment on 'Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models' "*, Phys. Rev. A **83**, 036102 (2011).

3. X. Ma, B. Dakić, W. Naylor, A. Zeilinger, and P. Walther , *Quantum simulation of the wavefunction to probe frustrated Heisenberg spin systems*, Nature Physics **7**, 399–405 (2011).

4. B. Dakić, V. Vedral, and Č. Brukner, *Necessary and sufficient condition for non-zero quantum discord* , Phys. Rev. Lett. **105**, 190502 (2010).

5. T. Paterek, B. Dakić, and Č. Brukner, *Theories of systems with limited information content*, New J. Phys. **12**, 053037 (2010).

6. B. Dakić, Milosević, and M. Damnjanović, *Generalized Bloch states and potentials of nanotubes and other quasi-1D systems II*, J. Phys. A: Math. Gen. **42**, 125202 (2009).

7. T. Paterek, B. Dakić, and Č. Brukner, *Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models*, Phys. Rev. A **79**, 012109 (2009).

8. B. Dakić, M. Suvakov, T. Paterek, and Č. Brukner, *Efficient Hidden-Variable Simulation of Measurements in Quantum Experiments*, Phys. Rev. Lett. **101**, 190402(ES) (2008).

9. B. Dakić, Milosević, and M. Damnjanović, *Generalized Bloch states and potentials of nanotubes and other quasi-1D systems*, J. Phys. A: Math. Gen. **42** 11833-11846 (2006).

10. E. Dobardzić, I. Milosević, B. Dakić, and M. Damnjanović, *Raman and infrared-active modes in MS_2 nanotubes (M=Mo,W)*, Phys. Rev. B **74**, 033403 (2006).

11. E. Dobardzić, B. Dakić, M. Damnjanović, and I. Milosević, *Zero m phonons in MoS_2 nanotubes*, Phys. Rev. B **71**, 121405(R) (2005).

Conference proceedings:

1. E. Dobardzić, I. Milosević, B. Dakić, and M. Damnjanović, *Phonons in MS_2 (M = Mo;W) nanotubes*, AIP Conf. Proc. **899**, 383–384 (2007).

2. E. Dobardzić, I. Milosević, B. Dakić, T. Mihaljev and M. Damnjanović, *MoS_2 tubes: electronic and optical properties*, J. Phys.: Conf. Ser. **92**, 012141 (2007).

Chapter 1

Generic probabilistic theories

Quantum formalism teaches us that a physical state is represented by density operator, a curious beast that operates in a Hilbert space. Unfortunately it does not provide us with an answer why is so, it only gives a prescription how to compute the probabilities of the measurement outcomes. The lack of a clear operational interpretation of quantum formalism indicates that there might be a possibility for some deeper foundations of the theory. For many years there has been lot of attempts to "embed" quantum mechanics in a more complete theory, such as various hidden-variable theories [19, 120, 92], collapse models [77, 110, 109, 60, 151, 149] and non-linear variants of the Schrödinger equation [22, 167, 169, 75]. All of them tempt to save one or another feature of classical physics, like determinism or localizability. Since quantum mechanics successfully survived experimental tests against such models, it has become clear that it should have a status of genuine probabilistic theory. On the other hand, from the operational point of view, quantum theory is just one among the many of probabilistic theories that one can think of. A vast majority of them share the same features with quantum theory such as no-signaling and no-cloning [14, 15] or monogamy of the correlations [163].

Still there is no global consensus among the physicist what is "typically" quantum. For example, no-signaling principle does not forbid the possibility of superstrong correlations, known as Popescu-Rorlich boxes [157]. But, why the superstrong correlations do not appear in nature? One answer to this question could be: because, they are prohibited by the Hilbert space formalism. For a pragmatist, such a statement is very naive, because *"quantum phenomena do not occur in a Hilbert space, they occur in a laboratory"*(A. Peres) [154].

In this chapter, an instrumentalist (operational) approach has been employed to study various topics. It is organized as follows:

In the first section, the principle of limited information content [197, 39, 40] is investigated from the operational perspective. Although, the set of quantum states is continuous, a finite dimensional quantum system can be used to transfer a finite amount of information only. More precisely, a d-level system contains at most $\log d$ bits of information, which is known as Holevo bound [102]. This can be considered as a fundamental principle of nature – the principle of limited information content. Some basic notions of this idea can be found already in the work of Weizsäcker [185] and the principle itself was further developed by Zeilinger [197]. If the finite amount of information is encoded in the state of system, then the system can reveal with certainty answers to a finite number of questions that are asked in the measurement. Therefore, the uncertainty of the measurement outcomes and the complementarity principle come as natural consequence. The principle is valid both in quantum and classical probability theory. For example, classical bits, and qubits are the two known examples of systems that are fundamentally limited to one bit of information. However, careful analysis shows that these are not the only examples. Whole hierarchy of theories share this feature with quantum and classical probability theory. The limited information content is introduced operationally, through a "blackbox" that can have different configurations. A system is used to probe the blackbox and after being measured it reveals some information about its configuration. The theory is characterized by the maximal number of mutually (complementary) exclusive questions that the system can answer when opposed to a measurement. A theory of a higher order contains all the theories of the lower order, in the same way that a quantum bit contains a classical bit. Furthermore, the computational power of the theories grows with its order as it can be seen trough Deutsch-Josza algorithm [57]. Some basic ingredients of these theories are derived. The systems dimension is computed for a composite systems using the *counting parameter argument* [96]. A possible experimental tests is discussed. It is assumed that an experimentalist posses all the quantum tools and that there exists in nature a genuine source that emits a state that can be described by some higher order theory, i.e. it goes beyond the set of quantum states. Furthermore, it is shown that genuine "non-quantum" evolution can be observed which can be used to detect the order of a theory that describes the source.

In the second section, the question of the existence of complete set of mutually unbiased bases (MUB) [104] in quantum theory is studied. The MUBs are closely related to the principle of complementarity, one of fundamental bases of quantum mechanics. They provide a neat way to encode an information in a physical state. Although, it is well known how to construct them when the system's dimension is prime or power

of prime, for other cases it is suspected that the complete set of MUB does not exist. An interesting connection between this problem and the problem of finding the set of mutually orthogonal Lattin squares (OLS) [66] is found. By applying known results for OLS one can disprove the existence of certain classes of MUBs when the system's dimensions is not a power of prime.

The third section presents the main work of the thesis. It tries to identify the set of physical principles behind quantum formalism. Such an attempt is known as reconstruction of quantum theory. The approach is operational, and it does not address the "ontological background" of quantum theory, for example if there could be a hidden determinism behind probabilities. It is rather phenomenological and gives the set of simple physical axioms from which the quantum formalism can be derived. The general setting involves a typical experimental situation where experimentalist faces preparation, transformation and the measurement device. Different operations can be performed by varying a knob (switch) on each device. The system is released in the preparation device and measured in the measurement device where it activates one of the outcomes, e.g. the "click" is recorded in one of the detectors. After many runs the measurement retrieves the probability. The set of probabilities for a different measurement outcomes define the state of system that is associated to the preparation. In such a scenario quantum theory is just one particular theory among the set of generalized probabilistic theories. What makes the difference between theories is particular set of physical principles from which a particular theory can be derived. For example, both classical and quantum are the theories with reversible dynamics. What can distinguish them is continuous in one case and discrete dynamics in other case [96]. The main objective of the work is to identify the set of an informational-based set of principles that can be used to single out quantum theory. The applied operational approach builds upon the works of Hardy [96] and Barrett [18]. The specific set of axioms on which the present reconstruction is based are: (1) (Information capacity) All systems with information carrying capacity of one bit are equivalent. (2) (Locality) The state of a composite system is completely determined by measurements on its subsystems. (3) (Reversibility) Between any two pure states there exists a reversible transformation. Remarkable, only classical and quantum theory are consistent with these principles. Furthermore, if one requires the transformation from the last assumption to be continuous, one separates quantum theory from the classical probabilistic one. A remarkable result following from the reconstruction is that no probability theory other than quantum theory can exhibit entanglement without contradicting one or more axioms.

1.1 Theories of systems with limited information content

We introduce a hierarchical classification of theories that describe systems with fundamentally limited information content. This property is introduced in an operational way and gives rise to the existence of mutually complementary measurements, i.e. a complete knowledge of future outcome in one measurement is at the expense of complete uncertainty in the others. This is characteristic feature of the theories and they can be ordered according to the number of mutually complementary measurements which is also shown to define their computational abilities. In the theories multipartite states may contain entanglement and tomography with local measurements is possible. The classification includes both classical and quantum theory and also generalized probabilistic theories with higher number of degrees of freedom, for which operational meaning is given. We also discuss thought experiments discriminating standard quantum theory from the generalizations.

Can one find a class of logically conceivable physical theories that all share some fundamental features with quantum mechanics? For example, in gravitational physics, general relativity and Brans-Dicke theory [30] belong to a broad class of relativistic classical theories of gravitation. By contrast, it is often assumed that any modification of quantum mechanics would produce internally inconsistent theories [186].

In this paper we identify a class of quantum-like theories describing systems with limited information content [197, 39, 40]. This limit does not arise from an observer's ignorance about the "true ontic states of reality" [175] — which would be a hidden-variable theory and would have to confront the theorems of Bell [19] and Kochen-Specker [116] — but rather is a fundamental limit. To introduce an operational notion of information content, we insert the system into a "black box", which itself has one of a number of configurations. After leaving the black box, the system is measured to reveal some of the properties of the configuration. The "limited information content of the system" represents the fundamental restriction on how much information about the configuration can be gained in this measurement.

We first consider a system with an information content of one bit, which we call a two-level system [1]. A measurement outcome can only reveal one bit of information, i.e. it can distinguish between two equally-sized subsets of possible configurations, without any possibility of discriminating between further subsets. This gives

[1] Even if more than two detectors are involved in the measurement of such system, it can only reveal one bit of information about the configuration in the black box.

rise to mutually complementary properties of black box configurations and the notion of complementary questions, which are questions about these properties. We study the information gain about these configurations which can be revealed using two-level systems described by different theories. The number of complementary system observables predicted by the theories limits the number of complementary black-box configurations which can be accessed. We use this to identify a hierarchical classification of quantum-like theories. We show that classical physics — with no complementary observables — and quantum physics — with three complementary observables for a qubit — are just two examples of theories within this hierarchy and present examples of other theories. A theory on a particular level of the hierarchy contains all lower-level theories, just as theory of quantum bits contains theory of classical bits.

We investigate the computational capabilities of the new theories in a manner similar to the work on no-signaling theories [133, 124, 18, 15, 17, 16, 183] and show that computational capabilities increase with the level of the theory in the hierarchy. We then consider composite systems, and demonstrate existence of complementary properties of many black boxes which cannot be accessed with (product of) independent subsystems, leading to necessity of entanglement in the corresponding theories. We also show that the number of parameters obtained from complementary measurements on a composite system consisting of many two-level systems agrees with the number of parameters obtained from correlations between complementary local measurements. This fact is a remarkable coincidence since a priori there is nothing in the definition of the hierarchy that hints at it. Finally, we present thought experiments aimed at distinguishing standard quantum theory from the generalized theories.

Other attempts have previously been made to introduce a hierarchy of models that includes both classical and quantum theory. The generalized models exploit different sum-rules for probabilities [172] or explore physical systems described by a number of parameters (sometimes also called "degrees of freedom") different than in quantum mechanics [194, 96, 199, 74, 48]. Our approach is related to the later in that we consider two-level systems with additional degrees of freedom. We show that the principle of limited information content together with an assumption that a system can reveal any of the complementary properties of black box configurations allows only specific values for the number of these degrees. The same number is derived by Wootters [194] and Hardy [96] using parameter counting argument for composite systems. Here, however, it follows already for a single system.

It should be noted that our aim here is not to derive the structure of quantum theory but rather to show alternative models whose parameters also have operational mean-

ing. It is interesting to ask which axioms of standard quantum theory such models defy. Compared with Hardy's axiomatization [96], our models for a single two-level system involve more degrees of freedom than a qubit and therefore include also those theories which Hardy excluded by the simplicity axiom (the simplicity axiom states that one should take the minimal number of degrees of freedom in agreement with other axioms). The probability axiom (in all experiments on a sufficiently big ensemble of systems prepared in the same way, the relative frequencies of measurement outcomes tend to the same values) is fulfilled in our models. The continuity axiom (there exists a continuous reversible transformation on a system between any two pure states of that system), is fulfilled by the presented models of a single system. For multiple two-level systems, assumption of limited information content together with requirement that systems reveal any of complementary properties implies Hardy's axiom about composite systems (local tomography is possible). It states that both the number of levels of a composite system, N, and the number of parameters describing its unnormalized states, K, are products of respective numbers for individual subsystems, i.e. $N = N_A N_B$ and $K = K_A K_B$. It was proved that Hardy's simplicity axiom is redundant [48], i.e. that only classical and quantum theories are in agreement with all other axioms. This implies for the multipartite theories studied here that they have to defy Hardy's subspace axiom (it states that a n-level subsystem of a higher-level system behaves like a system with n levels). This is a consequence of the fact that continuity is fulfilled by the presented models for a single system and therefore the subspace axiom implies continuity for many systems because any two states of a composite system are connected by a continuous transformation, introduced in a single particle case. As we already noted, this would constrain the possible theories to classical and quantum only due to the results of Ref. [48].

1.1.1 Limited information content

Consider the black box illustrated in Fig. 1.1. A Boolean function of a single s-valued argument, $y = f(x)$, with $x = 0, ..., s-1$ and $y = 0, 1$, is realized physically by putting one of two different (classical) objects in each of s different positions inside the box. As a result, there are 2^s different functions $f(x)$ and as many distinguishable configurations of the black box. If all the configurations have the same probability of occurring, s bits of information are necessary to identify a given function. A physical system with information content below s bits cannot therefore distinguish an individual function, but only groups of functions with certain properties.

For example, consider a black box with two positions inside which is probed by

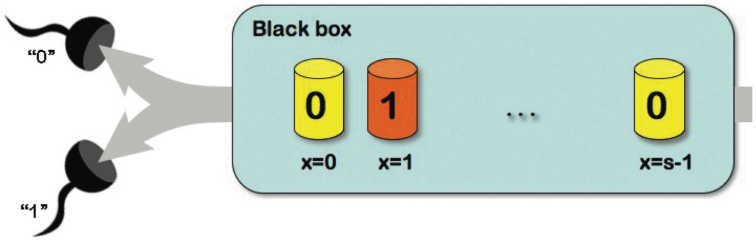

Figure 1.1: The configuration of items inside the black box is a physical realization of a function $y = f(x)$. The value of x is encoded in the position inside the box, whereas the value of y is encoded by putting a yellow ($y = 0$) or orange ($y = 1$) item at position x. A physical system enters the black box from the right, undergoes function-dependent transformations and is finally measured after leaving the box.

a single two-level system. The possible box configurations represent four Boolean functions of the position variable $x = 0, 1$, which can be indexed by $j = 2^1 f(0)+2^0 f(1)$. The readout step reveals one bit of information, splitting the four functions into two equally-sized sets. In this case, one finds three possible splits which can be illustrated by the three rows of the following tables (symbol $\oplus$ denotes addition modulo two):

0	1	2	3
0	2	1	3
0	3	1	2

$a = 0$		$a = 1$	
00	01	10	11
00	10	01	11
00	11	01	10

$f(0) = a?$
$f(1) = a?$
$f(0) \oplus f(1) = a?$

(1.1)

The table on the left-hand side shows the index j [2], and the middle table shows the functional values ordered as pairs $f(0)\,f(1)$. The table on the right-hand side gives the three complementary questions about the properties of the functions. They are answered by the functions in the left and right column of the middle table (left column $\rightarrow$ answer 0, right column $\rightarrow$ answer 1). We shall refer to such tables as the complementarity tables [145].

The black box forms a bridge between the abstract mathematical construction of complementarity tables and the physical world. The physical system can be used to probe the box configuration by subjecting it to configuration-dependent transformations. An appropriate measurement can then be used to identify the subset to which the configuration belongs. Two-level systems described by different physical theories

[2] An equivalent table was introduced by Spekkens within a different interpretational approach [175]. There, an individual quantum system is assumed to be in an ontic state, while here only the (classical) black box is in a well-defined "ontic" state.

allow one to answer different numbers of complementary questions.

In the simplest case, $s = 1$, the black box contains only one position. It is convenient to think of the value $f(0) = 0$ as an empty position and $f(0) = 1$ as an occupied position. This configuration can be revealed by a classical bit, which by definition can only either be flipped or left untouched. If its state is flipped only when the object is present, then knowing the initial and final states of the bit completely determines the box configuration, $f(0)$. This is possible because the box stores only one bit.

The next case, with two positions inside the black box, is qualitatively different because complementary questions now arise. A classical bit can no longer be used to answer any one of them. This can, however, be achieved using a quantum bit.

A quantum bit can be entirely expressed in terms of real vectors in three dimensions. The set of pure quantum states forms a unit Bloch sphere, with orthogonal axes representing the eigenstates of complementary observables. The set of operations on a qubit is no longer restricted only to bit flips, but includes any rotation. Consider the following interaction between the system and the black box. For $f(x) = 0$ (position x is empty), the qubit state is left untouched. If $f(x) = 1$ (occupied), the σ_x or σ_z Pauli rotation is applied to the qubit state for $x = 0$ or 1, respectively. The qubit propagates through the black box from right to left, giving a total transformation of $\sigma_x^{f(0)}\sigma_z^{f(1)}$. In Bloch coordinates, these rotations are represented by diagonal matrices, $\sigma_x \to \mathrm{diag}[1, -1, -1]$ and $\sigma_z \to \mathrm{diag}[-1, -1, 1]$. Thus, the interaction of the black box with the system is represented by the diagonal matrix

$$\mathrm{diag}[(-1)^{f(1)}, (-1)^{f(0)+f(1)}, (-1)^{f(0)}]. \tag{1.2}$$

The quantum probability to observe an outcome associated with the state $\vec{m}$, given a system prepared in state $\vec{n}$, is $P(\vec{m}|\vec{n}) = \frac{1}{2}(1 + \vec{n} \cdot \vec{m})$, where the dot denotes a scalar product in $\mathbb{R}^3$. Therefore, if the $|z\pm\rangle$ states are used as inputs, the measurement in this basis after the interaction reveals the value of $f(0)$. Similarly, using $|x\pm\rangle$ or $|y\pm\rangle$ as inputs, and measuring in these bases, reveals the value of $f(1)$ and $f(0) \oplus f(1)$, respectively. Thus, each of the complementary questions can be answered using the eigenstates of the complementary quantum observables.

1.1.2 Generalized theories

We next investigate a black box containing three positions, $x = 0, 1, 2$. The resulting complementarity table has *seven* rows:

0	1	2	3	4	5	6	7	$f(0) =?$
0	1	4	5	2	3	6	7	$f(1) =?$
0	1	6	7	2	3	4	5	$f(2) =?$
0	2	4	6	1	3	5	7	$f(0) \oplus f(1) =?$
0	2	5	7	1	3	4	6	$f(0) \oplus f(2) =?$
0	3	4	7	1	2	5	6	$f(1) \oplus f(2) =?$
0	3	5	6	1	2	4	7	$f(0) \oplus f(1) \oplus f(2) =?$

(1.3)

The table on the left-hand side presents the values of $j = 2^2 f(0) + 2^1 f(1) + 2^0 f(2)$. Given one bit of information that answers any single complementary question in the right-hand-side table, no information can be obtained about an answer to any of the other questions, i.e. the seven questions are logically independent [147].

In analogy to the previous cases, one can ask what "physical theory" for the system is required to answer any one of the complementary questions contained in table (1.3). Such a theory must contain features of complementarity, and we now generalize the Bloch representation of a quantum bit to produce a quantum-like theory related to the black box with three internal positions. Since there are seven complementary questions, there must be seven complementary measurements for the system and we assume its pure physical states are represented by vectors on a sphere in seven dimensions (state space postulate). Given a system prepared in a state $\vec{n}$, the probability to observe an outcome associated with the state $\vec{m}$, is chosen as $P(\vec{m}|\vec{n}) = \frac{1}{2}(1 + \vec{n} \cdot \vec{m})$, where the dot now denotes a scalar product in $\mathbb{R}^7$ (probability rule). To fulfill the physical requirement that immediate repetition of the same measurement should have the same outcome, the state $\vec{n}$ is updated in the measurement to $+\vec{m}$ or $-\vec{m}$, depending on the result (collapse postulate). The physical transformations, including temporal evolution, are represented in this theory by rotations belonging to SO(7). They preserve distinguishability between any two states as measured by the scalar product, and are continuously connected with the identity, i.e., no transformation.

The model just described allows us to answer any complementary question from table (1.3). The black box transformation can be chosen to be a product $R_0^{f(0)} R_1^{f(1)} R_2^{f(2)}$

of rotations

$$\begin{aligned} R_0 &\rightarrow \mathrm{diag}[-1,1,1,-1,-1,1,-1], \\ R_1 &\rightarrow \mathrm{diag}[1,-1,1,-1,1,-1,-1], \\ R_2 &\rightarrow \mathrm{diag}[1,1,-1,1,-1,-1,-1]. \end{aligned} \tag{1.4}$$

This product is a diagonal matrix with seven entries: $(-1)^{f(0)}$, $(-1)^{f(1)}$, $(-1)^{f(2)}$, $(-1)^{f(0)+f(1)}$, $(-1)^{f(0)+f(2)}$, $(-1)^{f(1)+f(2)}$, $(-1)^{f(0)+f(1)+f(2)}$, where the powers are specified by the complementary questions. Therefore, to answer a complementary question one propagates through the black box system prepared in a state related to the corresponding complementary measurement and finally performs this measurement.

In the general case of a black box with s internal positions, one finds $\binom{s}{1}+\binom{s}{2}+...+\binom{s}{s} = 2^s-1$ complementary questions. There are $\binom{s}{1}$ questions about the value of $f(x)$, $\binom{s}{2}$ questions about different sums of $f(x)\oplus f(x')$ with $x \neq x'$, and so forth. A physical theory of a two-level system can be constructed with 2^s-1 complementary measurements using the approach described above. Since s can be arbitrarily large, there are complementarity tables with arbitrarily many rows, and correspondingly many different theories for a two-level system.

Importantly, the derived number of independent parameters which completely specify the state in a generalized theory, i.e. 2^s-1, is the same as the one following from the parameter counting argument for composite systems [194, 96]. Here, however, it follows already for a single system: from the operational definition (via black box) of the limited information content and the assumption that a system can answer any of the complementary questions.

In all cases, the quantum-like models we have introduced possess rotationally invariant state spaces. There is therefore no preferred choice of a set of 2^s-1 complementary directions or any preferred state. One may expect information contained in all pure states $\vec{n}$ to be the same and independent of the choice of a complete set of complementary measurements. We ask how to quantify information gain in a single measurement $I(p_{+j}, p_{-j})$, with $p_{\pm j} = \frac{1}{2}(1 \pm \vec{n}\cdot\vec{m}_j)$ being probabilities for ± 1 results in measurement $\vec{m}_j$, such that this expectation is fulfilled. Assuming after Ref. [36] that information content of state $\vec{n}$ is the sum of information gained in all complementary measurements $I(\vec{n}) = \sum_{j=1}^{2^s-1} I(p_{+j}, p_{-j})$ the argument of Ref. [41] shows that in the set of information measures based on α-entropy, i.e. if one takes $I(p_{+j}, p_{-j}) = 1-k\frac{1-p_{+j}^{\alpha}-p_{-j}^{\alpha}}{\alpha-1}$ with a constant k and real parameter α, only for the quadratic measure, with $\alpha = 2$, the information content $I(\vec{n})$ is constant and invariant under a *continuous* change between different complete sets of mutually complementary directions. Fixing $k = 2$ sets

the units such that we have $I(n_j) = n_j^2$, where $n_j = \vec{n} \cdot \vec{m}_j$ and since the directions of complementary measurements are orthogonal one finds $I(\vec{n}) = |\vec{n}|^2$, which immediately generalizes the measure of Ref. [36]. This measure captures intuitive expectation that overall information contained in a pure state (revealed in the complete set of complementary measurements) is again one bit.

1.1.3 Computational abilities of generalized theories

The theories with different number of complementary measurements have different computational abilities. Consider the problem of determining properties of a function with a single query of the black box. As an example, think about table (1.9). A qubit propagating through the black box is able to reveal the value of any of $f(0)$, $f(1)$ or $f(0) \oplus f(1)$ by making the appropriate choice of input state and measurement [57]. Classically this is impossible. A classical bit can in principle reveal only one of the three properties because each of the items inside the black box can either keep the bit value or flip it. For example, if the classical bit is flipped after leaving the box, then we know that one of the internal positions is occupied, but it is impossible to determine which one no matter what initial state is used.

Likewise, table (1.3) illustrates the limitations of quantum computing. A single two-level system with seven complementary observables can encode an answer to any one of the seven complementary questions. By contrast, it is only possible to answer at most three of the questions using one qubit. A qubit can be embedded into all generalized theories, just as classical bit is embedded into quantum theory. A sphere in $2^s - 1$ dimensions, for $s > 2$, always contains as subspace a two-sphere of pure states of a quantum bit, and rotations on a two-sphere are a subset of all rotations on higher-dimensional spheres. The rotations of two-sphere, when applied in arbitrary order, never evolve the system outside the two-sphere. Therefore, even if the qubit interacts with more than two items in a black box, it can never answer more than three complementary questions. All generalized theories with more complementary observables are computationally more powerful than both classical and quantum physics.

1.1.4 Theories of many systems

The presentation so far has been limited to a single system. We operationally define the information content of N systems as a maximal possible information gain about the internal configuration of N black boxes, each for a single system. Therefore, the information content of N two-level systems is limited to N bits [197]. We show that

the number of independent real parameters obtained from (joint) complementary measurements, answering the questions about the complementary properties of N Boolean functions encoded in the black boxes, is the same as the number of parameters obtained from correlations between local complementary measurements.

To simplify the presentation we start with two quantum systems as an illustration of ideas and techniques, and next give general results [3]. The quantum case corresponds to $s = 2$. For two qubits we have two black boxes, each of which encodes one of four Boolean functions, see (1.9), and therefore there are in total $2^{Ns} = 16$ combinations of pairs of functions in two black boxes. Accordingly, every row of the complementarity table contains 16 items. Since in this case the final measurement reveals two bits of information, the table has $2^N = 4$ columns. Complementary properties of two Boolean functions are defined such that full knowledge of one property precludes any knowledge about the other property. They correspond to the rows of the table in which items from a fixed column of one row (full knowledge) are evenly distributed among all columns of any other row (no knowledge). For example, for two qubits we have:

$a_1 = 0$		$a_2 = 0$		$a_1 = 0$		$a_2 = 1$		$a_1 = 1$		$a_2 = 0$		$a_1 = 1$		$a_2 = 1$	
00	01	10	11	02	03	12	13	20	21	30	31	22	23	32	33
00	02	20	22	01	03	21	23	10	12	30	32	11	13	31	33
00	03	30	33	01	02	31	32	10	13	20	23	11	12	21	22
00	12	23	31	02	10	21	33	01	13	22	30	03	11	20	32
00	13	21	32	01	12	20	33	02	11	23	30	03	10	22	31

(1.5)

where each item is a pair of numbers $j_1\, j_2$ describing functions in the first and second black box respectively, i.e. $j_1 = 2f_1(0) + f_1(1)$ and $j_2 = 2f_2(0) + f_2(1)$. The complementary properties in this case are the following: (i) the first row corresponds to two binary questions, whether $f_1(0) = a_1$ and $f_2(0) = a_2$, (ii) the second row corresponds to asking whether $f_1(1) = a_1$ and $f_2(1) = a_2$, (iii) the third row is the "parity question", whether $f_1(0) \oplus f_1(1) = a_1$ and $f_2(0) \oplus f_2(1) = a_2$, (iv) the forth row coincides with asking whether $f_1(0) \oplus f_2(1) = a_1$ and $f_1(0) \oplus f_1(1) \oplus f_2(0) = a_2$, (v) the last row leads to asking if $f_1(1) \oplus f_2(0) = a_1$ and $f_1(0) \oplus f_1(1) \oplus f_2(1) = a_2$. The answers to these questions are in a form of two bit values $a_1\, a_2$ and the columns of the table from left to right correspond to the answers 00, 01, 10 and 11. Such complementarity tables are well-known in a mathematical theory of combinatorial designs. In the quantum case of $s = 2$ they are so-called net designs, and the maximal number of their rows gives

[3] For the simplest non-classical and non-quantum example, $N = 2$ and $s = 3$, the complementarity table has 21 rows and it is cumbersome to present it explicitly.

the number of complementary quantum measurements [145]. In a general case of arbitrary s, the complementarity table describing complementary properties of N Boolean functions of an s-valued argument has 2^{Ns} items in every row and 2^N columns. Such complementarity tables, with $s > 2$, are known as the generalized net designs (affine 1-designs) and the maximal number of their rows is given by the Bose-Bush bound [4]:

$$r_s(N) = \frac{2^{Ns} - 1}{2^N - 1}. \tag{1.6}$$

Each of the $r_s(N)$ mutually complementary (joint) measurements gives $2^N - 1$ independent real parameters (due to normalization) and therefore all the complementary measurements give altogether $r_s(N)(2^N - 1) = 2^{Ns} - 1$ independent real parameters.

The same number is found via "tomography with local measurements" [194, 96], in which case we are looking into correlations between the outcomes of all combinations of complementary local measurements (on every subsystem). Each single system is described by $2^s - 1$ real parameters. Additionally, one measures correlations between $2, 3, ..., N$ subsystems (if none of the subsystems is measured, no information is gained). This gives $(2^s - 1 + 1)^N - 1 = 2^{Ns} - 1$ independent real parameters. Thus, we have shown that the number of parameters obtained from joint and local measurements coincide. We see it as an argument that this number of parameters should completely specify a state of the system. Under this assumption, the models considered possess an intuitive feature that a physical state is equally well described by joint and individual measurements. These are then just two different ways of accessing the same information about the system. The equality of the number of parameters obtained by joint and local measurements also means that the models satisfy Hardy's axiom about composite systems: the number of levels of the whole system is a product of number of levels of subsystems and the number of parameters specifying the unnormalized joint state is also a product of the number of such parameters for the subsystems [96].

The complementary questions related to table (1.14) and similar tables for many two-level systems in the generalized theories reveal that the theories involve entanglement. One can recognize the first three questions of table (1.14) are just combinations of complementary questions for single systems, see (1.9). They are asked independently on every subsystem, i.e. the questions with the answer a_1 involve only function $f_1(x)$ and the questions with answer a_2 involve only function $f_2(x)$. With them, all the complementary questions for single subsystems are already exhausted. The same argument applies to any complementarity table of higher level theories. Since for any

[4] Pages 219-220 of Ref. [47]. In their notation, $\lambda = 2^{N(s-2)}$, $v = n = 2^N$ and k is the number of rows in the complementarity table.

such table related to many black boxes the maximal number of rows is greater than the number of rows of the table for a single system, there are complementary questions involving relational properties of functions encoded in different black boxes, such as e.g. the question of the value of $f_1(0) \oplus f_2(1)$ and $f_1(0) \oplus f_1(1) \oplus f_2(0)$. These questions cannot be answered by systems in a product state and we conclude that entanglement must be present in such models.

1.1.5 Experimental consequences

We give two experimental consequences of the generalized theories that differ from predictions of standard quantum theory of a single two-level system. Note that if the experimenter has access to generalized states, evolutions and measurements it is clear that standard quantum theory could be refuted. It is more realistic however to study if the other models can be identified by looking only at the data gathered in quantum measurements. A reason for this is that we now only know how to build apparatuses corresponding to quantum measurements. Furthermore, one can imagine that there is in Nature a source emitting states of generalized theories whereas we are still restricted to quantum measuring devices. Therefore, we make here an assumption that experimentalists have access only to measurements allowed by standard quantum mechanics (on the Bloch sphere) whereas states and evolutions obey generalized theories (on higher dimensional spheres).

The first consequence is a change of purity of an evolving closed system. When the system represented by a vector in a higher dimensional Bloch sphere evolves in time, the projected vector onto the standard two-sphere will in general change its length indicating "decoherence" and "recoherence" in the effective quantum state description. These effects would be present even when the system is closed and can be considered as isolated from environment according to all means of standard quantum theory.

Second, we present a gedanken experiment which tests a dimension of the sphere of states. Consider a scenario in which there are grounds to assume a source prepares random states from the entire higher dimensional Bloch ball (also mixed states) in such a way that the mean value of measurement along some $\vec{x}$ axis can be found for every random state. For example, the source is slowly randomly evolving such that within a short time interval the states emitted are basically the same, but if one waits a longer time and then measures again, the observed state will be unrelated to the previously observed one. The frequency with which a mean $\langle \vec{x} \rangle$ occurs, $f(\langle \vec{x} \rangle)$, is proportional to the number of states giving rise to this particular value of $\langle \vec{x} \rangle$, which is related to the projection of the state vector on the $\vec{x}$ axis. Since the higher the dimension of the

sphere the more states have the mean $\langle\vec{x}\rangle$ close to zero, the shape of $f(\langle\vec{x}\rangle)$ reveals the dimension. We now develop this idea quantitatively.

To make an illustration, we first describe how to distinguish between a theory in which all the states are within a disk (real quantum theory) and standard (complex) quantum theory having a three-dimensional ball of allowed states. If the state space is a disc, a random state is distributed with probability density $dp(x,y) = dxdy/\pi R^2$, where R is the radius of the disc. The frequency of observation of the average value m in a measurement of $\vec{x}$ is related to the length of the chord perpendicular to the x axis which crosses the axis at point m, $F_2(m) = 2\int_0^{\sqrt{R^2-m^2}} \frac{dy}{\pi R^2} = \frac{2\sqrt{R^2-m^2}}{\pi R^2}$. If the state space is a ball, a random state is distributed with probability density $dp(x,y,z) = dxdydz/\frac{4}{3}\pi R^3$, and the frequency of observation of the average value m is now related to the area of the disc orthogonal to x axis which crosses the axis at point m, $F_3(m) = \frac{\pi r^2}{\frac{4}{3}\pi R^3}$, where $r = \sqrt{R^2-m^2}$ is the radius of the disc. In general, for a state space which is a sphere in D dimensions, a random state is distributed according to probability density $dp(x_1,\ldots,x_D) = dx_1\ldots dx_D/V_D(R)$, where $V_D(R) = \frac{\pi^{D/2}R^D}{\Gamma(D/2+1)}$ is the volume of the sphere embedded in D dimensions and $\Gamma(x)$ is the gamma function. The frequency of the average value m is given by the ratio of volumes $F_D(m) = \frac{V_{D-1}(r)}{V_D(R)}$ with $r = \sqrt{R^2-m^2}$. Putting in the explicit formulae for the volumes gives

$$F_D(m) = \frac{1}{\beta(\frac{D}{2}+\frac{1}{2},\frac{1}{2})}\frac{(R^2-m^2)^{\frac{D-1}{2}}}{R^D}, \tag{1.7}$$

where $\beta(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$ is the Euler beta function and we used $\Gamma(1/2) = \sqrt{\pi}$. Fig. 1.2 shows $F_D(m)$ for various D and $R = 1$. Note that in principle D does not even have to be an integer.

If one measures not along a single direction, but along d orthogonal directions, the immediate generalization of the frequency formula (1.7) reads $F_D(m_1,\ldots,m_d) = \frac{V_{D-d}(r)}{V_D(R)}$ with $r = \sqrt{R^2-m_1^2-\cdots-m_d^2}$. This can be useful if a random state is not sampled from spherically symmetric space, providing a way to distinguish even more general models than those studied here. As an illustration, consider first a single $\vec{x}$ measurement and states sampled from a disc. We already know the distribution of m is $F_2(m) = \frac{2\sqrt{R^2-m^2}}{\pi R^2}$. The same distribution is obtained for the state space which is a half disc cut at the x axis, because both the probability density for state distribution and the probability for the mean value equal to m are half those for the disc space and their contributions cancel out in the fraction. Clearly, measurement along x and y could distinguish these two cases.

Summary.– In conclusion, we have introduced a hierarchy of theories describing systems with limited information content, which contains classical and quantum me-

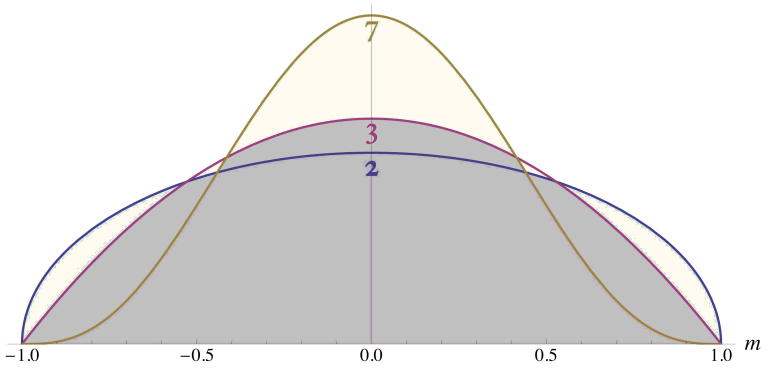

Figure 1.2: Detecting dimension of state space with a random sampler. Assuming that states are represented by vectors within higher-dimensional sphere, sampling them randomly in such a way that for each state the average value, m, along some direction $\vec{x}$ can be measured, provides a way to find the dimension. The dimension can be read from the histogram of m. The plot shows the histogram for three dimensions, $D = 2$, 3, and 7. Generally, after measuring the frequency of the average values one finds the dimension from the fit of the curve (1.7).

chanics as special cases. The order parameter of the hierarchy is the number of complementary questions about the properties of Boolean functions the systems described by the theory can experimentally answer. Typical quantum features such as irreducible randomness and complementarity inevitably occur in the theories. We consider a physical system able to encode the answer to any one of the complementary questions, and assume there is a measuring device which can reveal this information. While the appropriate measurement will reveal the answer to the selected question, the complementary measurements must reveal no information whatsoever — the readout has to give a completely random answer [147]. Further, since the information content of the system is fundamentally limited to one bit, no underlying hidden structure (in the form of hidden variables) is possible, and the results are irreducibly random. As a final remark, we note that we gave examples of generalized theories which share some essential features with quantum mechanics but nevertheless differ from it. Intriguingly, this perhaps suggests that either Nature admits additional conceptual ingredients that single out quantum theory from the more general class [48] or the alternatives are also realized in some domain that is still beyond our observations.

1.2 Mutually unbiased bases and orthogonal Latin squares

Mutually unbiased bases encapsulate the concept of complementarity – the impossibility of simultaneous knowledge of certain observables – in the formalism of quantum theory. Although this concept is at the heart of quantum mechanics, the number of these bases is unknown except for systems of dimension being a power of a prime. We develop the relation between this physical problem and the mathematical problem of finding the number of mutually orthogonal Latin squares. We derive in a simple way all known results about the unbiased bases, find their lower number, and disprove the existence of certain forms of the bases in dimensions different than power of a prime. Using the Latin squares, we construct hidden-variable models which efficiently simulate results of complementary quantum measurements.

Complementarity is a fundamental principle of quantum physics which forbids simultaneous knowledge of certain observables. It is manifested already for the simplest quantum mechanical system — spin $\frac{1}{2}$. If the system is in a definite state of, say, spin along x, the spin along y or z is completely unknown, i.e. the outcomes "spin up" and "spin down" occur with the same probability. The eigenbases of $\hat{\sigma}_x$, $\hat{\sigma}_y$ and $\hat{\sigma}_z$ Pauli operators form so-called *mutually unbiased bases* (MUBs): every vector from one basis has equal overlap with all the vectors from other bases. MUBs encapsulate the concept of complementarity in the quantum formalism. Although complementarity is at the heart of quantum physics, the question about the number of MUBs remains unanswered. Apart from being of foundational interest, MUBs find applications in quantum state tomography [195], quantum-key distribution [81] and the Mean King problem [181, 100].

A d-level quantum system can have at most $d+1$ MUBs, and such a set is referred to as the complete set of MUBs. In 1981 Ivanović proved by construction that there are indeed $d+1$ complementary measurements for d being a prime number [104]. This result was generalized by Wootters and Fields to cover powers of primes [195]. For other dimensions the number of MUBs is unknown, the simplest case being dimension six. A considerable amount of work was done towards understanding this problem. New proofs of previous results were established [13, 37, 119, 113, 63] and the problem was linked with other unsolved problems [29, 21]. It was also noticed that it is similar in spirit to certain problems in combinatorics [196, 20, 189] and finite geometry [161, 192]. Here, we build upon these relations.

We describe the problem of the number of orthogonal Latin squares (OLSs), which was initiated by Euler [66] and still attracts lots of attention in mathematics. Although this problem is not solved yet in full generality, more is known about it than about the

number of MUBs. Using a black box which physically encodes information contained in a Latin square, we link every OLS of order being a power of a prime with a MUB. For dimension six, our method gives three MUBs, which is the maximal number found by the numerical research [196, 21]. Utilizing known results for OLSs we derive a minimal number of MUBs, and disprove the existence of certain forms of MUBs for arbitrary d. Finally, using OLSs we construct hidden-variable models that efficiently simulate complementary quantum measurements.

1.2.1 Orthogonal Latin squares

A Latin square of order d is an array of numbers $\{0, ..., d-1\}$ where every row and every column contains each number exactly once. Two Latin squares, $A = [A_{ij}]$ and $B = [B_{ij}]$, are orthogonal if all *ordered* pairs (A_{ij}, B_{ij}) are distinct. There are at most $d-1$ OLSs and this set is called complete. The existence of L OLSs is equivalent to the existence of a combinatorial design called a *net* with $L+2$ rows [46]. The net design has a form of a table in which every row contains d^2 distinct numbers. They are split into d cells of d numbers each, in such a way that the numbers of any cell in a given row are distributed among all cells of any other row. The additional two rows of the net correspond to *orthogonal but not Latin* squares, with the entries $A_{ij} = j$ and $A_{ij} = i$.

The following algorithm allows to construct the net from a set of OLSs:

- Write the squares in the standard form in which the numbers of the first column are in ascending order (by permuting the entries, it is always possible to write the set of OLSs in the standard form without compromising Latiness and orthogonality).

- Augment the set of OLSs by the two orthogonal non-Latin squares $A_{ij} = j$ and $A_{ij} = i$.

- Write the rows of the squares as cells in a single row of the table. The number of the table's rows is now equal to the number of squares in the augmented set.

- In the row of the table which corresponds to the square $A_{ij} = j$, referred to as the "coordinate row", replace the number A_{ij} in the ith cell by $A'_{ij} = id + j$, where d is the order of the square.

- In every cell of the other rows replace number B_{ij} on position j by the integer associated to the number B_{ij} of the jth cell in the coordinate row, i.e. $B_{ij} \to B'_{ij} = jd + B_{ij}$.

We shall prove that the table generated by this procedure is indeed a net design. We use another property defining the design: two numbers in one cell do not repeat in any other cell. This already includes that any two cells of two different rows share exactly one common number, as if there were no common numbers shared by these cells, there would have to be at least two common numbers shared by other cells.

Due to the definitions of A'_{ij} and B'_{ij} and the fact that the columns of B_{ij} contain all distinct numbers $0, ..., d-1$, every row of the table contains d^2 distinct numbers $0, ..., d^2-1$. By construction, the numbers of any cell of the coordinate row are distributed among all the cells of all the other rows. Therefore, it is sufficient to prove the property of the net for the remaining rows. Assume to the contrary, that two numbers repeat in two cells of different rows, $(jd + B_{ij}, j'd + B_{ij'}) = (ld + C_{kl}, l'd + C_{kl'})$. Since $j, j', l, l', B_{ij}, C_{ij} \in \{0, ..., d-1\}$ the equality can only hold if $B_{ij} = C_{kj}$ and $B_{ij'} = C_{kj'}$, i.e. there are rows of the squares B and C which contain the same numbers, in the columns defined by j and j'. This, however, cannot be because one can always permute the entries of, say, square C such that its kth row becomes the ith row (without compromising orthogonality) and the two squares would not be orthogonal.

1.2.2 The qubit case

Consider the squares for $d = 2$. We link them with the complementary measurements of a qubit. The augmented set of orthogonal squares reads

$$\begin{array}{cc} 0 & 1 \\ 0 & 1 \end{array} \qquad \begin{array}{cc} 0 & 0 \\ 1 & 1 \end{array} \qquad \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \tag{1.8}$$

The right square is Latin, the left and middle square are orthogonal to each other and to the Latin square. These three squares lead to the following net design on the left, in which the numbers are represented by pairs $m\,n$ in modulo-two decomposition:

$b=0$		$b=1$		
00	01	10	11	$m = b$?
00	10	01	11	$n = b$?
00	11	01	10	$m + n = b$?

(1.9)

On the right, we write down the *complementary questions* associated with each row. They are answered by pairs $m\,n$ in the left and right column of the net design (left column → answer 0, right column → answer 1). In this way, the questions are linked to the orthogonal squares.

The complementary questions can be answered in quantum experiments involving MUBs. Consider a device encoding parameters m and n via application of the unitary $\hat{U} = \hat{\sigma}_x^m \hat{\sigma}_z^n$. When it acts on $|z\pm\rangle$ states, they get a phase dependent on n and are flipped m times. Thus, knowing the initial state, a final measurement in the $\hat{\sigma}_z$ eigenbasis reveals m, giving the answer to the first complementary question. Similarly, taking $|x\pm\rangle$ and $|y\pm\rangle$ as initial states, the results of σ_x and σ_y measurement answer the second and the third complementary question, respectively.

1.2.3 Prime dimensions

For prime d the net has $d + 1$ rows. This time, each of its entries takes on one of d values. The entries of the rows corresponding to the OLSs are generated from the following formula

$$n = am + b, \tag{1.10}$$

where the integer $a = 1, ..., d - 1$ enumerates the rows of the table, while the integer $b = 0, ..., d-1$ enumerates different columns, and the sum is modulo d. Additional two rows correspond to the questions about m and n, respectively. The table for the rows corresponding to the OLSs is built in the following way:

- Choose a row, a, and the column, b.
- Vary $m = 0, ..., d - 1$ and compute n using (1.10).
- Write pairs $m\,n$ in the cell.

For example, for $d = 3$, one has

$b=0$			$b=1$			$b=2$			
00	01	02	10	11	12	20	21	22	$m = b$?
00	10	20	01	11	21	02	12	22	$n = b$?
00	11	22	01	12	20	02	10	21	$n = m + b$?
00	12	21	01	10	22	02	11	20	$n = 2m + b$?

(1.11)

The complementary questions are given on the right. Different values of b enumerate possible answers.

We shall see, again, that the complementary questions can be answered using MUBs. Consider encoding of parameters m and n via application of $\hat{U} = \hat{X}^m \hat{Z}^n$, where

the Weyl-Schwinger operators $\hat{X}^m\hat{Z}^n$ span a unitary operator basis. In the basis of $\hat{Z}$, denoted as $|\kappa\rangle$, the two *elementary operators* satisfy

$$\hat{Z}|\kappa\rangle = \eta_d^\kappa|\kappa\rangle, \qquad \hat{X}|\kappa\rangle = |\kappa+1\rangle, \tag{1.12}$$

where $\eta_d = \exp(i2\pi/d)$ is a complex dth root of unity. For the same reasons as for a qubit, the first two questions are answered by applying $\hat{U}$ on an eigenstates of $\hat{Z}$ and $\hat{X}$ operators, and then by measuring the emerging state in these bases.

In all other cases the action of the device is $\hat{U} = \hat{X}^m\hat{Z}^{am+b} = \hat{X}^m\hat{Z}^{am}\hat{Z}^b$. The elementary operators do not commute, instead one has $\hat{Z}\hat{X} = \eta_d\hat{X}\hat{Z}$, and it follows that $\hat{X}^m\hat{Z}^{am} = \eta_d^{-\frac{1}{2}am(m-1)}(\hat{X}\hat{Z}^a)^m$. Finally, the action of the device is, up to the global phase, given by $\hat{U} \propto (\hat{X}\hat{Z}^a)^m\hat{Z}^b$. The eigenstates of the $\hat{X}\hat{Z}^a$ operator, expressed in the $\hat{Z}$ basis, are given by $|j\rangle_a = (1/\sqrt{d})\sum_{\kappa=0}^{d-1}\eta_d^{-j\kappa-as_\kappa}|\kappa\rangle$, where $s_\kappa = \kappa + ... + (d-1)$ [13], and the $\hat{Z}$ operator shifts them: $\hat{Z}|j\rangle_a = |j-1\rangle_a$. After the device, $|j\rangle_a$ is shifted exactly b times and subsequent measurement in this basis reveals the answer to the ath question. On the other hand, the eigenbases of $\hat{X}\hat{Z}^a$ for $a = 1, ..., d-1$ and eigenbases of $\hat{X}$ and $\hat{Z}$ are known to form a complete set of MUBs [13]. Not only the number of MUBs is the same as the number of OLSs, but they are indexed by the same variable, a. This allows to associate MUB to every OLS for prime d.

1.2.4 Powers of primes

If d is a power of a prime, a complete set of OLSs is obtained using operations in the finite field of d elements, and one expects that a complete set of MUBs also follows from the existence of the field. Indeed, explicit formulae for MUBs in terms of the field operations were presented in [195, 63, 113]. Here, we prove this result in a simple way related to [78], using the theorem of Bandyopadhyay *et al.* [13, 87]: *If there is a set of orthogonal unitary matrices, which can be partitioned into M subsets of d commuting operators, then there are at least M MUBs*. They are the joint eigenbases of the d commuting operators.

To illustrate the idea, consider again prime d. Take the orthogonal unitary operators $\hat{S}_{mn} = \hat{X}^m\hat{Z}^n$ with their powers $m\,n$ taken from the first column of the net. The cell of the first and second row corresponds to the eigenbases of $\hat{Z}$ and $\hat{X}$, respectively, whereas the other two rows are defined by $b = 0$, i.e. $n = am$. According to the commutation rule of the elementary operators $\hat{X}$ and $\hat{Z}$, $\hat{S}_{mn}$ and $\hat{S}_{m'n'}$ commute if and only if $mn' - m'n = 0 \mod d$. Thus, for a fixed row, i.e. fixed a, the set of d operators $\hat{S}_{mn}$ commute, because $m(am') - m'(am) = 0$, and, due to the mentioned theorem, there is a set of $d+1$ MUBs.

For $d = p^r$ being a power of a prime, the OLSs and the net are generated by the formula

$$n = a \odot m \oplus b, \tag{1.13}$$

where $\odot$ and $\oplus$ denote multiplication and addition in the field, $a, b, m, n \in \mathbb{F}_d$ are field elements, and $a \neq 0$. The first two rows of the table are defined by $m = b$ and $n = b$. In the case of $d = 4$, the four elements $\{0, 1, \omega, \omega + 1\}$ of the field $\mathbb{F}_4$ (ω is the root of $x^2 + x + 1$ [78]), when indexed with the numbers $\{0, 1, 2, 3\}$, lead to the following net design:

00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
00	10	20	30	01	11	21	31	02	12	22	32	03	13	23	33
00	11	22	33	01	10	23	32	02	13	20	31	03	12	21	30
00	12	23	31	01	13	22	30	02	10	21	33	03	11	20	32
00	13	21	32	01	12	20	33	02	11	23	30	03	10	22	31

(1.14)

We use the concept of a basis in the finite field $\mathbb{F}_d$. It consists of r elements e_i, with $i = 1, ..., r$. Every basis has a unique dual basis, $\overline{e}_j$, such that $\mathrm{tr}(e_i \odot \overline{e}_j) = \delta_{ij}$, where the trace in the field, $\mathrm{tr}(x)$, maps elements of $\mathbb{F}_d$ into the elements of the prime field $\mathbb{F}_p$. It has the following useful properties: $\mathrm{tr}(x \oplus y) = \mathrm{tr}(x) + \mathrm{tr}(y)$, and $\mathrm{tr}(a \odot x) = a\,\mathrm{tr}(x)$, where operations on the right-hand side are modulo p and a is in the prime field. We decompose m in the basis e_i, $m = m_1 \odot e_1 \oplus ... \oplus m_r \odot e_r$, where $m_i = \mathrm{tr}(m \odot \overline{e}_i)$, and n in the *dual* basis, $n = n_1 \odot \overline{e}_1 \oplus ... \oplus n_r \odot \overline{e}_r$, with $n_i = \mathrm{tr}(n \odot e_i)$. Due to the properties of the trace in the field and the dual basis

$$\mathrm{tr}(m \odot n) = \sum_{i=1}^{r} m_i n_i = \vec{m} \cdot \vec{n}, \tag{1.15}$$

where $\vec{m} = (m_1, ..., m_r)$ and $\vec{n} = (n_1, ..., n_r)$ have components in the prime field, i.e. numbers $\{0, ..., p - 1\}$.

Consider operators defined by the decomposition of m and n, $\hat{S}_{\vec{m}\vec{n}} = \hat{X}_p^{m_1} \hat{Z}_p^{n_1} \otimes ... \otimes \hat{X}_p^{m_r} \hat{Z}_p^{n_r}$, where e.g. $X_p^{m_i}$ is the unitary operator acting on the ith p-dimensional subspace of the global d-dimensional space. Operators $S_{\vec{m}\vec{n}}$ form an orthogonal basis. They commute, if and only if $\vec{m} \cdot \vec{n}' - \vec{m}' \cdot \vec{n} = 0 \mod p$. Take the operators corresponding to a fixed row of the first column of the net, i.e. a is fixed, $b = 0$ and therefore $n = a \odot m$. From Eq. (1.15), all these d operators commute if $\mathrm{tr}(m \odot a \odot m') = \mathrm{tr}(m' \odot a \odot m)$, which is satisfied due to associativity and commutativity of multiplication in the field. Therefore, their eigenbases define MUBs. Again, each row of the table is linked with the MUB.

To make an illustration, consider again the example of $d = 4$. Choose $(e_1, e_2) = (\omega, 1)$ as a basis in the field, such that the numbers m are decomposed into pairs $m \to m_1\, m_2$ in the usual way: $0 \to 0\,0$, $1 \to 0\,1$, $2 \to 1\,0$, $3 \to 1\,1$. The dual basis reads $(\overline{e}_1, \overline{e}_2) = (1, \omega + 1)$, which implies that the numbers n are decomposed into pairs $n \to n_1\, n_2$ as follows: $0 \to 0\,0$, $1 \to 1\,0$, $2 \to 1\,1$, $3 \to 0\,1$. Each pair of numbers of table (1.14) is now written *vertically* as a combination of two pairs of numbers:

00	01	01	00	00	01	01	00	10	11	11	10	10	11	11	10
00	00	01	01	10	10	11	11	00	00	01	01	10	10	11	11
00	00	10	10	01	01	11	11	01	01	11	11	00	00	10	10
00	10	00	10	00	10	00	10	01	11	01	11	01	11	01	11
00	01	11	10	01	00	10	11	01	00	10	11	00	01	11	10
00	10	01	11	00	10	01	11	01	11	00	10	01	11	00	10
00	01	10	11	01	00	11	10	01	00	11	10	00	01	10	11
00	11	01	10	00	11	01	10	01	10	00	11	01	10	00	11
00	00	11	11	01	01	10	10	01	01	10	10	00	00	11	11
00	11	00	11	00	11	00	11	01	10	01	10	01	10	01	10

(1.16)

MUBs are formed by the eigenbases of operators $\hat{\sigma}_x^{m_1}\hat{\sigma}_z^{n_1} \otimes \hat{\sigma}_x^{m_2}\hat{\sigma}_z^{n_2}$, where the powers are taken from the first column of this table. The result is in agreement with other methods [37, 119, 13]. The complementary questions answered by the states of these MUBs are formulated in terms of individual bits m_1, m_2, n_1, n_2, which are encoded by $\hat{U} = \hat{\sigma}_x^{m_1}\hat{\sigma}_z^{n_1} \otimes \hat{\sigma}_x^{m_2}\hat{\sigma}_z^{n_2}$. E.g., the question of the last row is about the values of $m_1 + n_1$ and $m_2 + n_2$.

An interesting feature strengthening the link between MUBs and OLSs is the existence of the set of OLSs and MUBs which cannot be completed. For example, the following net design

00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
00	10	20	30	01	11	21	31	02	12	22	32	03	13	23	33
00	11	22	33	01	12	23	30	02	13	20	31	03	10	21	32

(1.17)

cannot have more rows. The MUBs related to this table are the eigenbases of $\hat{X}$, $\hat{Z}$ and $\hat{X}\hat{Z}$ for $d = 4$. Correspondingly, there are no other bases which are mutually unbiased with respect to these three [86].

1.2.5 General dimension

Tarry was the first to prove that no two OLSs of order six exist [178], i.e. the net for $d = 6$ has only three rows. The operators $\hat{X}^m\hat{Z}^n$ commute for numbers m and n from the first cell of these rows and the corresponding MUBs are the eigenbases of $\hat{X}$, $\hat{Z}$ and $\hat{X}\hat{Z}$. Similarly to the case of $d = 4$ no other MUB with respect to these three exists [87]. Of course, the question whether different three MUBs can be augmented with additional MUBs remains open.

1.2.6 MacNeish's bound

More generally, the lower bound on the number of OLSs was given by MacNeish [130]. If two squares of order a are orthogonal, $A \perp B$, and two squares of order b are orthogonal, $C \perp D$, then the squares obtained by a direct product, of order ab, are also orthogonal, $A \times C \perp B \times D$. This implies that the number of OLSs, $\mathcal{L}$, of the order $d = p_1^{r_1}...p_n^{r_n}$, with p_i being prime factors of d, is at least $\mathcal{L} \geq \min_i(p_i^{r_i} - 1)$, where $p_i^{r_i} - 1$ is the number of OLSs of order $p_i^{r_i}$. A parallel result holds for MUBs [113, 87]. If $|a\rangle$ and $|b\rangle$ are the states of two MUBs in dimension d_1, and $|c\rangle$ and $|d\rangle$ are the states of MUBs in dimension d_2, then the tensor product bases $|a\rangle\otimes|c\rangle$ and $|b\rangle\otimes|d\rangle$ form MUBs in dimension d_1d_2. Thus, for $d = p_1^{r_1}...p_n^{r_n}$ there are at least $\min_i(p_i^{r_i} + 1)$ MUBs.

Latin operator basis

In general, we know more about the number of OLSs than about the number of MUBs [46]. We use this knowledge to derive conditions which restrict the form of MUBs. Consider the operators

$$\hat{B}_{n_0...n_d} = \mathbb{1} + \sum_{m=0}^{d}\sum_{\xi=1}^{d-1} \eta_d^{n_m\xi} S_m^{\xi}, \tag{1.18}$$

where $n_m = 0, ..., d-1$ and $S_m^{\xi} = \sum_{j=0}^{d-1} \eta_d^{j\xi}|j\rangle_m\langle j|$ have complete set of MUBs as eigenbases, $m = 0, ..., d$. We show that existence of such a set and orthogonality of d^2 operators $\hat{B}_{n_0...n_d}$ implies completeness of the set of OLSs. The trace scalar product $\mathrm{Tr}(\hat{B}^{\dagger}_{n_0...n_d}\hat{B}_{n'_0...n'_d})$ is given by $d^2(k-1)$, where k denotes the sum of Kronecker deltas, $k \equiv \delta_{n_0n'_0} + ... + \delta_{n_dn'_d}$. Operators $\hat{B}_{n_0...n_d}$ and $\hat{B}_{n'_0...n'_d}$ are orthogonal if and only if $k = 1$, i.e. $n_m = n'_m$ for exactly one m. This condition applied to d^2 orthogonal operators, defines a complete set of orthogonal squares. To see this, take d^2 orthogonal operators $\hat{B}_{n_0(b)...n_d(b)}$ with $b = 1, ..., d^2$ and consider $d+1$ squares defined by their indices $n_m(b)$ for a fixed m. If the squares were not orthogonal, one could find at least two identical

pairs, $(n_m(b), n_{m'}(b)) = (n_m(b'), n_{m'}(b'))$, implying that operators (1.18) are not orthogonal ($k > 1$). Therefore, e.g. for $d = 6$, there is no complete set of MUBs for which operators $\hat{B}_{n_0 \ldots n_d}$ are orthogonal because there is no complete set of OLSs in this case.

Orthogonal functions

The second condition is obtained by noting that a net defines "orthogonal" functions, $F_a(m, n)$, which give the column of the ath row where the pair $m\,n$ is entered. The orthogonality means that for the pairs $m\,n$ for which the function $F_a(m, n)$ has a fixed value, the function $F_{a'}(m, n)$ acquires all its values. We show that if d^2 unitaries, $\hat{U}_{mn}$, shift (up to a phase) the states of different bases in accordance with the net

$$\hat{U}_{mn}|j\rangle_a \propto |j + F_a(m, n)\rangle_a, \tag{1.19}$$

then these bases are MUBs. For the proof, note that $\sum_{i'=0}^{d-1} |{}_a\langle i|i'\rangle_{a'}|^2 = 1$. From orthogonality of the functions, this sum can be written as $\sum_{\mathcal{S}} |{}_a\langle j + F_a(m, n)|j' + F_{a'}(m, n)\rangle_{a'}|^2 = 1$, where $\mathcal{S}$ is the set of pairs $m\,n$ for which $F_a(m, n)$ has a fixed value. By (1.19), the last is $\sum_{\mathcal{S}} |{}_a\langle j|\hat{U}_{mn}^\dagger \hat{U}_{mn}|j'\rangle_{a'}|^2$, which due to unitarity, $\hat{U}_{mn}^\dagger \hat{U}_{mn} = \mathbb{1}$, is the sum of d identical terms $|{}_a\langle j|j'\rangle_{a'}|^2$. Therefore, $|{}_a\langle j|j'\rangle_{a'}|^2 = 1/d$. Further, given d^2 unitaries with property (1.19), one recovers the table in the following experiment: prepare $|0\rangle_a$, act on it with $\hat{U}_{mn}$, measure in the same basis, and write the pair $m\,n$ in the ath row and the column corresponding to the result. Thus, in dimension six, there cannot be 36 unitaries satisfying (1.19), with the orthogonal functions, for more than three bases, because otherwise one could construct more than three orthogonal squares of order six, which is impossible.

1.2.7 Hidden-variable simulation of MUBs

The net designs can be used to construct hidden-variable models which simulate results of complementary measurements on certain states. Recently, Spekkens showed that only four "ontic states" (hidden variables) are sufficient to simulate complementary measurements of a qubit prepared in a state of a MUB [175]. In his model, quantum states of MUBs correspond to the "epistemic states" satisfying the knowledge balance principle: the amount of knowledge one possesses about the ontic state is equal to the amount of knowledge one lacks [175]. This principle lies behind the net design. Left table of (1.9) corresponds to the original Spekkens' model: the numbers enumerate ontic states, cells correspond to the epistemic states and rows to the complementary measurements. All other tables generalize the model. To identify the ontic state one

needs two dits of information (there are d^2 ontic states), whereas the epistemic state is defined by a single dit, leaving the other one unknown. The quantum states described by these models require (a classical mixture of) only two dits to model d outcomes of $d+1$ quantum complementary measurements.

Our approach allows to ask the question how many epistemic states satisfying the knowledge balance principle, i.e. having d underlying ontic states, correspond to quantum states. For example, in the case of a two-level system there are four ontic states, and six possible epistemic states [see the net design of (1.9)]. All six correspond to quantum eigenstates of complementary observables. In general, any epistemic state is represented by a cell of d numbers $\boxed{i_1\ i_2\ ...\ i_d}$. Since each number takes on one of d^2 values, the numbers cannot repeat and their order is not important, there are $\mathcal{E}_d = \sum_{i_1=1}^{D} \sum_{i_2=i_1+1}^{D+1} \cdots \sum_{i_d=i_{d-1}+1}^{D+d-1}$ possible epistemic states, with $D = d^2 - d + 1$.

For d being a power of a prime the quantum states corresponding to the cells of the net design are basis vectors of a complete set of MUBs. They can be used to uniquely decompose arbitrary Hermitian operator

$$\hat{O} = -\mathrm{Tr}(\hat{O})\hat{1\!\!1} + \sum_{m=0}^{d} \sum_{j=0}^{d-1} p_j^{(m)} |j\rangle_m\langle j|, \tag{1.20}$$

where $p_j^{(m)} = {}_m\langle j|\hat{O}|j\rangle_m$ and $|j\rangle_m$ is the jth state of the mth MUB. For the proof, note that the complete set of MUBs can be used to define the operator basis in the Hilbert-Schmidt space $\hat{S}_m^{\xi} = \sum_{j=0}^{d-1} \eta_d^{j\xi} |j\rangle_m\langle j|$. There are d^2 such operators, because $m = 0, ..., d$, the power $\xi = 0, ..., d-1$ and all d operators $\hat{S}_m^0$ are equal to the identity operator. Since they are normalized as $\mathrm{Tr}[(\hat{S}_m^{\xi})^{\dagger} \hat{S}_{m'}^{\xi'}] = d\delta_{mm'}\delta_{\xi\xi'}$ any operator has a unique expansion $\hat{O} = \frac{1}{d}[\mathrm{Tr}(\hat{O})\hat{1\!\!1} + \sum_{m=0}^{d} \sum_{\xi=1}^{d-1} \mathrm{Tr}(\hat{O}(\hat{S}_m^{\xi})^{\dagger})\hat{S}_m^{\xi}]$ Writing $\hat{S}_m^{\xi}$ in terms of projectors on MUBs one finds Eq. (1.20).

If $\hat{O}$ is a quantum state, $\mathrm{Tr}(\hat{O}) = 1$ and $p_j^{(m)}$'s are probabilities to observe outcomes related to suitable states of MUBs. We consider general epistemic states, not necessarily those corresponding to the cells of the net design. Such epistemic states have "partial overlap" with the cells, defined as the number of common ontic states divided by d. For example, the epistemic state $\boxed{00\ 01\ 20}$ has an overlap of $\frac{2}{3}$ and $\frac{1}{3}$ with the first and third epistemic state of the first row of table (1.11), respectively. To construct operator $\hat{O}$ associated with a general epistemic state, we take these overlaps to define the probabilities $p_j^{(m)}$. Since we would like to see how many epistemic states correspond to quantum states we take operators $\hat{O}$ with a unit trace. If $\mathrm{Tr}(\hat{O}^2) = 1$ and $\mathrm{Tr}(\hat{O}^3) \neq 1$, the operator $\hat{O}$ cannot represent a quantum state, because the first condition excludes mixed states, and both of them exclude pure states [107]. We find that for $d = 3$ only the epistemic states of the net design correspond to the quantum

states. There are $Q_3 = 12$ such states, out of $\mathcal{E}_3 = 84$ different epistemic states. The ratio of $\mathcal{R}_d = Q_d/\mathcal{E}_d$ rapidly decreases with d: we checked $\mathcal{R}_3 = 1/7$, $\mathcal{R}_4 = 8/455$ and $\mathcal{R}_5 = 1/1771$. Thus, most of the epistemic states, constructed according to the "knowledge balance principle", do not represent a quantum-physical state.

Summary.– In conclusion, we showed a one-to-one relation between OLSs and MUBs, if d is a power of a prime. For general dimensions, we derive conditions which limit the structure of the complete set of MUBs and we presented parallelism between the MacNeish's bound on the minimal number of OLSs and the minimal number of MUBs. Interestingly, the MacNeish's bound is known not to be tight. There are at least five OLSs of order 35, where the MacNeish's bound is four [190]. Therefore, further insight into the relations between MUBs and OLSs would be gained from studies of MUBs for $d = 35$.

Finally, using the squares, we constructed hidden-variable models that efficiently simulate measurements of MUBs. However, the majority of states in these models do not have quantum-physical counterparts.

1.3 Reconstruction of quantum theory

Quantum theory makes the most accurate empirical predictions and yet it lacks simple, comprehensible physical principles from which the theory can be uniquely derived. A broad class of probabilistic theories exist which all share some features with quantum theory, such as probabilistic predictions for individual outcomes (indeterminism), the impossibility of information transfer faster than speed of light (no-signaling) or the impossibility of copying of unknown states (no-cloning). A vast majority of attempts to find physical principles behind quantum theory either fall short of deriving the theory uniquely from the principles or are based on abstract mathematical assumptions that require themselves a more conclusive physical motivation. Here, we show that classical probability theory and quantum theory can be reconstructed from three reasonable axioms: (1) (Information capacity) All systems with information carrying capacity of one bit are equivalent. (2) (Locality) The state of a composite system is completely determined by measurements on its subsystems. (3) (Reversibility) Between any two pure states there exists a reversible transformation. If one requires the transformation from the last axiom to be continuous, one separates quantum theory from the classical probabilistic one. A remarkable result following from our reconstruction is that no probability theory other than quantum theory can exhibit entanglement without contradicting one or more axioms.

The historical development of scientific progress teaches us that every theory that was established and broadly accepted at a certain time was later inevitably replaced by a deeper and more fundamental theory of which the old one remains a special case. One celebrated example is Newtonian (classical) mechanics which was superseded by quantum mechanics at the beginning of the last century. It is natural to ask whether in a similar manner there could be logically consistent theories that are more generic than quantum theory itself. It could then turn out that quantum mechanics is an effective description of such a theory, only valid within our current restricted domain of experience.

At present, quantum theory has been tested against very specific alternative theories that, both mathematically and in their concepts, are distinctly different. Instances of such alternative theories are non-contextual hidden-variable theories [116], local hidden-variable theories [19], crypto-nonlocal hidden-variable theories [120, 92], or some nonlinear variants of the Schrödinger equation [22, 167, 169, 75]. Currently, many groups are working on improving experimental conditions to be able to test alternative theories based on various collapse models [77, 110, 109, 60, 151, 149]. The common trait of all these proposals is to suppresses one or the other counter-intuitive

feature of quantum mechanics and thus keep some of the basic notions of a classical world view intact. Specifically, hidden-variable models would allow to preassign definite values to outcomes of all measurements, collapse models are mechanisms for restraining superpositions between macroscopically distinct states and nonlinear extensions of the Schrödinger equation may admit more localized solutions for wave-packet dynamics, thereby resembling localized classical particles.

In the last years the new field of quantum information has initialized interest in generalized probabilistic theories which share certain features – such as the no-cloning and the no-broadcasting theorems [14, 15] or the trade-off between state disturbance and measurement [18] – generally thought of as specifically quantum, yet being shown to be present in all except classical theory. These generalized probabilistic theories can allow for stronger than quantum correlations in the sense that they can violate Bell's inequalities stronger than the quantum Cirel'son bound (as it is the case for the celebrated "non-local boxes" of Popescu and Rohrlich [157]), though they all respect the "non-signaling" constraint according to which correlations cannot be used to send information faster than the speed of light.

Since the majority of the features that have been highlighted as "typically quantum" are actually quite generic for all non-classical probabilistic theories, one could conclude that additional principles must be adopted to single out quantum theory uniquely. Alternatively, these probabilistic theories indeed can be constructed in a logically consistent way, and might even be realized in nature in a domain that is still beyond our observations. The vast majority of attempts to find physical principles behind quantum theory either fail to single out the theory uniquely or are based on highly abstract mathematical assumptions without an immediate physical meaning (e.g. [129]).

On the way to reconstructions of quantum theory from foundational physical principles rather than purely mathematical axioms, one finds interesting examples coming from an instrumentalist approach [96, 50, 83], where the focus is primarily on primitive laboratory operations such as preparations, transformations and measurements. While these reconstructions are based on a short set of simple axioms, they still partially use mathematical language in their formulation.

Evidentally, added value of reconstructions for better understanding quantum theory originates from its power of explanation where the structure of the theory comes from. Candidates for foundational principles were proposed giving a basis for an understanding of quantum theory as a general theory of information supplemented by several information-theoretic constraints [159, 197, 39, 40, 44, 91]. In a wider context these approaches belong to attempts to find an explanation for quantum theory

by putting primacy on the concept of information or on the concept of probability which again can be seen as a way of quantifying information [193, 71, 176, 177, 27, 43, 73, 84, 85, 127, 175, 82]. Other principles were proposed for separation of quantum correlations from general non-signaling correlations, such as that communication complexity is not trivial [182, 31], that communication of m classical bits causes information gain of at most m bits ("information causality") [148], or that any theory should recover classical physics in the macroscopic limit [139].

In his seminal paper, Hardy [96] derives quantum theory from "five reasonable axioms" within the instrumentalist framework. He sets up a link between two natural numbers, d and N, characteristics of any theory. d is the number of degrees of freedom of the system and is defined as the minimum number of real parameters needed to determine the state completely. The dimension N is defined as the maximum number of states that can be reliably distinguished from one another in a single shot experiment. A closely related notion is the information carrying capacity of the system, which is the maximal number of bits encoded in the system, and is equal to $\log N$ bits for a system of dimension N.

Examples of theories with an explicit functional dependence $d(N)$ are classical probability theory with the linear dependence $d = N - 1$, and quantum theory with the quadratic dependence for which it is necessary to use $d = N^2 - 1$ real parameters to completely characterize the quantum state [5]. Higher-order theories with more general dependencies $d(N)$ might exist as illustrated in Figure 1. Hardy's reconstruction resorts to a "simplicity axiom" that discards a large class of higher-order theories by requiring that for each given N, $d(N)$ takes the minimum value consistent with the other axioms. However, without making such an *ad hoc* assumption the higher-order theories might be possible to be constructed in agreement with the rest of the axioms. In fact, an explicit quartic theory for which $d = N^4 - 1$ [199], and theories for generalized bit ($N = 2$) for which $d = 2^r - 1$ and $r \in N$ [146], were recently developed, though all of them are restricted to the description of individual systems only.

It is clear from the previous discussion that the question on basis of which physical principles quantum theory can be separated from the multitude of possible generalized probability theories is still open. A particulary interesting unsolved problem is whether the higher-order theories of Refs. [96, 199, 146] can be extended to describe non-trivial, i.e. *entangled*, states of composite systems. Any progress in theoretical understanding of these issues would be very desirable, in particular because experi-

[5] Hardy considers unnormalized states and for that reason takes $K = d + 1$ (in his notation) as the number of degrees of freedom.

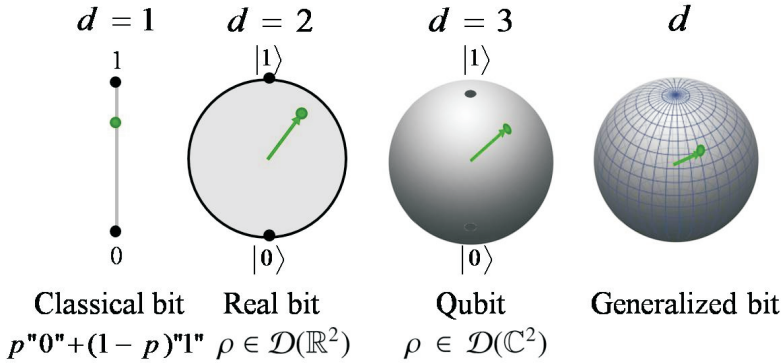

Figure 1.3: State spaces of a two-dimensional system in the generalized probabilistic theories analyzed here. d is the minimal number of real parameters necessary to determine the (generally mixed) state completely. From left to right: A classical bit with one parameter (the weight p in the mixture of two bit values), a real bit with two real parameters (state $\rho \in \mathcal{D}(\mathbb{R}^2)$ is represented by 2×2 real density matrix), a qubit (quantum bit) with three real parameters (state $\rho \in \mathcal{D}(\mathbb{C}^2)$ is represented by 2×2 complex density matrix) and a generalized bit for which d real parameters are needed to specify the state. Note that, when one moves continuously from one pure state (represented by a point on the surface of a sphere) to another, only in the classical probabilistic theory one must go trough the set of mixed states. Can probability theories that are more generic than quantum theory be extended in a logically consistent way to higher-dimensional and composite systems? Can entanglement exist in these theories? Where should we look in nature for potential empirical evidences of the theories?

mental research efforts in this direction have been very sporadic. Although the majority of experiments indirectly verify also the number of the degrees of freedom of quantum systems [6], there are only few dedicated attempts at such a direct experimental verification. Quaternionic quantum mechanics (for which $d = 2N^2 - N - 1$) was tested in a suboptimal setting [155] in a single neutron experiment in 1984 [152, 108], and more recently, the generalized measure theory of Sorkin [172] in which higher order interferences are predicted was tested in a three-slit experiment with photons [170]. Both experiments put an upper bound on the extent of the observational effects the two alternative theories may produce.

[6] As noted by Zyczkowski [199] it is thinkable that within the time scales of standard experimental conditions "hyper-decoherence" may occur which cause a system described in the framework of the higher-order theory to specific properties and behavior according to predictions of standard (complex) quantum theory.

1.3.1 Basic ideas and the axioms

Here we reconstruct quantum theory from three reasonable axioms. Following the general structure of any reconstruction we first give a set of physical principles, then formulate their mathematical representation, and finally rigorously derive the formalism of the theory. We will only consider the case where the number of distinguishable states is finite. The three axioms which separate classical probability theory and quantum theory from all other probabilistic theories are:

Axiom 1. *(Information capacity) An elementary system has the information carrying capacity of at most one bit. All systems of the same information carrying capacity are equivalent.*

Axiom 2. *(Locality) The state of a composite system is completely determined by local measurements on its subsystems and their correlations.*

Axiom 3. *(Reversibility) Between any two pure states there exists a reversible transformation.*

A few comments on these axioms are appropriate here. The most elementary system in the theory is a two-dimensional system. All higher-dimensional systems will be built out of two-dimensional ones. Recall that the dimension is defined as the maximal number of states that can be reliably distinguished from one another in a single shot experiment. Under the phrase "an elementary system has an information capacity of at most one bit" we precisely assume that for any state (pure or mixed) of a two-dimensional system there is a measurement such that the state is a mixture of *two* states which are distinguished reliable in the measurement. An alternative formulation could be that *any state of a two dimensional system can be prepared by mixing at most two basis (i.e. perfectly distinguishable in a measurement) states* (see Figure 2). Roughly speaking, axiom 1 assumes that a state of an elementary system can always be represented as a mixture of *two classical bits*. This part of the axiom is inspired by Zeilinger's proposal for a foundation principle for quantum theory [197].

The second statement in axiom 1 is motivated by the intuition that at the fundamental level there should be no difference between systems of the same information carrying capacity. All elementary systems – be they part of higher dimensional systems or not – should have equivalent state spaces and equivalent sets of transformations and measurements. This seems to be a natural assumption if one makes no prior restrictions to the theory and preserves the full symmetry between all possible elementary systems. This is why we have decided to put the statement as a part of axiom 1, rather than as

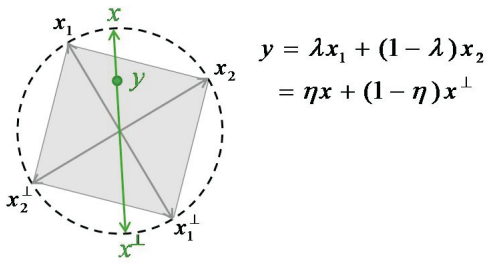

Figure 1.4: Illustration of the assumption stated in axiom 1. Consider a toy-world of a two-dimensional system in which the set of pure states consists of only $\mathbf{x}_1$ and $\mathbf{x}_2$ and their orthogonal states $\mathbf{x}_1^\perp$ and $\mathbf{x}_2^\perp$ respectively, and where only two measurements exist, which distinguish $\{\mathbf{x}_1, \mathbf{x}_1^\perp\}$ and $\{\mathbf{x}_2, \mathbf{x}_2^\perp\}$. The convex set (represented by the grey area within the circle) whose vertices are the four states contains all physical (pure or mixed) states in the toy-world. Now, choose a point in the set, say $\mathbf{y} = \lambda\mathbf{x}_1 + (1-\lambda)\mathbf{x}_2$. Axiom 1 states that any physical state can be represented as a mixture of two orthogonal states (i.e. states perfectly distinguishable in a single shot experiment), e.g. $\mathbf{y} = \eta\mathbf{x} + (1-\eta)\mathbf{x}^\perp$. This is not fulfilled in the toy world, but is satisfied in a theory in which the entire circle represents the pure states and where measurements can distinguish all pairs of orthogonal states.

a separate axiom. The particular formulation used here is from Grinbaum [90] who suggested to rephrase the "subspace axiom" of Hardy's reconstruction using physical language rather than mathematical. The subspace axiom states that a system whose state is constrained to belong to an M dimensional subspace (i.e. have support on only M of a set of N possible distinguishable states) behaves like a system of dimension M.

In logical terms axiom 1 means the following. We can think of two basis states as two binary propositions about an individual system, such as (1) "The outcome of measurement A is +1" and (2) "The outcome of measurement A is -1". An alternative choice for the pair of propositions can be propositions about joint properties of two systems, such as (1') "The outcomes of measurement A on the first system and of B on the second system are correlated" (i.e. either both +1 or both -1) and (2') "The outcomes of measurement A on the first system and of B on the second system are anticorrelated". The two choices for the pair of propositions correspond to two choices of basis states which each can be used to span the full state space of an abstract elementary system (also called "generalized bit"). As we will see later, taking the latter choice, it will follow from axiom 1 alone that the state space must contain entangled states.

Axiom 2 assumes that a specification of the probabilities for a complete set of local measurements for each of the subsystems plus the joint probabilities for corre-

lations between these measurements is sufficient to determine completely the global state. Note that this property does hold in both quantum theory and classical probability theory, but not in quantum theory formulated on the basis of real or quaternionic amplitudes instead of complex. A closely related formulation of the axiom was given by Barrett [18].

Finally, axiom 3 requires that transformations are reversible. This is assumed alone for the purposes that the set of transformations builds a group structure. It is natural to assume that a composition of two physical transformations is again a physical transformation. It should be noted that this axiom could be used to exclude the theories in which "non-local boxes" occur, because there the dynamical group is trivial, in the sense that it is generated solely by local operations and permutations of systems with no entangling reversible transformations (that is, non-local boxes cannot be prepared from product states) [94].

If one requires the reversible transformation from our axiom 3 to be continuous:

Axiom 3'. *(Continuity) Between any two pure states there exists a continuous reversible transformation,*

which separates quantum theory from classical probability theory. The same axiom is also present in Hardy's reconstruction. By a continuous transformation is here meant that every transformation can be made up from a sequence of transformations only infinitesimally different from the identity.

A remarkable result following from our reconstruction is that *quantum theory is the only probabilistic theory in which one can construct entangled states and fulfill the three axioms*. In particular, in the higher-order theories of Refs. [96, 199, 146] composite systems can only enjoy trivial separable states. On the other hand, we will see that axiom 1 alone requires entangled states to exist in all non-classical theories. This will allow us to discard the higher-order theories in our reconstruction scheme without invoking the simplicity argument.

As a by product of our reconstruction we will be able to answer why in nature only "odd" correlations (i.e. $(1,1,-1)$, $(1,-1,1)$, $(-1,1,1)$ and $(-1,-1,-1)$) are observed when two maximally entangled qubits (spin-1/2 particles) are both measured along direction x, y and z, respectively. The most familiar example is of the singlet state $|\psi^-\rangle = \frac{1}{2}(|0\rangle_1|1\rangle_2 - |0\rangle_1|1\rangle_2)$ with anticorrelated results for arbitrarily but the same choice of measurement directions for two qubits. We will show that the "mirror quantum mechanics" in which only "even" correlations appear cannot be extended consistently to composite systems of three bits.

Our reconstruction will be given in the framework of typical experimental situation an observer faces in the laboratory. While this instrumentalist approach is a useful paradigm to work with, it might not be necessary. One could think about axioms 1 and 3 as referring to objective features of elementary constituents of the world which need not necessarily be related to laboratory actions. In contrast, axiom 2 seems to acquire a meaning only within the instrumentalist approach as it involves the word "measurement". Even here one could follow a suggestion of Grinbaum [90] and rephrase the axiom to the assumption of "multiplicability of the information carrying capacity of subsystems."

Concluding this section, we note that the conceptual groundwork for the ideas presented here has been prepared most notably by Weizsäcker [185], Wheeler [187] and Zeilinger [197] who proposed that the notion of the elementary yes-no alternative, or the "Ur", should play a pivotal role when reconstructing quantum physics.

1.3.2 Basic notions

Following Hardy [96] we distinguish three types of devices in a typical laboratory. The preparation device prepares systems in some state. It has a set of switches on it for varying the state produced. After state preparation the system passes through a transformation device. It also has a set of switches on it for varying the transformation applied on the state. Finally, the system is measured in a measurement apparatus. It again has switches on it with which help an experimenter can choose different measurement settings. This device outputs classical data, e.g. a click in a detector or a spot on a observation screen.

We define the *state* of a system as that mathematical object from which one can determine the probability for any conceivable measurement. Physical theories can have enough structure that it is not necessary to give an exhaustive list of all probabilities for all possible measurements, but only a list of probabilities for some minimal subset of them. We refer to this subset as *fiducial* set. Therefore, the state is specified by a list of d (where d depends on dimension N) probabilities for a set of fiducial measurements: $\mathbf{p} = (p_1, \ldots, p_d)$. The state is *pure* if it is not a (convex) mixture of other states. The state is mixed if it is not pure. For example, the mixed state $\mathbf{p}$ generated by preparing state $\mathbf{p}_1$ with probability λ and $\mathbf{p}_2$ with probability $1 - \lambda$, is $\mathbf{p} = \lambda\mathbf{p}_1 + (1 - \lambda)\mathbf{p}_2$.

When we refer to an N-dimensional system, we assume that there are N states each of which identifies a different outcome of some measurement setting, in the sense that they return probability one for the outcome. We call this set a set of *basis* or *orthogonal states*. Basis states can be chosen to be pure. To see this assume that some mixed state

identifies one outcome. We can decompose the state into a mixture of pure states, each of which has to return probability one, and thus we can use one of them to be a basis state. We will show later that each pure state corresponds to a unique measurement outcome.

If the system in state $\mathbf{p}$ is incident on a transformation device, its state will be transformed to some new state $U(\mathbf{p})$. The transformation U is a linear function of the state $\mathbf{p}$ as it needs to preserve the linear structure of mixtures. For example, consider the mixed state $\mathbf{p}$ which is generated by preparing state $\mathbf{p}_1$ with probability λ and $\mathbf{p}_2$ with probability $1-\lambda$. Then, in each single run, either $\mathbf{p}_1$ or $\mathbf{p}_2$ is transformed and thus one has:

$$U(\lambda\mathbf{p}_1 + (1-\lambda)\mathbf{p}_2) = \lambda U(\mathbf{p}_1) + (1-\lambda)U(\mathbf{p}_2). \tag{1.21}$$

It is natural to assume that a composition of two or more transformations is again from a set of (reversible) transformations. This set forms some abstract group. Axiom 3 states that the transformations are reversible, i.e. for every U there is an inverse group element U^{-1}. Here we assume that every transformation has its matrix representation U and that there is an orthogonal representation of the group: there exists an invertible matrix S such that $O = SUS^{-1}$ is an orthogonal matrix, i.e. $O^{\mathrm{T}}O = \mathbb{1}$, for every U (We use the same notation both for the group element and for its matrix representation). This does not put severe restrictions to the group of transformations, as it is known that all compact groups have such a representation (the Schur-Auerbach lemma) [24]. Since the transformation keeps the probabilities in the range $[0, 1]$, it has to be a compact group [96]. All finite groups and all continuous Lie groups are therefore included in our consideration.

Given a measurement setting, the outcome probability P_{meas} can be computed by some function f of the state $\mathbf{p}$,

$$P_{\mathrm{meas}} = f(\mathbf{p}). \tag{1.22}$$

Like a transformation, the measurement cannot change the mixing coefficients in a mixture, and therefore the measured probability is a linear function of the state $\mathbf{p}$:

$$f(\lambda\mathbf{p}_1 + (1-\lambda)\mathbf{p}_2) = \lambda f(\mathbf{p}_1) + (1-\lambda)f(\mathbf{p}_2). \tag{1.23}$$

1.3.3 Elementary system: system of information capacity of 1 bit

A two-dimensional system has two distinguishable outcomes which can be identified by a pair of basis states $\{\mathbf{p}, \mathbf{p}^{\perp}\}$. The state is specified by d probabilities $\mathbf{p} = (p_1, ..., p_d)$ for d fiducial measurements, where p_i is probability for a particular outcome of the i-th fiducial measurement (the dependent probabilities $1 - p_i$ for the opposite outcomes

are omitted in the state description). Instead of using the probability vector $\mathbf{p}$ we will specify the state by its *Bloch representation* $\mathbf{x}$ defined as a vector with d components:

$$x_i = 2p_i - 1. \tag{1.24}$$

The mapping between the two different representations is an invertible linear map and therefore preserves the structure of the mixture $\lambda\mathbf{p}_1 + (1-\lambda)\mathbf{p}_2 \mapsto \lambda\mathbf{x}_1 + (1-\lambda)\mathbf{x}_2$.

It is convenient to define a *totaly mixed state* $\mathbf{E} = \frac{1}{\mathcal{N}} \sum_{x \in \mathcal{S}_{\text{pure}}} \mathbf{x}$, where $\mathcal{S}_{\text{pure}}$ denotes the set of pure states and $\mathcal{N}$ is the normalization constant. In the case of a continuous set of pure states the summation has to be replaced by a proper integral. It is easy to verify that $\mathbf{E}$ is a totally invariant state. This implies that every measurement and in particular the fiducial ones will return the same probability for all outcomes. In the case of a two-dimensional system this probability is $1/2$. Therefore, the Bloch vector of the totally mixed state is the zero-vector $\mathbf{E} = \vec{0}$.

The transformation U does not change the totaly mixed state, hence $U(\vec{0}) = \vec{0}$. The last condition together with the linearity condition (1.21) implies that any transformation is represented by some $d \times d$ real invertible matrix U. The same reasoning holds for measurements. Therefore, the measured probability is given by the formula:

$$P_{\text{meas}} = \frac{1}{2}(1 + \mathbf{r}^{\mathrm{T}}\mathbf{x}). \tag{1.25}$$

The vector $\mathbf{r}$ represents the outcome for the given measurement setting. For example, the vector $(1, 0, 0, \dots)$ represents one of the outcomes for the first fiducial measurement.

According to axiom 1 any state is a classical mixture of some pair of orthogonal states. For example, the totally mixed state is an equally weighted mixture of some orthogonal states $\vec{0} = \frac{1}{2}\mathbf{x} + \frac{1}{2}\mathbf{x}^{\perp}$. Take $\mathbf{x}$ to be the reference state. According to axiom 3 we can generate the full set of states by applying all possible transformations to the reference state. Since the totally mixed state is invariant under the transformations, the pair of orthogonal states is represented by a pair of antiparallel vectors $\mathbf{x}^{\perp} = -\mathbf{x}$. Consider the set $\mathcal{S}_{\text{pure}} = \{\, U\mathbf{x} \mid \forall U\}$ of all pure states generated by applying all transformations to the reference state. If one uses the orthogonal representation of the transformations, $U = S^{-1}OS$, which was introduced above, one maps $\mathbf{x} \mapsto S\mathbf{x}$ and $U \mapsto O$. Hence, the transformation $U\mathbf{x} \mapsto SU\mathbf{x} = OS\mathbf{x}$ is norm preserving. We conclude that all pure states are points on a d-dimensional ellipsoid described by $\|S\mathbf{x}\| = c$ with $c > 0$.

Now, we want to show that any vector $\mathbf{x}$ satisfying $\|S\mathbf{x}\| = c$ is a physical state and therefore the set of states has to be the whole ellipsoid. Let $\mathbf{x}$ be some vector satisfying $\|S\mathbf{x}\| = c$ and $\mathbf{x}(t) = t\mathbf{x}$ a line trough the origin (totaly mixed state) as given in Figure

1.5 (left). Within the set of pure states we can always find d linearly independent vectors $\{\mathbf{x}_1, \ldots, \mathbf{x}_d\}$. For each state $\mathbf{x}_i$ there is a corresponding orthogonal state $\mathbf{x}_i^\perp = -\mathbf{x}_i$ in a set of states. We can expand a point on the line into a linearly independent set of vectors: $\mathbf{x}(t) = t\sum_{i=1}^d c_i\mathbf{x}_i$. For sufficiently small t we can define a pair of non-negative numbers $\lambda_i(t) = \frac{1}{2}(\frac{1}{d} + tc_i)$ and $\lambda_i^\perp(t) = \frac{1}{2}(\frac{1}{d} - tc_i)$ with $\sum_i(\lambda_i(t) + \lambda_i^\perp(t)) = 1$ such that $\mathbf{x}(t)$ is a mixture $\mathbf{x}(t) = \sum_{i=1}^d \lambda_i(t)\mathbf{x}_i + \lambda_i^\perp(t)\mathbf{x}_i^\perp$ and therefore is a physical state. Then, according to axiom 1 there exists a pair of basis states $\{\mathbf{x}_0, -\mathbf{x}_0\}$ such that $\mathbf{x}(t)$ is a mixture of them

$$\mathbf{x}(t) = t\mathbf{x} = \alpha\mathbf{x}_0 + (1-\alpha)(-\mathbf{x}_0), \tag{1.26}$$

where $\alpha = \frac{1+t}{2}$ and $\mathbf{x} = \mathbf{x}_0$. This implies that $\mathbf{x}$ is a pure state and therefore all points of the ellipsoid are physical states.

For every pure state $\mathbf{x}$, there exists at least one measurement setting with the outcome $\mathbf{r}$ such that the outcome probability is one, hence $\mathbf{r}^{\mathrm{T}}\mathbf{x} = 1$. Let us define new coordinates $\mathbf{y} = \frac{1}{c}S\mathbf{x}$ and $\mathbf{m} = cS^{-1T}\mathbf{r}$ in the orthogonal representation. The set of pure states in the new coordinates is a $(d-1)$-sphere $\mathcal{S}^{d-1} = \{\mathbf{y} \mid \|\mathbf{y}\| = 1\}$ of the radius. The probability rule (1.25) remains unchanged in the new coordinates:

$$P_{\mathrm{meas}} = \frac{1}{2}(1 + \mathbf{m}^{\mathrm{T}}\mathbf{y}). \tag{1.27}$$

Thus, one has $\mathbf{m}^{\mathrm{T}}\mathbf{y} = 1$. Now, assume that $\mathbf{m} \neq \mathbf{y}$. Then $\|\mathbf{m}\| > 1$ and the vectors $\mathbf{m}$ and $\mathbf{y}$ span a two-dimensional plane as illustrated in Figure 1.5 (right). The set of pure states within this plane is a unit circle. Choose the pure state $\mathbf{y}'$ to be parallel to $\mathbf{m}$. Then the outcome probability is $P_{\mathrm{measur}} = \frac{1}{2}(1 + \|\mathbf{m}\|\|\mathbf{y}'\|) > 1$ which is non-physical, hence $\mathbf{m} = \mathbf{y}$. Therefore, to each pure state $\mathbf{y}$, we associate a measurement vector $\mathbf{m} = \mathbf{y}$ which identifies it. Equivalently, in the original coordinates, to each $\mathbf{x}$ we associate a measurement vector $\mathbf{r} = D\mathbf{x}$, where $D = \frac{1}{c^2}S^{\mathrm{T}}S$ is a positive, symmetric matrix. A proof of this relation for the restricted case of $d = 3$ can be found in Ref. [96].

From now one, instead of the measurement vector $\mathbf{r}$ we will use the pure state $\mathbf{x}$ which identifies it. When we say that the measurement along the state $\mathbf{x}$ is performed we mean the measurement given by $\mathbf{r} = D\mathbf{x}$. The measurement setting is given by a pair of measurement vectors $\mathbf{r}$ and $-\mathbf{r}$. The measured probability when the state $\mathbf{x}_1$ is measured along the state $\mathbf{x}_2$ follows from formula (1.25):

$$P(\mathbf{x}_1, \mathbf{x}_2) = \frac{1}{2}(1 + \mathbf{x}_1^{\mathrm{T}}D\mathbf{x}_2). \tag{1.28}$$

We can choose orthogonal eigenvectors of the matrix D as the fiducial set of states (measurements):

$$D\mathbf{x}_i = a_i\mathbf{x}_i, \tag{1.29}$$

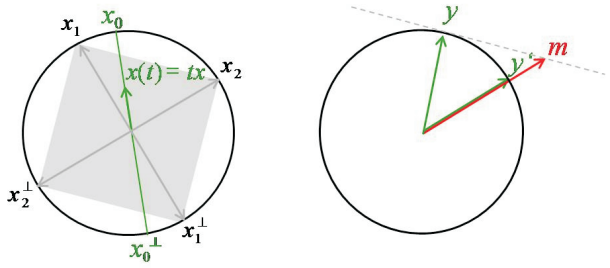

Figure 1.5: (Left) Illustration to the proof that the entire d-dimensional ellipsoid (here represented by a circle; $d = 2$) contains physical states. Consider a line $\mathbf{x}(t) = t\mathbf{x}$ through the origin. A point on the line can be expanded into a set of linearly independent vectors $\mathbf{x}_i$ (here $\mathbf{x}_1$ and $\mathbf{x}_2$). For sufficiently small t (i.e. when the line is within the gray square) the point $\mathbf{x}(t)$ can be represented as a convex mixture over $\mathbf{x}_i$ and their orthogonal vectors $\mathbf{x}_i^\perp$ and thus is a physical state. According to axiom 1, $\mathbf{x}(t)$ can be represented as a convex mixture of two orthogonal pure states $\mathbf{x}_0$ and $\mathbf{x}_0^\perp$: $\mathbf{x}(t) = t\mathbf{x} = \alpha\mathbf{x}_0 + (1-\alpha)(-\mathbf{x}_0)$, where $\mathbf{x} = \mathbf{x}_0$ (see text for details). This implies that every point in the ellipsoid is a physical state. (Right) Illustration to the proof that in the orthogonal representation the measurement vector $\mathbf{m}$ that identifies the state $\mathbf{x}$, i.e. for which the probability $P_{\text{meas}} = \frac{1}{2}(1 + \mathbf{m}^{\mathrm{T}}\mathbf{y}) = 1$, is identical to the state vector, $\mathbf{m} = \mathbf{y}$. Suppose that $\mathbf{m} \neq \mathbf{y}$, then $\|\mathbf{m}\| > 1$, since the state vector is normalized. But then the same measurement for state $\mathbf{y}'$ parallel to $\mathbf{m}$ would return a probability larger than 1, which is nonphysical. Thus $\mathbf{m} = \mathbf{y}$.

where a_i are eigenvalues of D. Since $\mathbf{x}_i$ are pure states, they satisfy $\mathbf{x}_i^{\mathrm{T}} D \mathbf{x}_j = \delta_{ij}$. The set of pure states becomes a unit sphere $\mathcal{S}^{d-1} = \{\mathbf{x} \mid \|\mathbf{x}\| = 1\}$ and the probability formula is reduced to

$$P(\mathbf{x}_1, \mathbf{x}_2) = \frac{1}{2}(1 + \mathbf{x}_1^{\mathrm{T}}\mathbf{x}_2). \tag{1.30}$$

This corresponds to a choice of a complete set of mutually complementary measurements (i.e. mutually unbiased basis sets) for the fiducial measurements. The states identifying outcomes of complementary measurements satisfy $P(\mathbf{x}_i, \mathbf{x}_j) = \frac{1}{2}$ for $i \neq j$. Two observables are said to be mutually complementary if complete certainty about one of the observables (one of two outcomes occurs with probability one) precludes any knowledge about the others (the probability for both outcomes is $1/2$). Given some state $\mathbf{x}$, the i-th fiducial measurement returns probability $p_i = \frac{1}{2}(1 + x_i)$. Therefore, x_i is a mean value of a dichotomic observable $\mathbf{b}_i = +1\mathbf{x}_i - 1\mathbf{x}_i^\perp$ with two possible outcomes $b_i = \pm 1$.

A theory in which the state space of the generalized bit is represented by a $(d-1)$-sphere has d mutually complementary observables. This is a characteristic feature of the theories and they can be ordered according to their number. For example, classical

physics has no complementary observables, real quantum mechanics has two, complex (standard) quantum mechanics has three (e.g. the spin projections of a spin-1/2 system along three orthogonal directions) and the one based on quaternions has five mutually complementary observables. Note that higher-order theories of a single generalized bit are such that the qubit theory can be embedded in them in the same way in which classical theory of a bit can be embedded in qubit theory itself.

Higher-order theories can have even better information processing capacity than quantum theory. For example, the computational abilities of the theories with $d = 2^r$ and $r \in N$ in solving the Deutsch-Josza type of problems increases with the number of mutually complementary measurements [146]. It is likely that the larger this number is the larger the error rate would be in secret key distribution in these theories, in a similar manner in which the 6-state is advantageous over the 4-state protocol in (standard) quantum mechanics. In the first case one uses all three mutually complementary observables and in the second one only two of them. (See Ref. [16] for a review on characterizing generalized probabilistic theories in terms of their information-processing power and Ref. [2] for investigating the same question in much more general framework of compact closed categories.)

A final remark on higher-order theories is of more speculative nature. In various approaches to quantum theory of gravity one predicts at the Planck scale the dimension of space-time to be different from 3 + 1 [6]. If one considers directional degrees of freedom (spin), then the $d - 1$-sphere (Bloch sphere) might be interpreted as the state space of a spin system embedded in real (ordinary) space of dimension d, in general different than 3 which is the special case of quantum theory.

The reversible transformation R preserves the purity of state $||R\mathbf{x}|| = ||x||$ and therefore R is an orthogonal matrix. We have shown that the state space is the full $(d - 1)$-sphere. According to axiom 3 the set of transformations must be rich enough to generate the full sphere. If $d = 1$ (classical bit), the group of transformations is discrete and contains only the identity and the bit-flip. If $d > 1$, the group is continuous and is some subgroup of the orthogonal group O(d). Every orthogonal matrix has determinant either 1 or -1. The orthogonal matrices with determinant 1 form a normal subgroup of O(d), known as the special orthogonal group SO(d). The group O(d) has two connected components: the identity component which is the SO(d) group, and the component formed by orthogonal matrices with determinant -1. Since every two points on the $(d - 1)$-sphere are connected by some transformation, the group of transformations is at least the SO(d) group. If we include even a single transformation with determinant -1, the set of transformations becomes the entire O(d) group. (Later we

will show that only some d are in agreement with our three axioms and for these d's the set of physical transformations will be shown to be the SO(d) group).

1.3.4 Composite system and the notion of locality

We now introduce a description of composite systems. We assume that when one combines two systems of dimension L_1 and L_2 into a composite one, one obtains a system of dimension $L_1 L_2$. Consider a composite system consisting of two geneneralized bits and choose a set of d complementary measurements on each subsystem as fiducial measurements. According to axiom 2 the state of the composite system is completely determined by a set of real parameters obtainable from local measurements on the two generalized bits and their correlations. We obtain $2d$ independent real parameters from the set of local fiducial measurements and additional d^2 parameters from correlations between them. This gives altogether $d^2 + 2d = (d+1)^2 - 1$ parameters. They are the components x_i, y_i, $i \in \{1, ..., d\}$, of the local Bloch vectors and T_{ij} of the correlation tensor:

$$x_i = p^{(i)}(A = 1) - p^{(i)}(A = -1), \tag{1.31}$$

$$y_j = p^{(j)}(B = 1) - p^{(j)}(B = -1), \tag{1.32}$$

$$T_{ij} = p^{(ij)}(AB = 1) - p^{(ij)}(AB = -1). \tag{1.33}$$

Here, for example, $p^{(i)}(A = 1)$ is the probability to obtain outcome $A = 1$ when the i-th measurement is performed on the first subsystem and $p^{(ij)}(AB = 1)$ is the joint probability to obtain correlated results (i.e. either $A = B = +1$ or $A = B = -1$) when the i-th measurement is performed on the first subsystem and the j-th measurement on the second one.

Note that axiom 2 "The state of a composite system is completely determined by local measurements on its subsystems and their correlations" is formulated in a way that the non-signaling condition is implicitly assumed to hold. This is because it is sufficient to speak about "local measurements" alone without specifying the choice of measurement setting on the other, potentially distant, subsystem. Therefore, x_i does not depend on j, and y_j does not depend on i.

We represent a state by the triple $\psi = (\mathbf{x}, \mathbf{y}, T)$, where $\mathbf{x}$ and $\mathbf{y}$ are the local Bloch vectors and T is a $d \times d$ real matrix representing the correlation tensor. The product (separable) state is represented by $\psi_p = (\mathbf{x}, \mathbf{y}, T)$, where $T = \mathbf{x}\mathbf{y}^{\mathrm{T}}$ is of product form, because the correlations are just products of the components of the local Bloch vectors. We call the pure state *entangled* if it is not a product state.

The measured probability is a linear function of the state ψ. If we prepare totaly mixed states of the subsystems $(0,0,0)$, the probability for any outcome of an arbitrary measurement will be $1/4$. Therefore, the outcome probability can be written as:

$$P_{\text{measur}} = \frac{1}{4}(1 + (r, \psi)), \tag{1.34}$$

where $r = (\mathbf{r}_1, \mathbf{r}_2, K)$ is a measurement vector associated to the observed outcome and $(..., ...)$ denotes the scalar product:

$$(r, \psi) = \mathbf{r}_1^{\mathrm{T}}\mathbf{x} + \mathbf{r}_2^{\mathrm{T}}\mathbf{y} + \mathrm{Tr}(K^{\mathrm{T}}T). \tag{1.35}$$

Now, assume that $r = (\mathbf{r}_1, \mathbf{r}_2, K)$ is associated to the outcome which is identified by some product state $\psi_p = (\mathbf{x}_0, \mathbf{y}_0, T_0)$. If we preform a measurement on the arbitrary product state $\psi = (\mathbf{x}, \mathbf{y}, T)$, the outcome probability has to factorize into the product of the local outcome probabilities of the form (1.30):

$$\begin{aligned} P_{\text{measur}} &= \frac{1}{4}(1 + \mathbf{r}_1^{\mathrm{T}}\mathbf{x} + \mathbf{r}_2^{\mathrm{T}}\mathbf{y} + \mathbf{x}^{\mathrm{T}}K\mathbf{y}) && (1.36)\\ &= P_1(\mathbf{x}_0, \mathbf{x})P_2(\mathbf{y}_0, \mathbf{y}) && (1.37)\\ &= \frac{1}{2}(1 + \mathbf{x}_0^{\mathrm{T}}\mathbf{x})\frac{1}{2}(1 + \mathbf{y}_0^{\mathrm{T}}\mathbf{y}) && (1.38)\\ &= \frac{1}{4}(1 + \mathbf{x}_0^{\mathrm{T}}\mathbf{x} + \mathbf{y}_0^{T}\mathbf{y} + \mathbf{x}^{\mathrm{T}}\mathbf{x}_0\mathbf{y}_0^{\mathrm{T}}\mathbf{y}), && (1.39) \end{aligned}$$

which holds for all $\mathbf{x}, \mathbf{y}$. Therefore we have $r = \psi_p$. For each product state ψ_p there is a unique outcome $r = \psi_p$ which identifies it. We will later show that correspondence $r = \psi$ holds for *all* pure states ψ.

If we preform local transformations R_1 and R_2 on the subsystems, the global state $\psi = (\mathbf{x}, \mathbf{y}, T)$ is transformed to

$$(R_1, R_2)\psi = (R_1\mathbf{x}, R_2\mathbf{y}, R_1 T R_2^{\mathrm{T}}). \tag{1.40}$$

T is a real matrix and we can find its singular value decomposition $\mathrm{diag}[t_1, \ldots, t_d] = R_1 T R_2^{\mathrm{T}}$, where R_1, R_2 are orthogonal matrices which can be chosen to have determinant 1. Therefore, we can choose the local bases such that correlation tensor T is a diagonal matrix:

$$(R_1, R_2)(\mathbf{x}, \mathbf{y}, T) = (R_1\mathbf{x}, R_2\mathbf{y}, \mathrm{diag}[t_1, \ldots, t_d]). \tag{1.41}$$

The last expression is called *Schmidt decomposition* of the state.

The local Bloch vectors satisfy $\|\mathbf{x}\|, \|\mathbf{y}\| \leq 1$ which implies a bound on the correlation $\|T\| \geq 1$ for all pure states. The following lemma identifies a simple entanglement witness for pure states. The proof of this and all subsequent lemmas is given in the Appendix.

Lemma 1. *The lower bound* $||T|| = 1$ *is saturated, if and only if the state is a product state* $T = \mathbf{x}\mathbf{y}^{\mathrm{T}}$.

Recall that for every transformation U we can find its orthogonal representation $U = SOS^{-1}$ (the Schur-Auerbach lemma), where S is an invertible matrix and $O^{\mathrm{T}}O = \mathbb{1}$. The matrix S is characteristic of the representation and should be the same for all transformations U. If we choose some local transformation $U = (R_1, R_2)$, U will be orthogonal and thus we can choose to set $S = \mathbb{1}$. The representation of transformations is orthogonal, therefore they are norm preserving. By applying simultaneously all (local and non-local) transformations U to some product state (the reference state) ψ and to the measurement vector which identifies it, $r = \psi$, we generate the set of all pure states and corresponding measurement vectors. Since we have $1 = P(r = \psi, \psi) = P(Ur, U\psi)$, correspondence $r = \psi$ holds for any pure state ψ. Instead of the measurement vector r in formula (1.34) we use the pure state which identifies it. If the state $\psi_1 = (\mathbf{x}_1, \mathbf{y}_1, T_1)$ is prepared and measurement along the state $\psi_2 = (\mathbf{x}_2, \mathbf{y}_2, T_2)$ is performed, the measured probability is given by

$$P_{12}(\psi_1, \psi_2) = \frac{1}{4}(1 + \mathbf{x}_1^{\mathrm{T}}\mathbf{x}_2 + \mathbf{y}_1^{\mathrm{T}}\mathbf{y}_2 + \mathrm{Tr}(T_1^{\mathrm{T}}T_2)). \tag{1.42}$$

The set of pure states obeys $P_{12}(\psi, \psi) = 1$. We can define the normalization condition for pure states $P_{12}(\psi, \psi) = \frac{1}{4}(1 + ||\mathbf{x}||^2 + ||\mathbf{y}||^2 + ||T||^2) = 1$ where $||T||^2 = \mathrm{Tr}(T^{\mathrm{T}}T)$. Therefore we have:

$$||\mathbf{x}||^2 + ||\mathbf{y}||^2 + ||T||^2 = 3, \tag{1.43}$$

for all pure states.

An interesting observation can be made here. Although seemingly axiom 2 does not imply any strong prior restrictions to d, we surprisingly have obtained the explicit number 3 in the normalization condition (1.43). As we will see soon this relation will play an important role in deriving $d = 3$ as the only non-classical solution consistent with the axioms.

1.3.5 The main proofs

We will now show that only classical probability theory and quantum theory are in agreement with the three axioms.

Ruling out the d even case

Let us assume the total inversion $E\mathbf{x} = -\mathbf{x}$ being a physical transformation. Let $\psi = (\mathbf{x}, \mathbf{y}, T)$ be a pure state of composite system. We apply total inversion to one of the

subsystems and obtain the state $\psi' = (E, \mathbb{1})(\mathbf{x}, \mathbf{y}, T) = (-\mathbf{x}, \mathbf{y}, -T)$. The probability

$$P_{12}(\psi, \psi') = \frac{1}{4}(1 - \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - \|T\|^2) \quad (1.44)$$

$$= \frac{1}{2}(\|\mathbf{y}\|^2 - 1) \quad (1.45)$$

has to be nonnegative and therefore we have $\|\mathbf{y}\| = 1$. Similarly, we apply $(\mathbb{1}, E)$ to ψ and obtain $\|\mathbf{x}\| = 1$. Since the local vectors are of the unit norm we have $\|T\| = 1$ and thus, according to lemma 1, the state ψ is a product state. We conclude that no entangled states can exist if E is a physical transformation. As we will soon see, according to axiom 1 entangled states must exist. Thus, E cannot represent a physical transformation. We will now show that this implies that d has to be odd. Recall that the set of transformations is at least the SO(d) group. d cannot be even since E would have unit determinant and would belong to SO(d). d has to be odd in which case E has determinant -1. The set of physical transformations is the SO(d) group.

Ruling out the $d > 3$ case.

Let us define one basis set of two generalized bit product states:

$$\psi_1 = (\mathbf{e}_1, \mathbf{e}_1, T_0 = \mathbf{e}_1\mathbf{e}_1^{\mathrm{T}}) \quad (1.46)$$

$$\psi_2 = (-\mathbf{e}_1, -\mathbf{e}_1, T_0) \quad (1.47)$$

$$\psi_3 = (-\mathbf{e}_1, \mathbf{e}_1, -T_0) \quad (1.48)$$

$$\psi_4 = (\mathbf{e}_1, -\mathbf{e}_1, -T_0) \quad (1.49)$$

with $\mathbf{e}_1 = (1, 0, \ldots, 0)^{\mathrm{T}}$. Now, we define two subspaces S_{12} and S_{34} spanned by the states ψ_1, ψ_2 and ψ_3, ψ_4, respectively. Axiom 1 states that these two subspaces behave like one-bit spaces, therefore they are isomorphic to the $(d-1)$-sphere $S_{12} \cong S_{34} \cong \mathcal{S}^{d-1}$. The state ψ belongs to S_{12} if and only if the following holds:

$$P_{12}(\psi, \psi_1) + P_{12}(\psi, \psi_2) = 1. \quad (1.50)$$

Since the $\psi_1, \ldots, \psi_4$ form a complete basis set, we have

$$P_{12}(\psi, \psi_3) = 0, \quad P_{12}(\psi, \psi_4) = 0. \quad (1.51)$$

A similar reasoning holds for states belonging to the S_{34} subspace. Since the states $\psi \in S_{12}$ and $\psi' \in S_{34}$ are perfectly distinguishable in a single shot experiment, we have $P_{12}(\psi, \psi') = 0$. Therefore, S_{12} and S_{34} are orthogonal subspaces.

Axiom 1 requires the existence of entangled states as it is apparent from the following Lemma 2.

Lemma 2. *The only product states belonging to S_{12} are ψ_1 and ψ_2.*

We define a local mapping between orthogonal subspaces S_{12} and S_{34}. Let the state $\psi = (\mathbf{x}, \mathbf{y}, T) \in S_{12}$, with $\mathbf{x} = (x_1, x_2, \ldots, x_d)^{\mathrm{T}}$ and $\mathbf{y} = (y_1, y_2, \ldots, y_d)^{\mathrm{T}}$. Consider the one-bit transformation R with the property $R\mathbf{e}_1 = -\mathbf{e}_1$. The local transformation of this type maps the state from S_{12} to S_{34} as shown by the following lemma:

Lemma 3. *If the state $\psi \in S_{12}$, then $\psi' = (R, \mathbb{1})\psi \in S_{34}$ and $\psi'' = (\mathbb{1}, R)\psi \in S_{34}$.*

Let us define $\mathbf{T}_i^{(x)} = (T_{i1}, \ldots, T_{id})$ and $\mathbf{T}_i^{(y)} = (T_{1i}, \ldots, T_{di})^{\mathrm{T}}$. The correlation tensor can be rewritten in two different ways:

$$T = \begin{pmatrix} \mathbf{T}_1^{(x)} \\ \mathbf{T}_2^{(x)} \\ \vdots \\ \mathbf{T}_d^{(x)} \end{pmatrix} \text{ or } \mathrm{T} = \begin{pmatrix} \mathbf{T}_1^{(y)} & \mathbf{T}_2^{(y)} & \ldots & \mathbf{T}_d^{(y)} \end{pmatrix}. \tag{1.52}$$

Consider now the case $d > 3$. We define local transformations R_i flipping the first and i-th coordinate and R_{jkl} flipping the first and j-th, k-th, and l-th coordinate with $j \neq k \neq l \neq 1$. Let $\psi = (\mathbf{x}, \mathbf{y}, (\mathbf{T}_1^{(x)}, \ldots, \mathbf{T}_d^{(x)})^{\mathrm{T}})$ belong to S_{12}. According to Lemma 2, the states $\psi_i = (R_i, \mathbb{1})\psi$ and $\psi_{jkl} = (R_{jkl}, \mathbb{1})\psi$ belong to S_{34}, therefore $P_{12}(\psi, \psi_i) = 0$ and $P_{12}(\psi, \psi_{jkl}) = 0$. We have:

$$\begin{aligned} 0 &= P_{12}(\psi, \psi_i) && (1.53)\\ &\quad 1 - x_1^2 + x_2^2 + \cdots - x_i^2 + \cdots + x_d^2 + \|\mathbf{y}\|^2 && (1.54)\\ &\quad -\|\mathbf{T}_1^{(x)}\|^2 + \|\mathbf{T}_2^{(x)}\|^2 + \cdots - \|\mathbf{T}_i^{(x)}\|^2 + \cdots + \|\mathbf{T}_d^{(x)}\|^2 && (1.55)\\ &= 1 - 2x_1^2 - 2x_i^2 - 2\|\mathbf{T}_1^{(x)}\|^2 - 2\|\mathbf{T}_i^{(x)}\|^2 + \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 + \|T\|^2 \\ &= 2(2 - x_1^2 - x_i^2 - \|\mathbf{T}_1^{(x)}\|^2 - \|\mathbf{T}_i^{(x)}\|^2). && (1.56) \end{aligned}$$

Similarly, we expand $P_{12}(\psi, \psi_{jkl}) = 0$ and together with the last equation we obtain:

$$\begin{aligned} &x_1^2 + x_i^2 + \|\mathbf{T}_1^{(x)}\|^2 + \|\mathbf{T}_i^{(x)}\|^2 = 2 && (1.57)\\ &x_1^2 + x_j^2 + x_k^2 + x_l^2 + \|\mathbf{T}_1^{(x)}\|^2 + \|\mathbf{T}_j^{(x)}\|^2 + \|\mathbf{T}_k^{(x)}\|^2 + \|\mathbf{T}_l^{(x)}\|^2 = 2. \end{aligned}$$

Since this has to hold for all i, j, k, l we have:

$$\begin{aligned} &x_2 = x_3 = \cdots = x_d = 0 && (1.58)\\ &\mathbf{T}_2^{(x)} = \mathbf{T}_3^{(x)} = \cdots = \mathbf{T}_d^{(x)} = 0. && (1.59) \end{aligned}$$

We repeat this kind of reasoning for the transformations $(\mathbb{1}, R_i)$ and $(\mathbb{1}, R_{jkl})$ and obtain:

$$\begin{aligned} &y_1^2 + y_i^2 + \|\mathbf{T}_1^{(y)}\|^2 + \|\mathbf{T}_i^{(y)}\|^2 = 2 && (1.60)\\ &y_1^2 + y_j^2 + y_k^2 + y_l^2 + \|\mathbf{T}_1^{(y)}\|^2 + \|\mathbf{T}_j^{(y)}\|^2 + \|\mathbf{T}_k^{(y)}\|^2 + \|\mathbf{T}_l^{(y)}\|^2 = 2. \end{aligned}$$

Therefore, we have

$$y_2 = y_3 = \cdots = y_d = 0 \tag{1.61}$$

$$\mathbf{T}_2^{(y)} = \mathbf{T}_3^{(y)} = \cdots = \mathbf{T}_d^{(y)} = 0. \tag{1.62}$$

The only non-zero element of the correlation tensor is T_{11} and it has to be exactly 1, since $\|T\| \geq 1$. This implies that ψ is a product state, furthermore $\psi = \psi_1$ or $\psi = \psi_2$.

This concludes our proof that only the cases $d = 1$ and $d = 3$ are in agreement with our three axioms. To distinguish between the two cases, one can invoke the continuity axiom (3') and proceed as in the reconstruction given by Hardy [96].

1.3.6 "Two" quantum mechanics

We now obtain two solutions for the theory of a composite system consisting of two bits in the case when $d = 3$. One of them corresponds to the standard quantum theory of two qubits, the other one to its "mirror" version in which the states are obtained from the ones from the standard theory by partial transposition. Both solutions are regular as far as one considers composite systems of two bits, but the "mirror" one cannot be consistently constructed already for systems of three bits.

Two conditions (1.50) and (1.51) put the constraint to the form of ψ:

$$x_1 = -y_1, \quad T_{11} = 1. \tag{1.63}$$

The subspace S_{12} is isomorphic to the sphere $\mathcal{S}^2$. Let us choose ψ complementary to the one bit basis $\{\psi_1, \psi_2\}$ in S_{12}. We have $P_{12}(\psi, \psi_1) = P_{12}(\psi, \psi_2) = 1/2$ and thus $x_1 = y_1 = 0$. For simplicity we write ψ in the form:

$$\psi = \left(\begin{pmatrix} 0 \\ \mathbf{x} \end{pmatrix}, \begin{pmatrix} 0 \\ \mathbf{y} \end{pmatrix}, \begin{pmatrix} 1 & \mathbf{T}_y^{\mathrm{T}} \\ \mathbf{T}_x & T \end{pmatrix} \right), \tag{1.64}$$

with $\mathbf{x} = (x_2, x_3)^{\mathrm{T}}$, $\mathbf{y} = (y_2, y_3)^{\mathrm{T}}$, $\mathbf{T}_y = (T_{12}, T_{13})^{\mathrm{T}}$, $\mathbf{T}_x = (T_{21}, T_{31})^{\mathrm{T}}$ and $T = \begin{pmatrix} T_{22} & T_{23} \\ T_{32} & T_{33} \end{pmatrix}$.

Let $R(\phi)$ be a rotation around the $\mathbf{e}_1$ axis. This transformation keeps S_{12} invariant. Now, we show that the state ψ as given by equation (1.64) cannot be invariant under local transformation $(\mathbb{1}, R(\phi))$. To prove this by *reductio ad absurdum* suppose the opposite, i.e. that $(\mathbb{1}, R(\phi))\psi = \psi$. We have three conditions

$$R(\phi)\mathbf{y} = \mathbf{y}, \quad \mathbf{T}_y^{\mathrm{T}} R^{\mathrm{T}}(\phi) = \mathbf{T}_y^{\mathrm{T}}, \quad T R^{\mathrm{T}}(\phi) = T, \tag{1.65}$$

which implies $\mathbf{y} = 0$, $\mathbf{T}_y^{\mathrm{T}} = 0$ and $T = 0$ thus

$$\psi = \left(\begin{pmatrix} 0 \\ x_2 \\ x_3 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ T_2 & 0 & 0 \\ T_3 & 0 & 0 \end{pmatrix} \right). \tag{1.66}$$

According to equations (1.57) and (1.60) we can easily check that $\|\mathbf{x}\| = 1$, and thus ψ is locally equivalent to the state:

$$\psi' = \left(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ T_2' & 0 & 0 \\ T_3' & 0 & 0 \end{pmatrix} \right). \tag{1.67}$$

Let $\chi_1 = (-\mathbf{e}_3, \mathbf{e}_1, -\mathbf{e}_3\mathbf{e}_1^{\mathrm{T}})$ and $\chi_2 = (-\mathbf{e}_3, -\mathbf{e}_1, \mathbf{e}_3\mathbf{e}_1^{\mathrm{T}})$. The two conditions $P(\psi', \chi_1) \geq 0$ and $P(\psi', \chi_2) \geq 0$ become

$$\frac{1}{4}(1 - 1 - T_3') = -\frac{1}{4}T_3' \geq 0 \tag{1.68}$$

$$\frac{1}{4}(1 - 1 + T_3') = \frac{1}{4}T_3' \geq 0 \tag{1.69}$$

and thus $T_3' = 0$. The normalization condition (1.43) gives $T_2' = \pm 1$. The state ψ' is not physical. This can be seen when one performs the rotation $(R, \mathbb{1})$ where

$$R = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{1.70}$$

The transformed correlation tensor has a component $\sqrt{2}$ which is non-physical. Therefore, the transformation $(\mathbb{1}, R(\phi))\psi$ draws a full circle of pure states in a plane orthogonal to ψ_1 within the subspace S_{12}. Similarly, the transformation $(R(\phi), \mathbb{1})$ draws the same set of pure states when applied to ψ. Hence, for every transformation $(\mathbb{1}, R(\phi_1))$ there exists a transformation $(R(\phi_2), \mathbb{1})$ such that $(\mathbb{1}, R(\phi_1))\psi = (R(\phi_2), \mathbb{1})\psi$. This gives us a set of conditions:

$$R(\phi_2)\mathbf{x} = \mathbf{x} \tag{1.71}$$

$$R(\phi_1)\mathbf{y} = \mathbf{y} \tag{1.72}$$

$$R(\phi_2)\mathbf{T}_x = \mathbf{T}_x \tag{1.73}$$

$$\mathbf{T}_y^{\mathrm{T}} R^{\mathrm{T}}(\phi_1) = \mathbf{T}_y^{\mathrm{T}} \tag{1.74}$$

$$R(\phi_2)T = TR^{\mathrm{T}}(\phi_1), \tag{1.75}$$

QM	xx	yy	zz
Φ^+	+1	-1	+1
Φ^-	-1	+1	+1
Ψ^+	+1	+1	-1
Ψ^-	-1	-1	-1

MQM	xx	yy	zz
Φ^+_{PT}	-1	+1	-1
Φ^-_{PT}	+1	-1	-1
Ψ^+_{PT}	-1	-1	+1
Ψ^-_{PT}	+1	+1	+1

Figure 1.6: Correlations between results obtained in measurements of two bits in a maximal entangled (Bell's) state in standard quantum mechanics (Left) and "mirror quantum mechanics" (Right) along x, y and z directions. Why do we never see correlations as given in the table on the right? The opposite sign of correlations on the right and on the left is not a matter of convention or labeling of outcomes. If one can transport the two bits parallel to the same detector, one can distinguish operationally between the two types of correlations [173].

which are fulfilled if $\mathbf{x} = \mathbf{y} = \mathbf{T}_x = \mathbf{T}_y = 0$ and $T = \mathrm{diag}[T_1, T_2]$. Equation (1.57) gives $T_2^2 = T_3^2 = 1$ and we finally end up with two different solutions:

$$\psi_{\mathrm{QM}} = (0, 0, \mathrm{diag}[1, -1, 1]) \quad \vee \quad \psi_{\mathrm{MQM}} = (0, 0, \mathrm{diag}[1, 1, 1]). \tag{1.76}$$

The first "M" in ψ_{MQM} stands for "mirror". The two solutions are incompatible and cannot coexist within the same theory. The first solution corresponds to the triplet state ϕ^+ of ordinary quantum mechanics. The second solution is a totally invariant state and has a negative overlap with, for example, the singlet state ψ^- for which $T = \mathrm{diag}[-1, -1, -1]$. That is, if the system were prepared in one of the two states and the other one were measured, the probability would be negative. Nevertheless, both solutions are regular at the level of two bits. The first belongs to ordinary quantum mechanics with the singlet in the "antiparallel" subspace S_{34} and the second solution is "the singlet state in the parallel subspace" S_{12}. We will show that one can build the full state space, transformations and measurements in both cases. The states from one quantum mechanics can be obtained from the other by partial transposition $\psi^{\mathrm{PT}}_{\mathrm{QM}} = \psi_{\mathrm{MQM}}$. In particular, the four maximal entangled states (Bell states) from "mirror quantum mechanics" have correlations of the opposite sign of those from the standard quantum mechanics (see Figure 4).

Now we show that the theory with "mirror states" is physically inconsistent when applied to composite system of three bits. Let us first derive the full set of states and transformations for two qubits in standard quantum mechanics. We have seen that the state ψ_{QM} belongs to the subspace S_{12}, and furthermore, that it is complementary (within S_{12}) to the product states ψ_1 and ψ_2. The totally mixed state within the S_{12} subspace is $E_{12} = \frac{1}{2}\psi_1 + \frac{1}{2}\psi_2$. The states ψ_1 and ψ_{QM} span one two-dimensional plane,

and the set of pure states within this plane is a circle:

$$\psi(x) = E_{12} + \cos x\,(\psi_1 - E_{12}) + \sin x\,(\psi_{\rm QM} - E_{12}) \quad (1.77)$$

$$= (\cos x\,\mathbf{e}_1, \cos x\,\mathbf{e}_1, \mathrm{diag}[1, -\sin x, \sin x]). \quad (1.78)$$

We can apply a complete set of local transformations to the set $\psi(x)$ to obtain the set of all pure two-qubit states. Let us represent a pure state $\psi = (\mathbf{x}, \mathbf{y}, T)$ by the 4×4 Hermitian matrix ρ:

$$\rho = \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} + \sum_{i=1}^{3} x_i \sigma_i \otimes \mathbb{1} + \sum_{i=1}^{3} y_i \mathbb{1} \otimes \sigma_i + \sum_{i,j=1}^{3} T_{ij} \sigma_i \otimes \sigma_j), \quad (1.79)$$

where σ_i, $i \in \{1, 2, 3\}$, are the three Pauli matrices. It is easy to show that the set of states (1.77) corresponds to the set of one-dimensional projectors $|\psi(x)\rangle\langle\psi(x)|$, where $|\psi(x)\rangle = \cos\frac{x}{2}|00\rangle + \sin\frac{x}{2}|11\rangle$. The action of local transformations $(R_1, R_2)\psi$ corresponds to local unitary transformation $U_1 \otimes U_2 |\psi\rangle\langle\psi| U_1^\dagger \otimes U_2^\dagger$, where the correspondence between U and R is given by the isomorphism between the groups SU(2) and SO(3):

$$U\rho U^\dagger = \frac{1}{2}\left(\mathbb{1} + \sum_{i=1}^{3}\left(\sum_{j=1}^{3} R_{ij} x_j\right)\sigma_i\right). \quad (1.80)$$

Here $R_{ij} = \mathrm{Tr}(\sigma_i U \sigma_j U^\dagger)$ and $x_i = \mathrm{Tr}\sigma_i\rho$. When we apply a complete set of local transformations to the states $|\psi(x)\rangle$ we obtain the whole set of pure states for two qubits. The group of transformations is the set of unitary transformations SU(4).

The set of states from "mirror quantum mechanics" can be obtained by applying partial transposition to the set of quantum states. Formally, partial transposition with respect to subsystem 1 is defined by action on a set of product operators:

$$\mathrm{PT}_1(\rho_1 \otimes \rho_2) = \rho_1^{\rm T} \otimes \rho_2. \quad (1.81)$$

where ρ_1 and ρ_2 are arbitrary operators. Similarly, we can define the partial transposition with respect to subsystem 2, PT_2. To each unitary transformation U in quantum mechanics we define the corresponding transformation in "mirror mechanics", e.g. with respect to subsystem 1: $\mathrm{PT}_1 U \mathrm{PT}_1$. Therefore, the set of transformations is a conjugate group $\mathrm{PT}_1\mathrm{SU}(4)\mathrm{PT}_1 := \{\mathrm{PT}_1 U \mathrm{PT}_1 \mid U \in \mathrm{SU}(4)\}$. Note that we could equally have chosen to apply partial transposition with respect to subsystem 2, and would obtain the same set of states. In fact, one can show that $\mathrm{PT}_1 U \mathrm{PT}_1 = \mathrm{PT}_2 U^* \mathrm{PT}_2$, where U^* is a conjugate unitary transformation (see Lemma 4 in the Appendix). Therefore, the two conjugate groups are the same $\mathrm{PT}_1\mathrm{SU}(4)\mathrm{PT}_1 = \mathrm{PT}_2\mathrm{SU}(4)\mathrm{PT}_2$. We can generate

the set of "mirror states" by applying all the transformations PTUPT to some product state, regardless of which particular partial transposition is used.

Now, we show that "mirror mechanics" cannot be consistently extended to composite systems consisting of three bits. Let $\psi_p = (\mathbf{x}, \mathbf{y}, \mathbf{z}, T_{12}, T_{13}, T_{23}, T_{123})$ be some product state of three bits, where $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ are local Bloch vectors, T_{12}, T_{13}, T_{23} and T_{123} are two- and three-body correlation tensors, respectively. We can apply the transformations PTU_{ij}PT to a composite system of i and j, and we are free to choose with respect to which subsystem (i or j) to take the partial transposition. Furthermore, we can combine transformations in 12 and 13 subsystems such that the resulting state is genuine three-partite entangled, and we can choose to partially transpose subsystem 2 in both cases. We obtain the transformation

$$\begin{aligned} U_{123} &= \mathrm{PT}_2 U_{12} \mathrm{PT}_2 \mathrm{PT}_2 U_{23} \mathrm{PT}_2 && (1.82) \\ &= \mathrm{PT}_2 U_{12} U_{23} \mathrm{PT}_2. && (1.83) \end{aligned}$$

When we apply U_{123} to ψ_p we obtain the state $\mathrm{PT}_2 U_{12} U_{23} \phi_p$, where $\phi_p = \mathrm{PT}_2 \psi_p$ is again some product state. The state $U_{12} U_{23} \phi_p$ is a quantum three qubit state. Since states ψ_p and ϕ_p are product states and do belong to standard quantum states, we can use the formalism of quantum mechanics and denote them as $|\psi_p\rangle$ and $|\phi_p\rangle$. Furthermore, since the state $|\psi_p\rangle$ is an arbitrary product state, without loss of generality we set $|\phi_p\rangle = |0\rangle|0\rangle|0\rangle$. We can choose U_{12} and U_{23} such that:

$$\begin{aligned} U_{12}|0\rangle|0\rangle &= |0\rangle|0\rangle && (1.84) \\ U_{12}|0\rangle|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) && (1.85) \\ U_{23}|0\rangle|0\rangle &= \frac{1}{\sqrt{3}}|0\rangle|1\rangle + \sqrt{\frac{2}{3}}|1\rangle|0\rangle. && (1.86) \end{aligned}$$

This way we can generate the W-state

$$\begin{aligned} |W\rangle &= U_{12} U_{23} |0\rangle|0\rangle|0\rangle && (1.87) \\ &= \frac{1}{\sqrt{3}}(|0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |1\rangle|0\rangle|0\rangle). && (1.88) \end{aligned}$$

When we apply partial transposition with respect to subsystem 2, we obtain the corresponding "mirror W-state" which we denote as W_{M}-state, $W_{\mathrm{M}} = \mathrm{PT}_2 W$. The local Bloch vectors and two-body correlation tensors for the W state are

$$\begin{aligned} \mathbf{x} = \mathbf{y} = \mathbf{z} &= (0, 0, \tfrac{1}{3})^{\mathrm{T}}, && (1.89) \\ T_{12} = T_{13} = T_{23} &= \mathrm{diag}[\tfrac{2}{3}, \tfrac{2}{3}, -\tfrac{1}{3}], && (1.90) \end{aligned}$$

where $|0\rangle$ corresponds to result +1. Consequently, the local Bloch vectors and the correlation tensor for W_{M}-state are

$$\mathbf{x} = \mathbf{y} = \mathbf{z} = (0, 0, \tfrac{1}{3})^{\mathrm{T}}, \tag{1.91}$$

$$T_{12} = T_{23} = \mathrm{diag}[\tfrac{2}{3}, -\tfrac{2}{3}, -\tfrac{1}{3}], \tag{1.92}$$

$$T_{13} = \mathrm{diag}[\tfrac{2}{3}, \tfrac{2}{3}, -\tfrac{1}{3}]. \tag{1.93}$$

The asymmetry in the signs of correlations in the tensors T_{12}, T_{23} and T_{13} leads to inconsistencies because they define three different reduced states $\psi_{ij} = (\mathbf{x}_i, \mathbf{x}_j, T_{ij})$, $ij \in \{12, 23, 13\}$, which cannot coexist within a single theory. The states ψ_{12} and ψ_{23} belong to "mirror quantum mechanics", while the state ψ_{13} belongs to ordinary quantum mechanics. To see this, take the state $\psi = (0, 0, \mathrm{diag}[-1, -1, 1])$ which is locally equivalent to state $\psi_{\mathrm{MQM}} = (0, 0, \mathbb{1})$. The overlap (measured probability) between the states ψ_{13} and ψ is negative

$$P(\psi, \psi_{13}) = \frac{1}{4}(1 - \frac{2}{3} - \frac{2}{3} - \frac{1}{3}) = -\frac{1}{6}. \tag{1.94}$$

We conclude that "mirror quantum mechanics" – while being a perfectly regular solution for a theory of two bits – cannot be consistently extended to also describe systems consisting of many bits. This also answers the question why we find in nature only four types of correlations as given in the table (Figure 4) on the left, rather than all eight logically possible ones.

1.3.7 Higher-dimensional systems and state up-date rule in measurement

Having obtained $d = 3$ for a two-dimensional system we have derived quantum theory of this system. We have also reconstructed quantum mechanics of a composite system consisting of two qubits. Further reconstruction of quantum mechanics can be proceeded as in Hardy's work [96]. In particular, the reconstruction of higher-dimensional systems from the two-dimensional ones and the general transformations of the state after measurement are explicitly given there. We only briefly comment on them here.

In order to derive the state space, measurements and transformations for a higher-dimensional system, we can use quantum theory of a two-dimensional system in conjunction with axiom 1. The axiom requires that upon any two linearly independent states one can construct a two-dimensional subspace that is isomorphic to the state space of a qubit (2-sphere). The state space of a higher dimensional system can be

characterized such that if the state is restricted to any given two dimensional subspace, then it behaves like a qubit. The fact that all other (higher-dimensional) systems can be built out of two-dimensional ones suggests that the latter can be considered as fundamental constituents of the world and gives a justification for the usage of the term "elementary system" in the formulations of the axioms.

When a measurement is performed and an outcome is obtain, our knowledge about the state of the system changes and its representation in form of the probabilities must be updated to be in agreement with the new knowledge acquired in the measurement. This is the most natural update rule present in any probability theory. Only if one views this change as a real physical process conceptual problems arise related to discontinuous and abrupt "collapse of the wave function". There is no basis for any such assumption. Associated with each outcome is the measurement vector p. When the outcome is observed the state after the measurement is updated to p and the measurement will be a certain transformation on the initial state. Update rules for more general measurements can accordingly be given.

1.3.8 What the present reconstruction tells us about quantum mechanics?

It is often said that reconstructions of quantum theory within an operational approach are devoid of ontological commitments, and that nothing can be generally said about the ontological content that arises from the first principles or about the status of the notion of realism. As a supporting argument one usually notes that within a realistic world view one would anyway expect quantum theory at the operational level to be deducible from some underlying theory of "deeper reality". After all, we have the Broglie-Bohm theory [25, 26] which is a nonlocal realistic theory in full agreement with the predictions of (non-relativistic) quantum theory. Having said this, we cannot but emphasize that realism does stay "orthogonal" to the basic idea behind our reconstruction.

Be it local or nonlocal, realism asserts that outcomes correspond to actualities objectively existing prior to and independent of measurements. On the other hand, we have shown that the finiteness of information carrying capacity of quantum systems is an important ingredient in deriving quantum theory. This capacity is not enough to allow assignment of definite values to outcomes of all possible measurements. The elementary system has the information carrying capacity of one bit. This is signified by the possibility to decompose any state of an elementary system (qubit) in quantum

mechanics in two orthogonal states. In a realistic theory based on hidden variables and an "epistemic constraint" on an observer's knowledge of the variables' values one can reproduce this feature at the level of the entire distribution of the hidden variables [7]. That this is possible is not surprising if one bears in mind that hidden-variable theories were at the first place introduced to *reproduce* quantum mechanics and yet give a more complete description [8]. But any realism of that kind at the same time assumes an *infinite information capacity* at the level of hidden variables. Even to reproduce measurements on a single qubit requires infinitely many orthogonal hidden-variable states [97, 138, 49]. It might be a matter of taste whether or not one is ready to work with this "ontological access baggage" [97] not doing any explanatory work at the operational level. But it is certainly conceptually distinctly different from the theory analyzed here, in which the information capacity of the most elementary systems – those which are by definition not reducible further – is fundamentally limited.

To further clarify our position consider the Mach-Zehnder interferometer in which both the path information and interference observable are dichotomic, i.e. two-valued observables. It is meaningless to speak about "the path the particle took in the interferometer in the interference experiment" because this would already require to assign 2 bits of information to the system, which would exceed its information capacity of 1 bit [38]. The information capacity of the system is simply not enough to provide definite outcomes to all possible measurements. Then, by necessity the outcome in some experiments must contain an element of randomness and there must be observables that are complementarity to each other. Entanglement and consequently the violation of Bell's inequality (and thus of local realism) arise from the possibility to define an abstract elementary system carrying at most one bit such that correlations ("00" and "11" in a joint measurement of two subsystems) are basis states.

Summary.– Quantum theory is our most accurate description of nature and is fundamental to our understanding of, for example, the stability of matter, the periodic table of chemical elements, and the energy of the sun. It has led to the development of great inventions like the electronic transistor, the laser, or quantum cryptography. Given the enormous success of quantum theory, can we consider it as our final and ultimate theory? Quantum theory has caused much controversy in interpreting what its philosophical and epistemological implications are. At the heart of this controversy lies the fact that the theory makes only probabilistic predictions. In recent years it was

[7] See Ref [175] for a local version of such hidden-variable theory in which quantum mechanical predictions are partially reproduced.

[8] That this cannot be done without allowing nonlocal influences from space-like distant regions is a valid point for itself, which we do not want to follow here further.

however shown that some features of quantum theory that one might have expected to be uniquely quantum, turned out to be highly generic for generalized probabilistic theories. Is there any reason why the universe should obey the laws of quantum theory, as opposed to any other possible probabilistic theory?

In this work we have shown that classical probability theory and quantum theory – the only two probability theories for which we have empirical evidences — are special in a way that they fulfill three reasonable axioms on the systems' information carrying capacity, on the notion of locality and on the reversibility of transformations. The two theories can be separated if one restricts the transformations between the pure states to be continuous [96]. An interesting finding is that quantum theory is the *only* non-classical probability theory that can exhibit entanglement without conflicting one or more axioms. Therefore – to use Schrödinger's words [164, 165] – entanglement is not only "*the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought", but also the one that enforces the departure from a broad class of more general probabilistic theories.

Appendix

In this appendix we give the proofs of the lemmas from the main text.

Lemma 1. *The lower bound* $||T|| = 1$ *is saturated, if and only if the state is a product state* $T = \mathbf{x}\mathbf{y}^{\mathrm{T}}$.

Proof. If the state is a product state then $||T||^2 = ||\mathbf{x}||^2||\mathbf{y}||^2 = 1$. On the other hand, assume that the state $\psi = (\mathbf{x}, \mathbf{y}, T)$ satisfies $||T|| = 1$. Normalization (1.43) gives $||\mathbf{x}|| = ||\mathbf{y}|| = 1$. Let $\phi_p = (-\mathbf{x}, -\mathbf{y}, T_0 = \mathbf{x}\mathbf{y}^{\mathrm{T}})$ be a product state. We have $P(\psi, \phi_p) \geq 0$ and therefore

$$1 - ||\mathbf{x}||^2 - ||\mathbf{y}||^2 + \mathrm{Tr}(T^{\mathrm{T}}T_0) = -1 + \mathrm{Tr}(T^{\mathrm{T}}T_0) \geq 0. \tag{1.95}$$

The last inequality $\mathrm{Tr}(T^{\mathrm{T}}T_0) \geq 1$ can be seen as $(T, T_0) \geq 1$ where $(,)$ is the scalar product in Hilbert-Schmidt space. Since the vectors T, T_0 are normalized, $||T|| = ||T_0|| = 1$, the scalar product between them is always $(T, T_0) \leq 1$. Therefore, we have $(T, T_0) = 1$ which is equivalent to $T = T_0 = \mathbf{x}\mathbf{y}^{\mathrm{T}}$.

QED

Lemma 2. *The only product states belonging to* S_{12} *are* ψ_1 *and* ψ_2.

Proof. Let $\psi_p = (\mathbf{x}, \mathbf{y}, \mathbf{x}\mathbf{y}^{\mathrm{T}}) \in S_{12}$. We have

$$\begin{aligned} 1 &= P_{12}(\psi_p, \psi_1) + P_{12}(\psi_p, \psi_2) && (1.96)\\ &= \frac{1}{4}(1 + \mathbf{x}\mathbf{e}_1 + \mathbf{y}\mathbf{e}_1 + (\mathbf{x}\mathbf{e}_1)(\mathbf{y}\mathbf{e}_1)) && (1.97)\\ &+ \frac{1}{4}(1 - \mathbf{x}\mathbf{e}_1 - \mathbf{y}\mathbf{e}_1 + (\mathbf{x}\mathbf{e}_1)(\mathbf{y}\mathbf{e}_1)) && (1.98)\\ &= \frac{1}{2}(1 + (\mathbf{x}\mathbf{e}_1)(\mathbf{y}\mathbf{e}_1)) && (1.99)\\ &\Rightarrow \mathbf{x}\mathbf{e}_1 = \mathbf{y}\mathbf{e}_1 = 1 \ \vee \ \mathbf{x}\mathbf{e}_1 = \mathbf{y}\mathbf{e}_1 = -1 && (1.100)\\ &\Leftrightarrow \mathbf{x} = \mathbf{y} = \mathbf{e}_1 \ \vee \ \mathbf{x} = \mathbf{y} = -\mathbf{e}_1. && (1.101) \end{aligned}$$

QED

Lemma 3. *If the state $\psi \in S_{12}$, then $\psi' = (R, \mathbb{1})\psi \in S_{34}$ and $\psi'' = (\mathbb{1}, R)\psi \in S_{34}$.*

Proof. If $\psi \in S_{12}$ we have

$$\begin{aligned} 1 &= P_{12}(\psi, \psi_1) + P_{12}(\psi, \psi_2) && (1.102)\\ &= P_{12}((R, \mathbb{1})\psi, (R, \mathbb{1})\psi_1) + P_{12}((R, \mathbb{1})\psi, (R, \mathbb{1})\psi_2) && (1.103)\\ &= P_{12}(\psi', \psi_3) + P_{12}(\psi', \psi_4). && (1.104) \end{aligned}$$

Similarly, one can show that $(\mathbb{1}, R)\psi \in S_{34}$.

QED

Lemma 4. *Let U be some operator with the following action in the Hilbert-Schmidt space; $U(\rho) = U\rho U^{\dagger}$, and PT_1 and PT_2 are partial transpositions with respect to subsystems 1 and 2, respectively. The following identity holds:* $\mathrm{PT}_1 U \mathrm{PT}_1 = \mathrm{PT}_2 U^* \mathrm{PT}_2$, *where U^* is the complex-conjugate operator.*

Proof. We can expand U into some product basis in the Hilbert-Schmidt space $U = \sum_{ij} u_{ij} A_i \otimes B_j$. We have

$$\begin{aligned} \mathrm{PT}_1 U \mathrm{PT}_1(\rho_1 \otimes \rho_2) &= \mathrm{PT}_1\{U\rho_1^{\mathrm{T}} \otimes \rho_2 U^{\dagger}\} && (1.105)\\ &= \sum_{ijkl} u_{ij} u_{kl}^* (A_k^* \rho_1 A_i^{\mathrm{T}}) \otimes (B_j \rho_2 B_l^{\dagger})\\ &= \mathrm{PT}_2\{\sum_{ijkl} u_{ij} u_{kl}^* (A_k^* \rho_1 A_i^{\mathrm{T}}) \otimes (B_l^* \rho_2^{\mathrm{T}} B_j^{\mathrm{T}})\}\\ &= \mathrm{PT}_2\{\sum_{ijkl} u_{kl}^* u_{ij} (A_k^* \otimes B_l^*)(\rho_1 \otimes \rho_2^{\mathrm{T}})(A_i^T \otimes B_j^T)\}\\ &= \mathrm{PT}_2 U^* \mathrm{PT}_2(\rho_1 \otimes \rho_2), \end{aligned}$$

for arbitrary operators ρ_1 and ρ_2.

QED

Chapter 2

Quantum statistics, correlations and simulations

In this chapter three topics are analyzed: classical description of quantum statistics, quantum correlations captured by quantum discord and quantum simulations. It is organized as follows:

In the first section the question of "cost" for a classical (hidden-variable) description of quantum statistics is investigated. It is known that any attempt to give classical description for quantum phenomena necessarily leads to "quantum paradoxes" [19, 116, 88]. The classical states (hidden-variables) that provide a hidden determinism behind quantum probabilities have to be non-local in order to violate Bell's inequality [19]. In general, non-locality can be seen as a special case of contextually [116], i.e. velues determined by hidden variables depend on the measurement context. Apart from this counterintuitive features (from classical perspective), one can ask how "economical" (in terms of resources) determinism can be? In other words, given a measurement data table of a certain size, what is the minimal number of hidden-variables (HVs) needed to reproduce such a table, regardless of whether they are contextual or not. This is called an "ontological baggage" [97]. It has been shown that already a plausible description of one qubit requires infinite amount of classical bits [97]. But how exactly, does the amount of HVs scale with the number of measurements? This question is particularly important because in practice one can never perform a full sampling of all measurement settings, because of finite measurement accuracy. The total number of HVs scales exponentially with the number of measurements, but not all of them are necessarily needed. This is called an "ontological compression" [160]. For example, Spekkens toy model [175] that reproduces the statistics for three complementary states and measurements for a qubit requires only four out of eight HVs. By

exploring the combinatorial properties of convex sets a nice geometrical picture for ontological compression is found. It is shown that in fact, one can always find a model that requires a polynomial number of HVs only. In the limit of a continuous number of measurement settings the model converges to the model where each quantum state represents hidden-variable itself. This confirms that quantum mechanics is indeed the most economical description of itself [137].

The second section is devoted to the quantum simulation of spin models. Solving a many-body Schrödinger equation is known to be a very hard task on a classical computer. On the other hand a universal quantum computer is capable of completing the task [125]. Quantum simulator is a controllable quantum system that can be used to simulate another quantum system of interest. The idea goes back to Feynman [70, 69] who has shown an exponential advantage of quantum simulators over classical computers. Recent technological development increased the motivation to use a quantum simulator as a powerful tool to address the most important and difficult problems in many-body physics and quantum chemistry. There are two basic types of quantum simulator: analog (based on adiabatic evolution) and digital (based on discrete gate operations) [42]. In the present work the photonic quantum simulator is investigated that combines in a way both types, by utilizing a tunable quantum gates without the necessity of either discretizing the quantum evolution or engineering the physical interactions for an adiabatic quantum simulation. The photonic simulator is used to prepare the ground state of a frustrated spin-$1/2$ tetramer and simulate an adiabatic evolution via tunable quantum gate. Furthermore an exotic states such as spin liquid state [4] appears to be the ground states of a tetramer for a certain value of the system's parameters that can be well controlled in the experiment.

The topic of the third section is quantum discord [141, 101]. Quantum discord (QD) has been proposed as a measure of "non-classicality" of quantum correlations. While entanglement is known to be the sufficient resource for quantum-information processing, it is not clear to what extend separable states are useful for quantum information processing. Unlike quantum entanglement, QD exists also in separable states. Among others it has been proposed as a key resource for deterministic quantum computation with one qubit (DQC1) [54]. In the work the necessary and sufficient condition for non-zero quantum discord was found. An experimentally friendly and easy implementable criterion is found that enables an experimentalist to check the presence of QD straight from the (tomographic) measurement results. In the past the evaluation of QD required a complicated minimization procedures and analytic expressions were known only for specific classes of states. In the work a geometric measure of QD is

defined that can be evaluated directly from the measurement results without the need of a density matrix reconstruction and minimization procedures. At the end of the section the resources in DQC1 model are analyzed. It has been found that QD is very unlike to be the reason for the DQC1 speedup.

2.1 How much does it cost to simulate quantum statistics?

We prove that the results of a finite set of general quantum measurements on an arbitrary dimensional quantum system can be simulated using a polynomial (in measurements) number of hidden-variable states. In the limit of infinitely many measurements, our method gives models with the minimal number of hidden-variable states, which scales linearly with the number of measurements. These results can find applications in foundations of quantum theory, complexity studies and classical simulations of quantum systems.

In classical physics, the position and momentum of a particle determine the outcomes of all possible measurements that can be performed upon it. They define a deterministic classical state. If the state is not fully accessible, a general probabilistic classical state is a mixture of the deterministic states, arising from the inaccessibility. Since quantum mechanics gives only probabilistic predictions, it was puzzling already to the fathers of the theory whether it can be completed with an underlying classical-like model [64]. The quantum probabilities would then arise from an inaccessibility of some *hidden variables* (HV) describing analogs of deterministic classical states, the hidden-variable states, which determine the results of all quantum measurements.

Since the seminal work of Kochen and Specker (KS), it has been known that HV models must be *contextual* [116]. On the operational level, the contextual HV models cannot be distinguished from quantum mechanics. However, one may ask how plausible these models are in terms of resources, e.g., how many HV states (also called the "*ontic states*" [174, 160, 175]) they require. In addition to the fundamental question of the minimal HV model for a quantum system, this research is motivated by problems in quantum information theory. In particular, HV models allow a fair comparison between complexities of quantum and classical algorithms [1, 98], as a quantum algorithm can now be represented by a classical circuit.

For an infinite number of measurement settings, already a *single* qubit requires *infinitely* many HV states, the result proved by Hardy [97] and, in a different context, by Montina [137, 138]. However, these authors did not consider the scaling of the number of HV states with the number of measurements. Harrigan and Rudolph found a deterministic HV model that requires exponentially many HV states to simulate results of the finite set of measurements on *all* quantum states [99]. Our construction also provides such models and consumes at most a *polynomial* number of HV states, bringing exponential improvement. In the limit of infinitely many measurements, the

number of HV states for an indeterministic model scales *linearly* with the number of measurements. Moreover, the number of real parameters that specify these HV states saturates the lower bound derived by Montina [138] and, consequently, is the minimal number possible. Our method also allows a universal generalization of the Spekkens model [175].

2.1.1 General Setting

Consider a finite number, N, of projective measurements on a d-level quantum system in a state ρ. The probability to observe the rth result in the nth measurement is $p_r^{(n)}(\hat{\rho}) = \mathrm{Tr}[\hat{\rho}\hat{\Pi}_r^{(n)}]$, where $\hat{\Pi}_r^{(n)}$ is a projector on the rth orthogonal state of the nth measurement, i.e., $r = 1, ..., d$ and $n = 1, ..., N$. We form a d-dimensional vector, $\mathbf{p}^{(n)} = (p_1^{(n)}, \ldots, p_d^{(n)})^T$, composed of the probabilities for distinct outcomes in the nth measurement. For the set of measurements, we build a dN-dimensional *preparation vector*, $\mathbf{p} = (\mathbf{p}^{(1)}, ..., \mathbf{p}^{(N)})^T$ [96]. The deterministic HV states predetermine the results of *all* measurements and can be represented as a dN-dimensional vector

$$\mathbf{O}_{r_1 \ldots r_N} = (0, \ldots, 1, \ldots, 0| \ldots |0, \ldots, 1, \ldots, 0)^T, \tag{2.1}$$

where r_n is the position of 1 in the nth sequence ($r_n = 0, \ldots, d-1$ indicates that outcome r_n occurs in the nth measurement). The space of all HV states, Λ, is formed by classical mixtures of d^N deterministic states $\mathbf{O}_{r_1 \ldots r_N}$.

A set of κ quantum states $\rho_1, \ldots, \rho_\kappa$ has a HV model for N measurements, if one can find L vectors $\mathbf{O}_1, \ldots, \mathbf{O}_L \in \Lambda$ such that

$$\mathbf{p}(\rho_k) = \sum_{l=1}^{L} \alpha_l(k)\mathbf{O}_l, \qquad \text{for all } k = 1, ..., \kappa \tag{2.2}$$

where $\alpha_l(k) \geq 0$ and $\sum_l \alpha_l(k) = 1$. The model is called *deterministic* if all $\mathbf{O}_l$ are deterministic HV states; otherwise, it is called *indeterministic*. The model is *preparation-universal*, if the HV states simulate any physical state ρ, and it is *measurement-universal* if they simulate any measurement.

Formally, the set Λ is a convex polytope in $\mathbb{R}^{dN}$ having the states $\mathbf{O}_l$ as vertices. Since all probabilities satisfy $0 \leq p_r^{(n)} \leq 1$, any preparation vector $\mathbf{p}(\rho)$ lies inside this polytope and has a HV model. We study the number of HV states required for the model.

2.1.2 Two-level system

We begin with a specific deterministic HV model for a two-level quantum system (qubit) which we shall often refer to later on. An arbitrary state of a qubit can be represented as $\hat{\rho} = \frac{1}{2}(\mathbb{1} + \sum_{i=1}^{3} x_i \hat{\sigma}_i)$, where $\hat{\sigma}_i$'s are the Pauli matrices and $\mathbf{x} = (x_1, x_2, x_3)^T$ is a Bloch vector, in a unit ball $|\mathbf{x}| \leq 1$. A set of N projective measurements, with $2N$ outcomes (states on which the qubit is projected), is described by $2N$ unit vectors $\pm\mathbf{m}_1, \ldots, \pm\mathbf{m}_N$ on the Bloch sphere. The preparation vector for these directions is $\mathbf{p}(\mathbf{x}) = (\frac{1\pm\mathbf{m}_1\mathbf{x}}{2}, \ldots, \frac{1\pm\mathbf{m}_N\mathbf{x}}{2})$. Since the probability for the measurement $-\mathbf{m}$ is fully determined by the one for the $+\mathbf{m}$, one can reduce ("compress") preparation vector to $\mathbf{p}(\mathbf{x}) = (\frac{1+\mathbf{m}_1\mathbf{x}}{2}, \ldots, \frac{1+\mathbf{m}_N\mathbf{x}}{2})$. Similarly, the deterministic HV states are reduced to N-dimensional vectors $\mathbf{O}_{r_1 \ldots r_N} = (r_1, \ldots, r_N)^T$, where $r_n = 0, 1$. The (reduced) space Λ is a hypercube in N dimensions, with 2^N vertices defined by these states. By Carathéodory's theorem [1] for each vector $\mathbf{p}(\mathbf{x}) = (p_1, \ldots, p_N)^T$, one can identify $N + 1$ HV states the convex hull of which contains $\mathbf{p}(\mathbf{x})$. For a given $\mathbf{x}$, the vector $\mathbf{p}(\mathbf{x})$ can be written as a permutation of a reordered preparation vector $\mathbf{p}^{\downarrow}(\mathbf{x})$ wherein the probabilities appear in increasing order, $p_1^{\downarrow} \leq p_2^{\downarrow} \leq \cdots \leq p_N^{\downarrow}$, and the latter can be expressed in terms of $N + 1$ HV states as

$$\mathbf{p}^{\downarrow}(\mathbf{x}) = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{N-1} \\ \alpha_N \end{pmatrix}, \tag{2.3}$$

where the columns of the displayed matrix are the HV states. The expansion coefficients are

$$\begin{aligned} \alpha_0 &= 1 - p_N^{\downarrow}, \qquad \alpha_1 = p_1^{\downarrow}, \\ \alpha_n &= p_n^{\downarrow} - p_{n-1}^{\downarrow} \quad \text{for} \quad n = 2, ..., N, \end{aligned} \tag{2.4}$$

and, due to the ordering of probabilities, the coefficients are all positive and sum up to 1. One can suitably permute the rows in matrix given by (2.3) to bring the probabilities in order given by $\mathbf{p}(\mathbf{x})$. Thus, $\mathbf{p}(\mathbf{x})$ can be written as a convex combination of $N + 1$ columns (HV states) of a reordered matrix. The number of $N + 1$ states can be further reduced. E.g., for two equal probabilities, $p_1 = p_2$, the number of HV states

[1] The Carathéodory's theorem states that a point, x, in a convex polytope in $\mathbb{R}^n$ can be written as a convex combination of $n + 1$ vertices.

is decreased because $\alpha_2 = 0$. If, say, $p_2 = 1 - p_1$, one can exchange $\mathbf{m}_1 \to -\mathbf{m}_1$, such that the probabilities become equal, leading to another reduction. Importantly, different quantum states are generally modeled by *different* sets of $N + 1$ HV states.

As an illustrative example, consider a model for three complementary measurements along $\mathbf{m}_x, \mathbf{m}_y, \mathbf{m}_z$. We show a nonuniversal model, only for the eigenstates of these measurements: $\pm\mathbf{m}_x, \pm\mathbf{m}_y, \pm\mathbf{m}_z$. The corresponding preparation vectors are: $\mathbf{p}_x^{(+)} = (1, \frac{1}{2}, \frac{1}{2})$, $\mathbf{p}_x^{(-)} = (0, \frac{1}{2}, \frac{1}{2})$, $\mathbf{p}_y^{(+)} = (\frac{1}{2}, 1, \frac{1}{2})$, $\mathbf{p}_y^{(-)} = (\frac{1}{2}, 0, \frac{1}{2})$, and $\mathbf{p}_z^{(+)} = (\frac{1}{2}, \frac{1}{2}, 1)$, $\mathbf{p}_z^{(-)} = (\frac{1}{2}, \frac{1}{2}, 0)$. Applying the method of (2.3) to each of these preparation vectors, one finds that $L = 4$ HV states are sufficient for the simulation: $\mathbf{O}_0 = (1, 1, 1)^T$, $\mathbf{O}_1 = (1, 0, 0)^T$, $\mathbf{O}_2 = (0, 1, 0)^T$, and $\mathbf{O}_3 = (0, 0, 1)^T$. These four states, together with their decomposition of the preparation vectors,

$$\begin{aligned}
\mathbf{p}_x^{(+)} &= \frac{1}{2}\mathbf{O}_0 + \frac{1}{2}\mathbf{O}_1, \quad \mathbf{p}_x^{(-)} = \frac{1}{2}\mathbf{O}_2 + \frac{1}{2}\mathbf{O}_3, \\
\mathbf{p}_y^{(+)} &= \frac{1}{2}\mathbf{O}_0 + \frac{1}{2}\mathbf{O}_2, \quad \mathbf{p}_y^{(-)} = \frac{1}{2}\mathbf{O}_1 + \frac{1}{2}\mathbf{O}_3, \\
\mathbf{p}_z^{(+)} &= \frac{1}{2}\mathbf{O}_0 + \frac{1}{2}\mathbf{O}_3, \quad \mathbf{p}_z^{(-)} = \frac{1}{2}\mathbf{O}_1 + \frac{1}{2}\mathbf{O}_2.
\end{aligned} \tag{2.5}$$

are equivalent to the toy model of Spekkens [175].

We give a constructive proof that a *preparation-universal* simulation of N quantum measurements on a qubit can be achieved with the number of HV states that is polynomial in N. Let $\mathcal{M}$ denote a polytope formed as a convex hull of the measurement settings, $\mathcal{M} = \text{conv}\{\pm\mathbf{m}_1, \ldots, \pm\mathbf{m}_N\}$. Its *dual polytope* is a set [2],

$$\mathcal{D}_\mathcal{M} = \{\mathbf{y} \in \mathbb{R}^3 | -1 \leq \mathbf{m}_n\mathbf{y} \leq 1, n = 1 \ldots N\}. \tag{2.6}$$

The polytope $\mathcal{M}$ lies inside the Bloch sphere and its dual contains the sphere. Therefore, every Bloch vector can be written as a convex combination of the vertices, $\mathbf{y}_l$, of the dual polytope, $\mathbf{x} = \sum_l \alpha_l(\mathbf{x})\mathbf{y}_l$. The components of the measurement vector can now be decomposed as $p_n(\mathbf{x}) = \sum_l \alpha_l(\mathbf{x})\frac{1}{2}(1 + \mathbf{m}_n\mathbf{y}_l)$. According to the definition of the dual polytope, the quantity $\frac{1}{2}(1 + \mathbf{m}_n\mathbf{y}_l) \in [0, 1]$ and can be interpreted as the nth component (probability) of the lth HV state. Since the Bloch vectors corresponding to projections onto orthogonal states sum up to the zero vector, the corresponding probabilities assigned by a HV state sum up to 1, as it should be. Thus, the set of HV states corresponding to vertices of the dual polytope is sufficient for a preparation-universal HV model. Note that this model can in general be indeterministic. In such a case, each indeterministic HV state can be further reduced into at most $N - 2$ deterministic HV

[2] In the special case of measurement settings within a plane, we consider the dual polygon lying in that plane.

states, according to (2.3). The reason for $N-2$, and not $N+1$, states stems from the observation that a vertex of the dual polytope saturates at least three of the inequalities defining the polytope (at least three facets have to meet at each vertex), i.e., the corresponding probability is 1 or 0, and reduces the number of required deterministic HV states. Finally, the total number of HV states required for an indeterministic model is $L \leq F$, and for a deterministic model is $L \leq (N-2)F$, where F is the number of vertices of the dual polytope or, equivalently, the number of facets of the measurement polytope. A convex polytope with $2N$ vertices (in three-dimensional space) can have $N+2 \leq F \leq 4(N-1)$ facets [134], which implies that indeterministic HV models require at most a number of HV states that is *linear* in N, and deterministic ones require *quadratic* number of HV states.

Using the dual polytope approach, we generalize Spekkens' model [175], originally formulated to explain the measurement results on the eigenstates of the three complementary directions, to the preparation-universal model. For these directions, the measurement polytope is an octahedron, see Fig. 2.1(a). The dual polytope is a cube, whose interior forms the whole space of HV states, with the vertices being the deterministic states. Another interesting example is illustrated in Fig. 2.1(b).

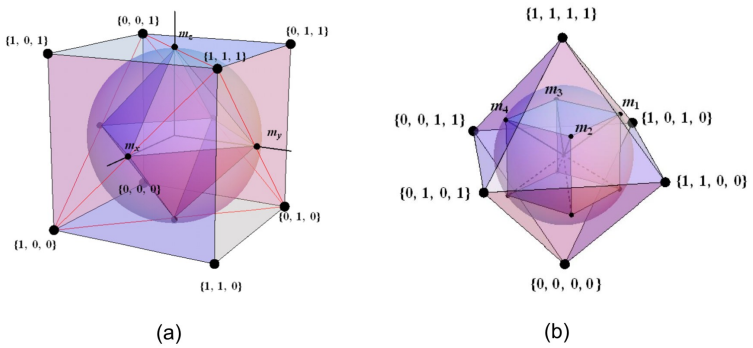

Figure 2.1: Preparation-universal HV models and dual polytopes. **(a)** The vertices of the octahedron inside the Bloch sphere define the three complementary qubit measurements. A *preparation-universal* HV model for these measurements requires eight HV states, which are written near their representative vertices of the cube containing the sphere. It generalizes the Spekkens model [175], which is not universal and utilizes only four out of eight states (see main text). Their corresponding vertices span a tetrahedron inside the cube, which does not contain the whole Bloch sphere. **(b)** Here, the measurement directions form a cube inside the sphere. Although more measurements are to be simulated, the universal HV model requires only six HV states, which are written near their representative vertices of the octahedron containing the sphere.

The dual polytope approach can be applied to arbitrary preparation vectors. However, efficient simulations are only expected for highly symmetric polytopes. For this reason, we move to more complicated Platonic solids and general symmetry considerations.

Consider a set of measurement directions $\pm\mathbf{m}_1, \ldots, \pm\mathbf{m}_N$, which is generated by a group; e.g., an octahedron and a cube can be generated via the chiral octahedral group O with 24 rotations. Generally, if G is a symmetry of the measurement polytope, $\mathcal{M}$, it is also a symmetry of its dual, $\mathcal{D}_\mathcal{M}$; i.e., the dual polytope can also be generated by G. The group action permutes the vectors $\pm\mathbf{m}_n$ as well as vertices of the dual polytope. Since the last are related to the HV states, we can define the permutation representation of the group in the HV space, $D_\mathrm{P}(G)$. The HV state, $\mathbf{h}(\mathbf{y}')$, corresponding to a vertex of a dual polytope, $\mathbf{y}' = g\mathbf{y}$, which is generated by $g \in G$ acting on an initial vertex, $\mathbf{y}$, can be found using the group representation:

$$\mathbf{h}(g\mathbf{y}) = D_\mathrm{P}(g)\mathbf{h}(\mathbf{y}). \tag{2.7}$$

Decomposing $\mathbf{h}(\mathbf{y})$ into deterministic HV states brings (2.7) to the form $\mathbf{h}(g\mathbf{y}) = \sum_{l=1} \alpha_l D_\mathrm{P}(g)\mathbf{O}_l$. Therefore, the set of deterministic HV states required for the preparation-universal model is the union of a number of group orbits $\{D_\mathrm{P}(g)\mathbf{O}_l | g \in G\}$. Because of the symmetries involved, the minimal number of HV states cannot be smaller than the number of elements in the smallest orbit.

Let us consider two other Platonic solids, the icosahedron and the dodecahedron [3]. Both of them posses the same symmetry, the chiral icosahedral group $\mathcal{I}$, with 60 rotations. Consider the icosahedron as the measurement polytope, $N = 6$. Its dual, the dodecahedron, has 20 vertices corresponding to *indeterministic* HV states that can be further reduced to deterministic HV states. The total number of possible deterministic HV states is $2^6 = 64$ in this case. We have found four different orbits of action of $\mathcal{I}$ with $12, 12, 20, 20$ different elements, respectively. Only one orbit, with 20 elements, gives deterministic states for universal simulation. For $N = 10$ measurement settings, the dodecahedron is the measurement polytope. Its dual, the icosahedron, has 12 vertices. The total number of possible deterministic HV states is $2^{10} = 1024$, which is partitioned into 24 different orbits: 2 with 12 elements, 8 with 20, and 14 with 60 elements. The two lowest orbits are suitable for the universal model. Thus, the minimal deterministic model, among all HV models obtained through the dual polytope construction, requires only 24 HV states, twice the number of vertices of the dual polytope.

[3] Similar analysis applies to cube and octahedron.

2.1.3 Arbitrary dimension

The presentation so far was limited to qubits. However, a similar line of reasoning applies to any d-level quantum system. In the general case, Pauli operators have to be replaced by generalized Gell-Mann operators, $\hat{\lambda}_i$, which naturally leads to the generalized, $D \equiv d^2 - 1$ dimensional, Bloch representation. An arbitrary quantum state, $\hat{\rho} = \frac{1}{d}[\mathbb{1} + (d-1)\sum_{i=1}^{D} x_i \hat{\lambda}_i]$, is now represented by a generalized Bloch vector, $\mathbf{x}$, with components $x_i = \mathrm{Tr}(\hat{\rho}\hat{\lambda}_i)$. We normalize the Gell-Mann operators as $\mathrm{Tr}(\hat{\lambda}_i\hat{\lambda}_j) = \frac{d}{d-1}\delta_{ij}$, such that pure quantum states are represented by normalized generalized Bloch vectors. Contrary to the qubit case, not every unit vector corresponds to a physical state. The probability of an outcome associated with a projector on a state represented by $\mathbf{m}_n$, in a measurement on a state represented by $\mathbf{x}$, is $p_n(\mathbf{x}) = \frac{1}{d}[1 + (d-1)(\mathbf{m}_n\mathbf{x})]$. The requirement of positive probabilities reveals that, e.g., the vector $\mathbf{x} = -\mathbf{m}_n$ does not represent a physical state.

In analogy to the dual polytope, for a set of dN preparaion vectors, representing N d-valued observables, we introduce a convex polytope the interior of which includes all vectors $\mathbf{y}$ leading to physically allowed probabilities $p_n(\mathbf{y}) \in [0, 1]$:

$$\mathcal{P}_{\mathcal{M}} = \{\mathbf{y} \in \mathbb{R}^D | -\tfrac{1}{d-1} \leq \mathbf{m}_n\mathbf{y} \leq 1, n = 1, ..., dN\}. \tag{2.8}$$

Among others, this polytope contains all the vectors of quantum states. The generalized Bloch vectors corresponding to a complete set of orthogonal quantum states sum up to the zero vector, implying the probabilities assigned by a HV state for different outcomes of any measurement sum up to 1, as it should be. Again, the vectors of quantum states can be expressed as a convex combination of vertices of $\mathcal{P}_{\mathcal{M}}$, and their number gives the upper bound on the amount of HV states sufficient for preparation-universal simulation. The polytope $\mathcal{P}_{\mathcal{M}}$ is specified by $q = 2dN$ linear inequalities, two inequalities for each vector $\mathbf{m}_n$, and its maximal number of vertices is given by $L \leq \binom{q-\delta}{q-D} + \binom{q-\delta'}{q-D}$, where $\delta \equiv \lfloor (D+1)/2 \rfloor$, $\delta' \equiv \lfloor (D+2)/2 \rfloor$, and $\lfloor x \rfloor$ is the integer part of x [134]. In the special case of a qubit, the dual polytope is defined by $2N$, and not $4N$, inequalities because the two bounds of Eq. (2.6) are the same for the vectors $\pm\mathbf{m}_n$. Since the binomial coefficient $\binom{a}{b}$ increases with a, $L \leq 2\binom{q-\delta}{q-D}$. Using $\binom{a}{b} = \binom{a}{a-b}$, we have $L \leq 2\binom{q-\delta}{D-\delta}$, and since $\binom{a}{b} \leq a^b/b!$, the maximal number of vertices is *polynomial* in N, $L \sim (2dN - \delta)^{D-\delta}$. The related HV states can in general be indeterministic, and each of them can be decomposed to $O(N)$ deterministic HV states, using decomposition (2.3) in the dN dimensional space Λ. Therefore, for any system, the number of (in)deterministic HV states required for a preparation-universal simulation is polynomial in N.

In the limit of infinitely many measurements, our method gives (preparation and measurement) universal models with the minimal number of HV states. As proved by Montina, in this limit the optimal model requires $2(d-1)$ real parameters to describe the HV states [138]. We show that for an infinite number of settings the set of universal HV states converges to the set of pure quantum states, which is known to be parameterized by $2(d-1)$ real numbers. First, consider a finite set of projectors $\hat{\Pi}_n$ with $n = 1, ..., dN$, and the corresponding polytope (2.8) in the Hilbert-Schmidt space of Hermitian operators with unit trace. The operators of its vertices, $\hat{y}_l$, correspond to the HV states, i.e., for all n, $\mathrm{Tr}(\hat{y}_l\hat{\Pi}_n)$ gives the probability that is assigned by the HV state, of the outcome associated with projector $\hat{\Pi}_n$. For other projectors, not within the set of dN, the trace does not have to represent a probability and therefore the set of operators $\hat{y}_l$ is larger than the set of quantum states [4]. However, in the limit of infinitely many measurements, $\mathrm{Tr}(\hat{y}_l\hat{\Pi}_n) \in [0,1]$ for all possible projectors; therefore, the eigenvalues of $\hat{y}_l$'s lie within the $[0,1]$ interval. Since $\mathrm{Tr}(\hat{y}_l) = 1$, the operators $\hat{y}_l$ are just quantum states and the HV states corresponding to pure quantum states are universal. Their number scales *linearly* with N, because N measurements correspond to dN projectors and each of them represents one HV state (and also one pure quantum state).

Regarding the polytope $\mathcal{P}_\mathcal{M}$ in the space of Hermitian operators allows for an easy generalization of our approach to POVM measurements. POVM elements, $\hat{E}_n$, are positive operators being vertices of a measurement polytope. The polytope $\mathcal{P}_\mathcal{M}$ includes all the unit-trace operators $\hat{y}$ for which $\mathrm{Tr}(\hat{y}\hat{E}_n) \in [0,1]$. Since for all quantum states $\mathrm{Tr}(\hat{\rho}\hat{E}_n) \in [0,1]$, the polytope $\mathcal{P}_\mathcal{M}$ contains all of them and, as before, its vertices define HV states.

For a d-level system the KS argument disqualifies non-contextual HV theories [116], and one might wonder how contextuality enters our models. Consider the KS argument of Peres [153]. It involves 33 different vectors in $\mathbb{R}^3$, which belong to 16 different orthogonal triads. Non-contextuality requires a value associated with a single vector to be the same irrespectively of other vectors in the triad. In the present models, the results of 16 different measurements are described by HV states with $3 \cdot 16 = 48$ components; i.e., a value assigned to the same vector can depend on the other vectors in the triad.

Summary.– In conclusion, we proved that a preparaion-universal HV model of the results of N quantum measurements requires at most a number of HV states which is polynomial in N. In the limit of infinitely many measurements, our method gives

[4] E.g., if the preparation vector of a qubit involves projectors on $|z\pm\rangle$ and $|x\pm\rangle$, it is valid to consider $\hat{y}_l = \frac{1}{2}\mathbb{1} + \hat{\sigma}_x + \hat{\sigma}_z$, which is not a quantum state.

optimal preparation- and measurement-universal HV models, with the minimal number of real parameters describing the HV states. There is no HV model that would require less HV states than the model in which every quantum state is associated with a HV state [138]. Furthermore, since there are infinitely many measurements that can be performed on a quantum system, its HV description requires infinitely many HV states. This "ontological baggage" [97] can be seen as an argument against the HV approach because it is extremely resource demanding already for a single qubit.

2.2 Quantum simulation of a frustrated Heisenberg spin system

Quantum simulators are capable of calculating properties of quantum systems unfeasible for classical computers. Here we report the analog quantum simulation of arbitrary Heisenberg-type interactions among four spin-1/2 particles. This spin-1/2 tetramer is the two-dimensional archetype system whose ground state belongs to the class of valence-bond states. Depending on the interaction strength, frustration within the system emerges such that the ground state evolves from a localized to a resonating valence-bond state. This spin-1/2 tetramer is created using the polarization states of four photons. We utilize the particular advantages of the precise single-particle addressability and a tunable measurement-induced interaction to obtain fundamental insights into entanglement dynamics among individual particles. We also directly extract ground-state energies and pair-wise quantum correlations, which enable our quantum simulator to investigate the frustration of entanglement. Remarkably, the pair-wise correlations are restricted by quantum monogamy.

During the past years, there has been an explosion of interest in quantum-enhanced technologies. The applications are many-fold and reach from quantum metrology [80] to quantum information processing [198]. In particular quantum computation has generated a lot of interest due to the discovery of quantum algorithms [58, 168, 95] which outperform classical ones. The first proposed application for which quantum computation can give an exponential enhancement over classical computation was suggested by Richard Feynman [70, 69]. He considered a universal quantum mechanical simulator, which is a controllable quantum system that can be used to imitate other quantum systems, therefore being able to tackle problems that are intractable on classical computers. Since then the motivation to use a quantum simulator as a powerful tool to address the most important and difficult problems in multidisciplinary science has led to many theoretical proposals [125, 9, 179, 42]. Vast technological developments allowed for recent realizations of such devices in atoms [89, 105, 122, 180], trapped ions [121, 72, 76, 112], NMR [171, 150, 61] and single photons [126, 144, 118]. The quantum simulation of strongly correlated quantum systems (e.g. frustrated spin systems) is of special interest and would provide new results that cannot be otherwise classically simulated [184].

In order to manipulate and measure individual properties of microscopic quantum systems the complete control over all degrees of freedom for each particle is required. Typically, atoms in optical lattices [89] are used for realizing physical systems that can

simulate various models in condensed-matter physics. The fact that the experimental addressability of single atoms in optical lattices remains very challenging [11, 10] leads to the studies of bulk properties of the atomic ensemble ($\approx 10^5$ atoms) instead of single particles. Therefore we utilize single photons in separate spatial modes and measurement-induced interactions as a quantum simulator, thus the particles are individually accessible. The tunable interaction between two entangled photon-pairs allows for the precise simulation of the ground state of a spin-1/2 tetramer. We obtain the ground-state energy and have direct access to the distribution of pair-wise quantum correlations as a function of the competing spin-spin interactions. We also observe the influence of monogamy [45, 56, 143] in this strongly correlated quantum system.

2.2.1 Analog quantum simulator

The main challenge in the understanding of strongly correlated quantum systems is to calculate the energies and ground state properties of many-body systems as this becomes exponentially difficult with increasing number of particles when using a classical computer. In contrast, quantum simulators use quantum systems to store and process data which allows them to polynomially mimic the evolution of the quantum system of interest.

Usually, the system being simulated is defined by its Hamiltonian $H(t, J, B, \dots)$ that is dependent on parameters such as time, t, interaction strength, J, external field, B, etc. One method of realizing a quantum simulator is based on discrete gate operations and the phase estimation algorithm [9, 118], referred to as a digital quantum simulator [42]. An alternative approach utilizes the adiabatic theorem [28], where an initial Hamiltonian, whose ground state is easy to prepare, can be adiabatically evolved to a final Hamiltonian with a nontrivial ground state of interest [125, 67, 23]. An adiabatic quantum simulator can be built by engineering interactions among particles using tunable external parameters (e.g. an external magnetic field). The system will remain in its ground state if the system parameters change gradually enough.

Our experimental technique combines the advantages of both approaches by utilizing a tunable quantum gate without the necessity of either discretizing the quantum evolution or engineering the physical interactions for an adiabatic quantum simulation. Thus, we consider our simulator as an analog quantum computer [89, 72, 112], where the change of the quantum evolution can be obtained by a tunable quantum gate. Figure 2.2 shows the concept of this analog simulator.

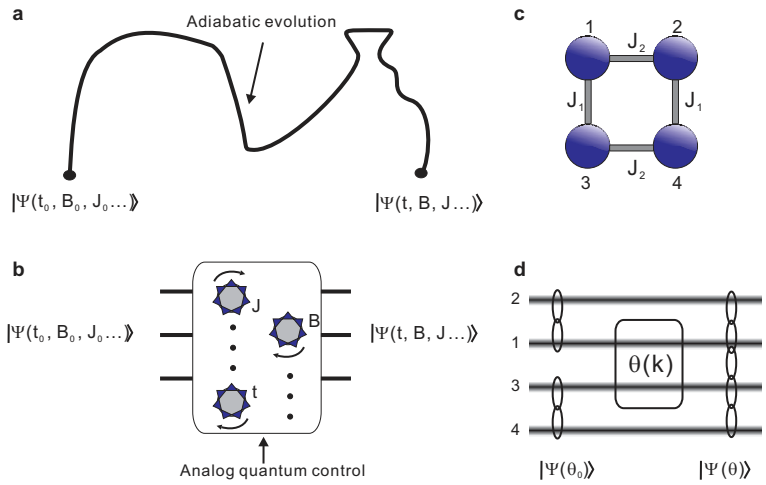

Figure 2.2: Mimicking an adiabatic quantum evolution with an analog quantum simulator. (**a**) Adiabatic quantum evolution. The system is prepared in an initial ground state $|\psi(t_0, B_0, J_0, \dots)\rangle$. Then the gradual change of the system parameters (t, B, J, etc.) causes an adiabatic evolution to the final ground state of interest $|\psi(t, B, J, \dots)\rangle$. (**b**) Analog quantum simulation. The adiabatic evolution of the system to be simulated is mapped onto a controllable evolution of a quantum system. A set of tunable gates give access to the change of parameters. (**c**) Model used to study the valence-bond states. The nearest-neighbor Heisenberg-type interactions of strength J_1 and J_2 among four spin-1/2 particles are drawn as connecting bonds and form a spin-1/2 tetramer. All the properties of the tetramer depend only upon the coupling ratio $\kappa = J_2/J_1$. (**d**) Quantum simulation of a spin-1/2 tetramer using a photonic analog quantum simulator. The initial ground state, $|\Psi(\theta_0)\rangle$, is prepared by generating the photon-pairs 1 & 2 and 3 & 4 in two singlet states. Then the analog quantum simulation is performed utilizing the measurement-induced interaction, consisting of quantum interference and the detection of a four-photon coincidence after superimposing photons 1 & 3 on a tunable beam splitter. Mapping the coupling ratio κ on the beam splitter's splitting ratio $\tan^2\theta$, leads to the ground state of interest, $|\Psi(\theta)\rangle$.

2.2.2 Simulation of a spin-1/2 tetramer

Over the last 60 years the fundamental interest in studies of ground states of Heisenberg-type Hamiltonians has led to a few exact theorems, which may serve as guidelines for quantum simulators. Based on Marshall's theorem [132] and its extension [123] the absolute ground state has total spin zero ($S^2 = 0$) for N spins on a bipartite lattice with nearest-neighbor Heisenberg-type interactions. This constraint requires the creation of valence bonds, where a pair of antiferromagnetically interacting spins forms a spin-zero singlet state. If all the spins are covered by valence bonds, which are maximally entangled states, then the ground state's total spin is zero and non-magnetic.

This is established by valence bonds that are either static and localized or fluctuating as a superposition of different partitionings of spins. In general, the equally weighted superposition of two different localized valence-bond states corresponds to a quantum spin liquid, the so-called resonating valence-bond state [4, 12].

The smallest configuration for studying and simulating these phenomena on a two-dimensional square lattice is four spin-1/2 particles forming a tetramer. In the case of such a spin-1/2 tetramer the Heisenberg-type interactions lead to the creation of three possible dimer-covering configurations for the localized valence-bond states, $|\Phi_=\rangle \equiv |\psi^-\rangle_{12}|\psi^-\rangle_{34}$, $|\Phi_\parallel\rangle \equiv |\psi^-\rangle_{13}|\psi^-\rangle_{24}$ and $|\Phi_\times\rangle \equiv |\psi^-\rangle_{14}|\psi^-\rangle_{23}$, where $|\psi^-\rangle_{ij}$ is the singlet of particle i and j (Fig. 2.2c). Since the total spin-zero subspace for this system is two-dimensional, these three dimer-covering states are not independent and $|\Phi_\times\rangle$ can be written as $|\Phi_\times\rangle = |\Phi_\parallel\rangle - |\Phi_=\rangle$ in the $|\Phi_=\rangle/|\Phi_\parallel\rangle$ basis. This state, $|\Phi_\times\rangle$, like any other equal superposition of these two dimer-covering states represents a resonating valence-bond state. Particularly interesting states are resonating valence-bond states [179, 131]with s-wave pairing symmetry, $|\Phi_\parallel\rangle + |\Phi_=\rangle$ (up to normalization), and with the exotic d-wave pairing symmetry, $|\Phi_\times\rangle = |\Phi_\parallel\rangle - |\Phi_=\rangle$. The studies of these states are of high interest, because it was conjectured that a transition from an localized valence-bond configuration to the superposition of different valence-bond states, which become mobile and superconducting upon doping, might explain high-temperature superconductivity in cuprates [8]. A quantum simulator capable of preparing such arbitrary superpositions of dimer-covering states is thus sufficient for simulating any Heisenberg-type interactions of four spin-1/2 particles on a two-dimensional lattice. It is the particular strength of our optical quantum simulator that the simulated ground states can be restricted to the spin-zero singlet subspace by utilizing the quantum interference of photons at a tunable beam splitter.

Here, we experimentally demonstrate an optical analog quantum simulator by producing two polarization entangled photon pairs (see Fig. 2.3a), $|\psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|\mathrm{HV}\rangle_{12} - |\mathrm{VH}\rangle_{12})$ and $|\psi^-\rangle_{34} = \frac{1}{\sqrt{2}}(|\mathrm{HV}\rangle_{34} - |\mathrm{VH}\rangle_{34})$, in the spatial modes 1 & 2 and 3 & 4. $|H\rangle$ and $|V\rangle$ denote horizontal and vertical polarization states, respectively. The tunable interaction among these singlet states is achieved by a tunable directional coupler (TDC), followed by a projective measurement of one photon in each of the four output modes. This tunability allows us to continuously change the measurement-induced interaction between photons 1 and 3. The TDC is an optical fiber device that transfers optical signals between fibers acting as a beam splitter with controllable splitting ratio. The control of the splitting ratio is achieved by adjusting the relative positions of the fibers (Fig. 2.3b). The transmittivity and reflectivity of this TDC go as $\cos^2\theta$

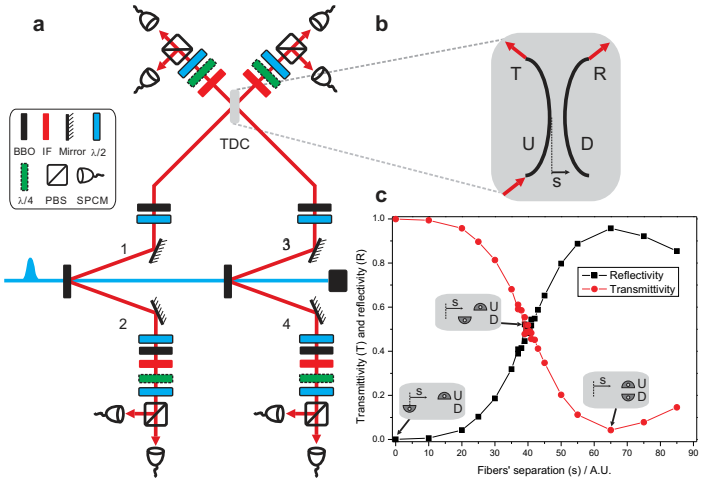

Figure 2.3: Experimental setup. (**a**) Femtosecond laser pulses ($\approx$ 140 fs, 76 MHz, 404 nm) penetrate two β-barium borate (BBO) crystals generating two pairs of photons in the spatial modes 1 & 2 and 3 & 4 (two-fold coincident count rate per pair $\approx$ 20 kHz). The walk-off effects are compensated with a half-wave plate (HWP) followed by a BBO crystal in each mode. The photon's spectral and spatial distinguishability is erased with interference filters (IF, FWHM = 3 nm) and single-mode fibers. The polarization of each photon is analyzed by a combination of a quarter-wave plate (QWP), a HWP and a polarizing beam splitter (PBS). Single photons are detected by single-photon counting modules (SPCM). (**b**) Schematic diagram of the fiber-based tunable directional coupler (TDC). The view from the top of the TDC illustrates the coupling of the evanescent light as depending on the fiber separation. The coupling between these two fibers is controlled by adjusting the horizontal position of the D fiber. (**c**) Experimental calibration of TDC's transmittivity (red circles) and reflectivity (black circles) with respect to the position of the D fiber (s) is performed by using weak laser beams and SPCM. The fibers' separations for 0%, 50% and 100% transmittivity are shown in the insets. The error bars are based on a Poissonian distribution are smaller than 0.5% of the mean values.

and $\sin^2\theta$, respectively, where θ parameterizes the fibers' separation. We calibrate the TDC's transmittivity and reflectivity such that the modulating visibilities (Michaelson visibility) are above 95% for both inputs, as required for high-precision quantum control (Fig. 2.3c).

A successful detection of a four-fold coincidence event from each spatial mode gives the four-photon state,

$$\begin{aligned} |\psi(\theta)\rangle_{1234} = \frac{1}{\sqrt{n(\theta)}}[\quad & - \quad \cos^2\theta(|\mathrm{HHVV}\rangle + |\mathrm{VVHH}\rangle) \\ & + \quad \sin^2\theta(|\mathrm{HVVH}\rangle + |\mathrm{VHHV}\rangle) \\ & + \quad \cos 2\theta(|\mathrm{HVHV}\rangle + |\mathrm{VHVH}\rangle)], \end{aligned} \tag{2.9}$$

where $n(\theta) = \frac{1}{2}(\cos^4\theta + \cos^2 2\theta + \sin^4\theta)$ is the normalization constant. The experimentally obtained density matrix, ρ_{exp}, is reconstructed from a set of 1,296 local measurements using the maximum-likelihood technique [188, 106]. For this, all combinations of mutually unbiased basis sets for individual qubits, that is $|H/V\rangle$, $|+/-\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$ and $|R/L\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm i|V\rangle)$, are measured. The duration of each measurement for a given setting of the polarization analyzers and the TDC was 200 s and the average detected four-fold coincidence rate was 3 Hz. In total eight density matrices for different settings of θ are reconstructed and are summarized in the Supplementary Information. Uncertainties in quantities extracted from these density matrices are calculated using a 10 run Monte Carlo simulation of the whole state tomography analysis, with Poissonian noise added to each experimental data point in each run.

For our quantum simulation we consider four spin-1/2 particles on a square lattice (tetramer) that interact via nearest-neighbor Heisenberg-type interactions of the strength J_1 and J_2 (Fig. 2.2c). The system is described by the Hamiltonian

$$H = J_1\vec{S}_1\vec{S}_3 + J_1\vec{S}_2\vec{S}_4 + J_2\vec{S}_1\vec{S}_2 + J_2\vec{S}_3\vec{S}_4, \tag{2.10}$$

where $\vec{S}_i$ is the Pauli spin operator for spin i. All the properties of the system depend only on the coupling ratio $\kappa = J_2/J_1$ therefore we re-normalize the Hamiltonian to

$$H(\kappa) = H_0 + \kappa H_1, \tag{2.11}$$

where $H(\kappa) = H/J_1$ is the final Hamiltonian, $H_0 = \vec{S}_1\vec{S}_3 + \vec{S}_2\vec{S}_4$ the initial Hamiltonian and $H_1 = \vec{S}_1\vec{S}_2 + \vec{S}_3\vec{S}_4$ the competing Hamiltonian of H_0. By adjusting κ, we can change $H(\kappa)$ and hence its ground state. For convenience we introduce a new parameter, θ, where $\tan^2\theta = \kappa + \sqrt{\kappa^2 - \kappa + 1}$ represents the splitting ratio of the TDC used in the experiment (see Fig. 2.3). This enables the full control of the interactions among the spins (coupling ratio κ) via adjusting the splitting ratio of the TDC. The ground state of the Hamiltonian given in Eq. (2.11) is

$$|\Psi^{(0)}(\theta)\rangle = \frac{1}{\sqrt{n(\theta)}}(\cos 2\theta|\Phi_=\rangle - \cos^2\theta|\Phi_\parallel\rangle). \tag{2.12}$$

The ground state energy of $|\Psi^{(0)}(\theta)\rangle$ is $E^{(0)} = -2(1+\kappa) - 4\sqrt{1-\kappa+\kappa^2}$. The TDC's angel, θ, takes the values from the interval of $0 \le \theta \le \frac{\pi}{2}$. Using our photonic quantum simulator, we can mimic the adiabatic change of the Hamiltonian shown in Eq. (2.11), where the full range of the coupling ratio $-\infty \le \kappa \le +\infty$ is experimentally covered by tuning the angle of the TDC between $\arctan\frac{1}{\sqrt{2}} \le \theta \le \frac{\pi}{2}$. For $\kappa = 0$ ($\theta = \frac{\pi}{4}$), the ground

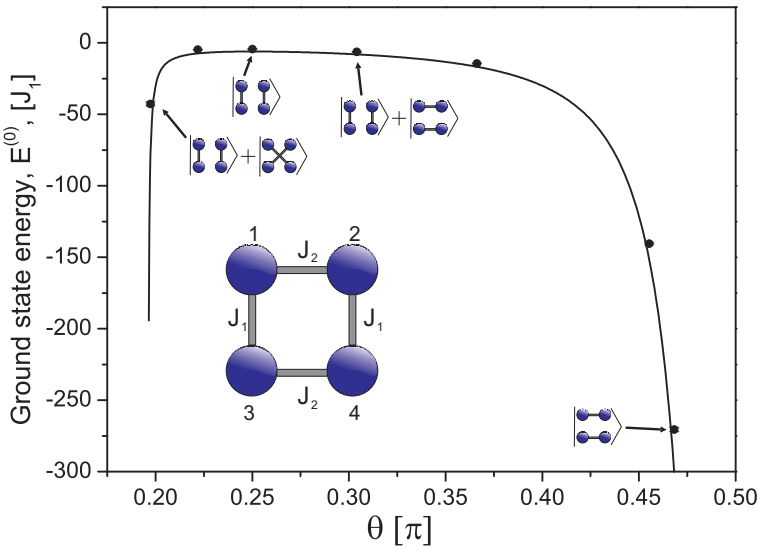

Figure 2.4: Ground state energy of the spin-1/2 tetramer. By tuning θ, where $\tan^2\theta = \kappa + \sqrt{\kappa^2 - \kappa + 1}$ represents the splitting ratio of the tunable directional coupler, we gradually change the ground state of the spin-1/2 tetramer. The full range of the coupling ratio $-\infty \leq \kappa = \frac{J_2}{J_1} \leq \infty$ is covered by tuning θ from $\arctan\frac{1}{\sqrt{2}}$ to $\frac{\pi}{2}$. We measure the ground state energy for seven different configurations. Of particular interest are the quantum states $|\Phi_{\|}\rangle + |\Phi_{\times}\rangle$, $|\Phi_{\|}\rangle$, $|\Phi_{\|}\rangle + |\Phi_{=}\rangle$ and $|\Phi_{=}\rangle$, shown explicitly. The black circles represent the experimental data and the solid line is parameter-free theoretical prediction. The error bars follow Poissonian statistics and are smaller than the data points.

state is $|\Phi_{\|}\rangle$, while for $\kappa = +\infty$ ($\theta = \frac{\pi}{2}$), the ground state changes to $|\Phi_{=}\rangle$. These two cases are dimer-covering states.

Tuning the coupling ratio to $\kappa = -\infty$ results in the equally weighted superposition $|\Phi_{\times}\rangle + |\Phi_{\|}\rangle$, whereas $\kappa = 1$ leads to the interesting resonating valence-bond state [8, 4, 12] $|\Phi_{=}\rangle + |\Phi_{\|}\rangle$. In Fig. 2.4, we present $E^{(0)}$ as a function of θ and obtain good agreement with theoretical prediction.

In Fig.2.5, we show the experimentally obtained density matrices of the four valence-bond states, $|\Phi_{=}\rangle + |\Phi_{\times}\rangle$, $|\Phi_{\|}\rangle$, $|\Phi_{=}\rangle + |\Phi_{\|}\rangle$ and $|\Phi_{=}\rangle$, which correspond to the setting of $\theta = 0.197\pi$, $\theta = 0.25\pi$, $\theta = 0.304\pi$ and $\theta = 0.468\pi$. The state fidelity is defined as $F(\Psi, \rho) = \langle\Psi|\rho|\Psi\rangle$, where $|\Psi\rangle$ is the target and ρ is experimentally obtained quantum state. Due to the high quality of our quantum simulator, we obtain four-photon state fidelities that range from $F = 0.712(4)$ to $F = 0.888(2)$ (see Supplementary Information).

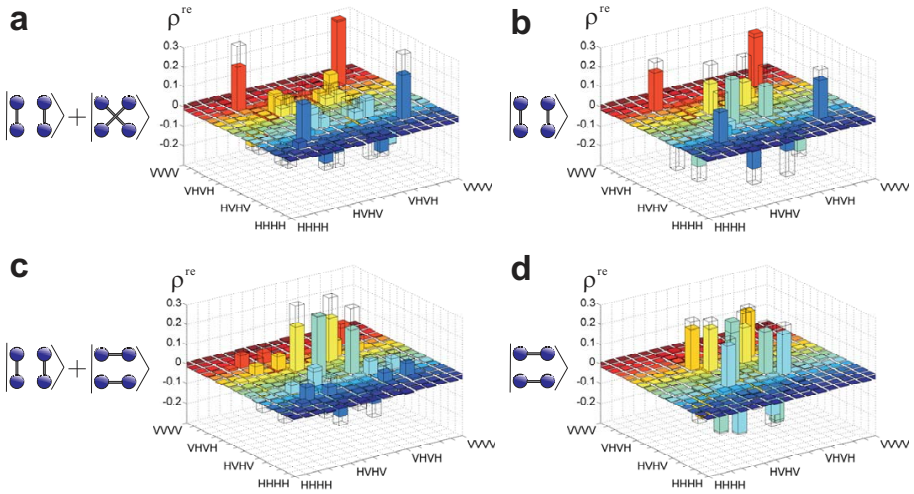

Figure 2.5: Density matrices of various spin-1/2 tetramer configurations in the computational basis ($|H\rangle/|V\rangle$). Shown are the real parts of the density matrices for the cases of (**a**) equal superposition of dimer-covering states, (**b**,**d**) dimer-covering states and (**c**) resonating valence-bond state. The imaginary parts are small and shown in the Supplementary Information. The wire grids indicate the expected values for the ideal case. The density matrices are reconstructed from the experimental four-photon tomography data for the settings of (**a**) $\theta = 0.197\pi$, (**b**) $\theta = 0.25\pi$, (**c**) $\theta = 0.304\pi$ and (**d**) $\theta = 0.468\pi$. The fidelities, F, of the measured density matrix with the ideal state are (**a**) $F = 0.745(4)$, (**b**) $F = 0.712(4)$, (**c**) $F = 0.746(6)$ and (**d**) $F = 0.888(2)$. The uncertainties in fidelities extracted from these density matrices are calculated using a Monte Carlo routine and assumed Poissonian errors.

2.2.3 Quantum monogamy and complementarity

Monogamy is one of the most fundamental properties of quantum entanglement [45, 56, 143]. It restricts the shareability of quantum correlations among parties and is of essential importance in many quantum information processing protocols, including quantum cryptography and entanglement distillation. Recent work showed that in the context of condensed-matter physics, monogamy gives rise to frustration effects in e.g., Heisenberg antiferromagnets. The ideal ground state for an antiferromagnet would consist of singlets between all interacting spins. But, due to the monogamy relation a particle can only share one unit of entanglement (singlet) with its neighbors. Therefore, it will spread entanglement in an optimal way with all its neighbors leading to a strongly correlated ground state [143].

To study the dynamics of pair-wise interactions, in which the monogamy of bipartite quantum entanglement distribution plays a crucial role, we characterize the distribution of the two-body energies and correlations between one spin with respect to the

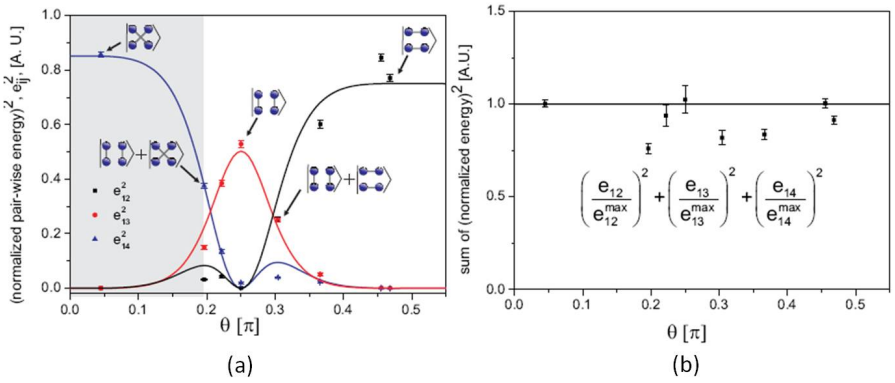

Figure 2.6: Experimentally extracted pair-wise Heisenberg energies. (**a**) Experimental observation of quantum monogamy when comparing the pair-wise normalized Heisenberg energy, e_{ij}, it acts as a two-particle entanglement witness, for the spin pairs 1 & 2 (black square), 1 & 3 (red circle) and 1 & 4 (blue triangle). The highlighted area corresponds to the full range of the coupling ratio $-\infty \leq \kappa = \frac{J_2}{J_1} \leq \infty$. For the case of $\kappa = 0$ ($\theta = \frac{\pi}{4}$), the ground state of this spin-1/2 tetramer is $|\Phi_{\|}\rangle = |\psi^-\rangle_{13}|\psi^-\rangle_{24}$ and the amount of entanglement of the pair 1 & 3 reaches its maximum while the pairs 1 & 2 and 1 & 4 are not entangled. Similarly, for the case of $\kappa = +\infty$ ($\theta = \frac{\pi}{2}$), the ground state is reduced to $|\Phi_{=}\rangle = |\psi^-\rangle_{12}|\psi^-\rangle_{34}$, where pair 1 & 2 is now maximally entangled, and pairs 1 & 3 and 1 & 4 are disentangled. In the case of the resonating valence-bond state, entanglement distributions are equal between the pairs 1 & 2 and 1 & 3 (i.e. $e_{12} = e_{13}$). In other cases, entanglement is distributed according to the monogamy relation. (**b**) Experimental demonstration of the complementarity relation in a spin-1/2 tetramer. For each valence-bond configuration we measured pair-wise Heisenberg energies, e_{ij}, which are normalized by its maximal value, $e_{ij}^{\max}$. The sum of these renormalized energy values are in good agreement with the theoretical prediction (shown as line in the plot). The uncertainties represent standard deviations deduced from propagated Poissonian statistics.

others with the normalized Heisenberg energy per unit of interaction, e_{ij}. It is defined as $e_{ij} = -\frac{1}{3}\mathrm{Tr}(\rho_{ij}\vec{S}_i\vec{S}_j)$. Note that ρ_{ij} is the density matrix of spins i and j. The normalized Heisenberg energy per unit of interaction is also an entanglement witness [35, 7] and reaches its maximum value of $e_{ij} = 1$ for the singlet state. The amount of entanglement can also be quantified by concurrence [191], which is directly related to e_{ij} with $C(e_{ij}) = \max\{0, -\frac{1}{2} + \frac{3}{2}e_{ij}\}$. For our four-spin system the dependencies of the pair-wise energies with respect to the TDC's angle θ are given by $e_{12} = -\frac{1}{n}(\sin^2\theta\cos 2\theta)$, $e_{13} = \frac{1}{n}(\sin^2\theta\cos^2\theta)$, and $e_{14} = \frac{1}{n}(\cos^2\theta\cos 2\theta)$.

Remarkably, monogamy is manifested in the constraint of the energy distribution for the considered spin pair through a complementarity relation [65, 34]

$$e_{12}^2 + e_{13}^2 + e_{14}^2 = 1. \tag{2.13}$$

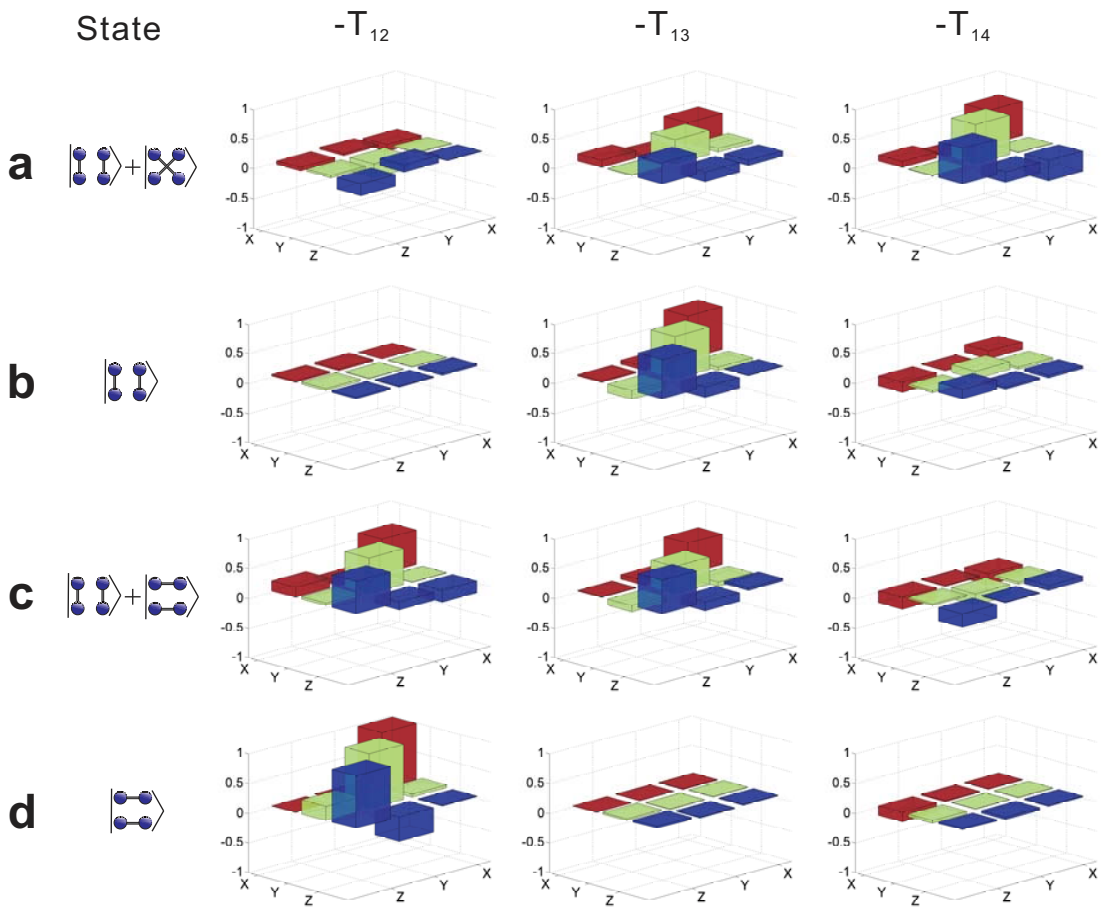

Figure 2.7: Directly observed pair-wise correlation functions of various valence-bond states. The correlation tensors T_{12} (photons 1 & 2), T_{13} (photons 1 & 3) and T_{14} (photons 1 & 4) are obtained from correlation measurements directly in the bases $X = \sigma_x$, $Y = \sigma_y$ and $Z = \sigma_z$. For a convenient graphical representation, the negative values of the correlation tensors are shown. The structure of (**a**) the superposition state and (**c**) resonating valence-bond state show that the quantum correlations are equally distributed among two competing pairs. (**b**) and (**d**) belong to dimer-covering states, in which only one pair is maximally correlated in a singlet state.

This restricts the maximal amount of energy or entanglement associated with correlated spin systems (see Fig. 2.6a). For instance, in the experiment we obtain the normalized Heisenberg energy per unit interaction between photons 1 and 2 (e_{12}) with the correlation measurements in three mutually unbiased bases ($S_1^{(w)} \otimes S_2^{(w)}$, where $w = 1, 2, 3$).

As shown in Fig. 2.6a, the adiabatic change of the coupling between the four spins is simulated by tuning the angle of the TDC, θ, from $\arctan \frac{1}{\sqrt{2}}$ to $\frac{\pi}{2}$. This corresponds to the full range of the coupling ratio $-\infty \leq \kappa = \frac{J_2}{J_1} \leq \infty$. In the ideal case, the maximum of e_{ij} is unity which corresponds to a singlet state shared by spins i and j. However,

imperfections in the generation of entangled photon pairs and the two-photon interference on the TDC reduce the measured value of e_{ij} by a constant factor, independent of θ. For the individual photon pairs we obtain the maximal Heisenberg energy of $e_{12}^{\max} = 0.920(7)$, $e_{13}^{\max} = 0.727(9)$, and $e_{14}^{\max} = 0.926(5)$. In order to demonstrate the complementarity relation [62] we re-normalized each energy e_{ij} by its maximal value $e_{ij}^{\max}$ and obtain a good agreement with the theoretical prediction shown in Fig.2.6b.

The advantage of the individual addressability for our particles in the ground state allows for the direct extraction of the pair-wise quantum correlations. The pair-wise quantum correlation is defined as:

$$T(S_i^{(w)}, S_j^{(v)}) = \frac{C(S_i^{(w)}, S_j^{(v)}) + C(S_i^{(w)\perp}, S_j^{(v)\perp}) - C(S_i^{(w)\perp}, S_j^{(v)}) - C(S_i^{(w)}, S_j^{(v)\perp})}{C(S_i^{(w)}, S_j^{(v)}) + C(S_i^{(w)\perp}, S_j^{(v)\perp}) + C(S_i^{(w)\perp}, S_j^{(v)}) + C(S_i^{(w)}, S_j^{(v)\perp})},$$

where $C(S_i^{(w)}, S_j^{(v)})$ are the corresponding coincidence counts between pair i and j in the bases of $S^{(w)}$ and $S^{(v)}$, respectively. In Fig. 2.7, the pair-wise correlation functions for the ground states, $|\Phi_=\rangle + |\Phi_\times\rangle$, $|\Phi_\parallel\rangle$, $|\Phi_=\rangle + |\Phi_\parallel\rangle$ and $|\Phi_=\rangle$, are shown. As expected from the monogamy relation, in the cases of dimer-covering states, one pair of the photons is maximally correlated, e.g. photons 1 and 3 in Fig. 2.7b, and photons 1 and 2 in Fig. 2.7c. In the cases of the equal superposition of two dimers (Fig. 2.7a) and the resonating valence-bond state (Fig. 2.7d), correlations are distributed among different pairs.

Summary.– We demonstrate the feasibility of an all-optical analog quantum simulator by enabling quantum control of the measurement-induced interaction among photonic quantum states. Various ground states, including the resonating valence-bond states for four interacting spin-1/2 particles are generated and characterized by extracting the total energy and the pair-wise quantum correlations. The simulation of a spin-1/2 tetramer also proves that the pair-wise entanglement and energy distribution are restricted by the role of quantum monogamy. Our results provide promising insights for quantum simulations of small quantum systems, where individual addressability and control over all degrees of freedom on the single-particle level is required. This is of particular interest for quantum chemistry with small numbers of particles and might allow in the near future the simulation of aromatic systems and chemical reactions [111]. Although it was shown that efficient scalable quantum computing with single photons, linear-optical elements, and projective measurements is possible [115], the most important challenges for future optical approaches will be (a) the realization of high-quality quantum control, (b) generating systems with more qubits and (c) developing efficient methods of simulating other classes of complex Hamiltonians by

using optical elements. Ideally, this and related work will open a new and promising avenue for the experimental simulation of various quantum systems.

2.2.4 Supplementary Information - Experimental photonic analog quantum simulation

Quantum state tomography

We perform quantum state tomography for the simulated ground states of a spin-1/2 tetramer. The studies of the eight different ground states lead to 10368 coincidence count measurements with a total 414724 four-fold coincidence counts. The reconstructed density matrices are plotted in Fig. 2.8 and 2.9.

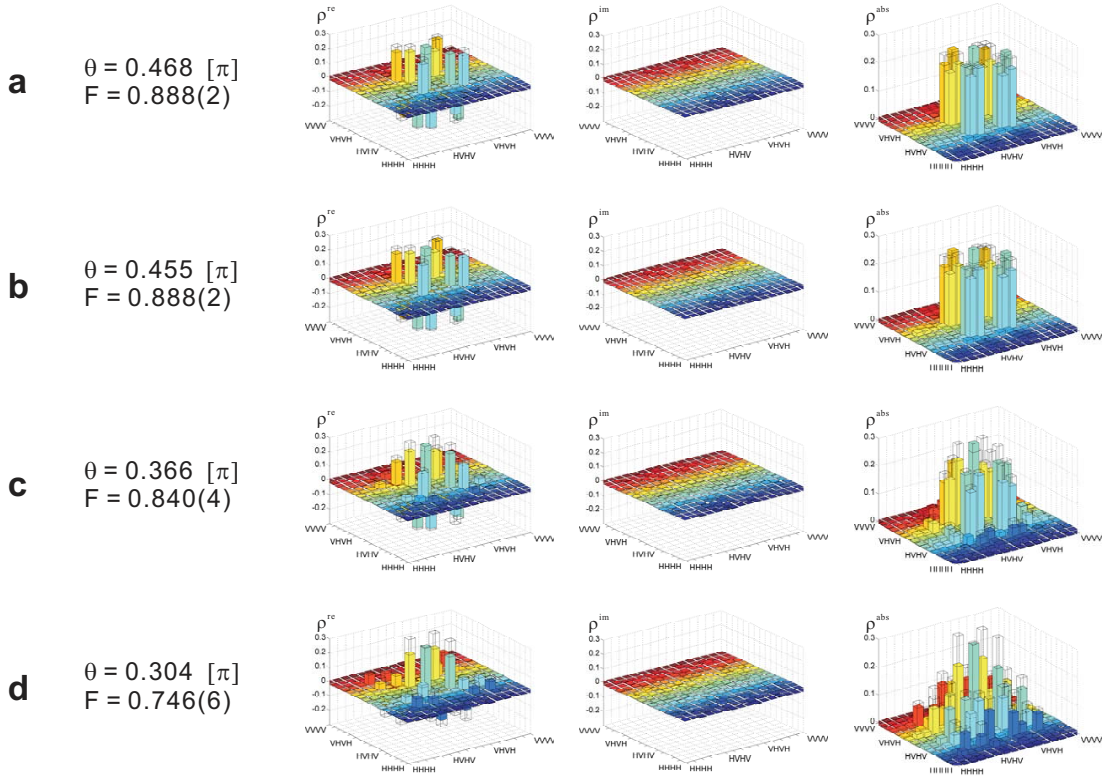

Figure 2.8: Density matrices of various spin-1/2 tetramer configurations in the computational basis ($|H\rangle/|V\rangle$). Shown are the real parts (ρ^{re}), imaginary part (ρ^{im}), and absolute values (ρ^{abs}) of the density matrices for the different settings of the splitting ratio of θ of the tunable direction coupler: (**a**), $\theta = 0.468\pi$, (**b**), $\theta = 0.455\pi$, (**c**), $\theta = 0.366\pi$ and (**d**), $\theta = 0.304\pi$. The wire grids indicate the expected values for the ideal case. The fidelities, F, of the measured density matrix with the ideal state are (**a**), F = 0.888(2), (**b**), F = 0.888(2), (**c**), F = 0.840(4) and (**d**), F = 0.746(6).

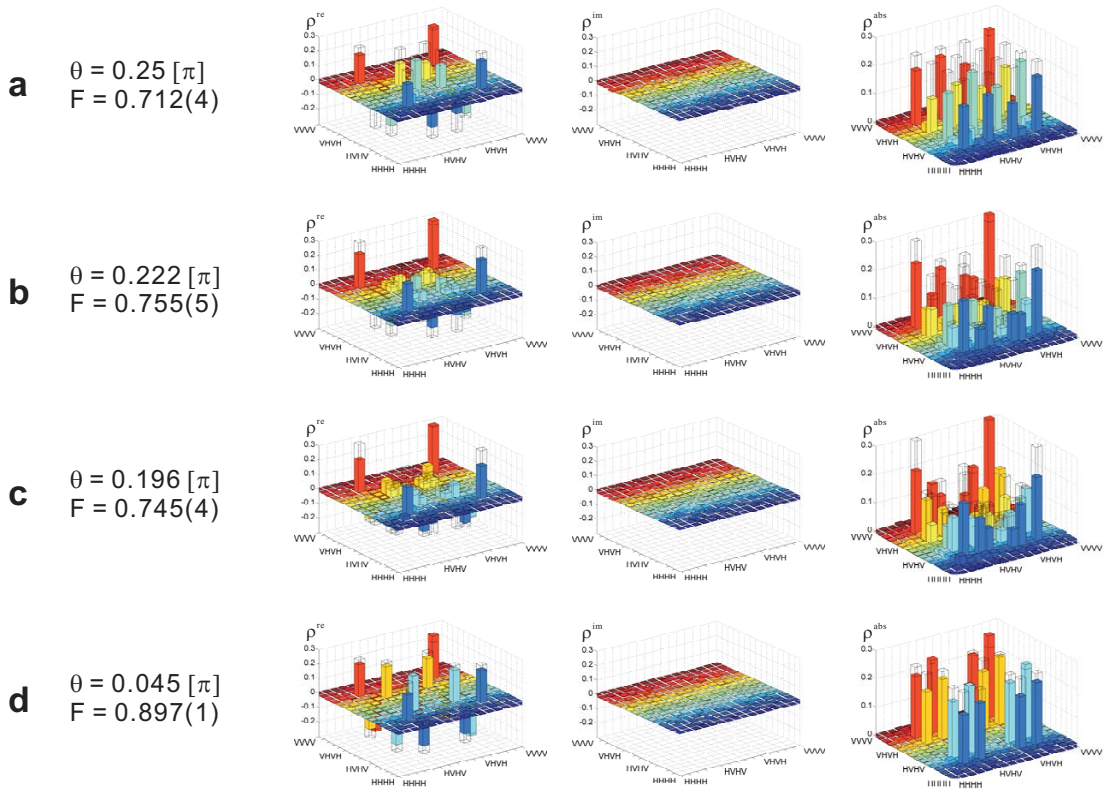

Figure 2.9: Density matrices of various spin-1/2 tetramer configurations in the computational basis ($|H\rangle/|V\rangle$). Shown are the real parts (ρ^{re}), imaginary part (ρ^{im}), and absolute values (ρ^{abs}) of the density matrices for the different settings of the splitting ratio of θ of the tunable direction coupler: (**a**), $\theta = 0.25\pi$, (**b**), $\theta = 0.222\pi$, (**c**), $\theta = 0.197\pi$ and (**d**), $\theta = 0.045\pi$. The wire grids indicate the expected values for the ideal case. The fidelity, F, of the measured density matrix with the ideal state are (**a**), F = 0.712(4), (**b**), F = 0.755(5), (**c**), F = 0.745(4) and (**d**), F = 0.897(1).

2.3 Necessary and sufficient condition for non-zero quantum discord

Quantum discord characterizes "non-classicality" of correlations in quantum mechanics. It has been proposed as the key resource present in certain quantum communication tasks and quantum computational models without containing much entanglement. We obtain a necessary and sufficient condition for the existence of non-zero quantum discord for any dimensional bipartite states. This condition is easily experimentally implementable. Based on this, we propose a geometrical way of quantifying quantum discord. For two qubits this results in a closed form of expression for discord. We apply our results to the model of deterministic quantum computation with one qubit (DQC1), showing that quantum discord is unlikely to be the reason behind its speedup.

Quantum states of a composite system can be divided into entangled and separable once. Entangled states display "nonlocal features" violating Bell's inequalities [19] and are considered a necessary resource for quantum communication and pure quantum computation allowing computational speedup over the best classical algorithm [140]. On the contrary, separable states are generally considered as purely classical, since they do not violate Bell's inequalities and can be prepared by local operations and classical communication. However, it is valid to ask if highly mixed states, and in particular separable states, are completely useless from quantum information perspective. Recent investigations give compelling evidences that this is not the case. A highly mixed state in the DQC1 model [114] is believed to perform a task exponentially faster than any classical algorithm ("without containing much entanglement"). Furthermore, it has been shown that even some separable states contain nonclassical correlations [141, 101] and can create an advantage for computing and information processing tasks over their classical counterparts [32, 135, 53, 55, 54, 117].

The "non-classicality" of bipartite correlations is measured via *quantum discord* [141]– the discrepancy between quantum versions of two classically equivalent expressions for mutual information. Recently, it has been shown that almost all quantum states have non-vanishing discord [68]. Quantum discord was proposed as a figure of merit for characterizing the nonclassical resources present in the DQC1 [54]. It has been shown that initial zero-discord system-environment state is necessary and sufficient condition for completely-positive map evolution of the system when the environment is traced out [166, 158]. Furthermore, in Ref. [156] is demonstrated that if the state can be locally broadcasted than it has vanishing discord.

Despite increasing evidences for relevance of quantum discord in describing non-

classical resources in information processing, there is no straightforward criterion to verify the presence of discord in a given quantum state. Its evaluation involves optimization procedure and analytical results are known only in a few cases [127, 59, 162, 5, 3, 79]. In this Letter we derive the necessary and sufficient condition for non-vanishing quantum discord. The criterion is simple and also experimentally friendly, since it can be evaluated directly from a (sub)set of measurements standardly used for quantum state tomography. Based on this, we introduce the geometrical measure of discord and derive an explicit expression for the case of two qubits. Finally, we give arguments putting in question appropriateness of quantum discord to describe the non-classical resource in DQC1 computational model.

2.3.1 Quantum discord

Correlations between two random variables of classical systems A and B are in information theory quantified by the mutual information $I(A:B) = H(A) + H(B) - H(A,B)$. If A and B are classical systems, than $H(.)$ stands for the Shannon entropy $H(\mathbf{p}) = -\sum_i p_i \log p_i$, where $\mathbf{p} = (p_1, p_2, \dots)$ is the probability distribution vector, while $H(.,.)$ is the Shannon entropy of the joint probability distribution p_{ij}. For quantum systems A and B, function $H(.)$ denotes the von Neumann entropy $H(\rho) = -\mathrm{Tr}\rho\log\rho$ where ρ is the density matrix. In the classical case, we can use the Bayes rule and find an equivalent expression for the mutual information $I(A:B) = H(A) - H(A|B)$ where $H(A|B)$ is the Shannon entropy of A conditioned on the measurement outcome on B. For quantum systems, this quantity is different from the first expression for the mutual information and the difference defines the quantum discord.

Consider a quantum composite system defined by the Hilbert space $\mathcal{H}_{\mathrm{AB}} = \mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$. Let dimensions of the local Hilbert spaces be $\dim\mathcal{H}_{\mathrm{A}} = d_{\mathrm{A}}$ and $\dim\mathcal{H}_{\mathrm{B}} = d_{\mathrm{B}}$, while $d = \dim\mathcal{H}_{\mathrm{AB}} = d_{\mathrm{A}}d_{\mathrm{B}}$. Given a state ρ (density matrix) of a composite system, the total amount of correlations is quantified by quantum mutual information [93]:

$$I(\rho) = H(\rho_{\mathrm{A}}) + H(\rho_{\mathrm{B}}) - H(\rho), \tag{2.14}$$

where $H(\rho)$ is the von Neumann entropy and $\rho_{\mathrm{A,B}} = \mathrm{Tr}_{\mathrm{B,A}}(\rho)$ are reduced density matrices. A generalization of the classical conditional entropy is $H(\rho_{\mathrm{B|A}})$, where $\rho_{\mathrm{B|A}}$ is the state of B given a measurement on A. By optimizing over all possible measurements in A, we define an alternative version of the mutual information

$$Q_A(\rho) = H(\rho_{\mathrm{B}}) - \min_{\{E_k\}} \sum_k p_k H(\rho_{\mathrm{B}|k}), \tag{2.15}$$

where $\rho_{\mathrm{B}|k} = \mathrm{Tr}_{\mathrm{A}}(E_k \otimes \mathbb{1}_{\mathrm{B}}\rho)/\mathrm{Tr}(E_k \otimes \mathbb{1}_{\mathrm{B}}\rho)$ is the state of B conditioned on outcome k in A and $\{E_k\}$ represents the set of positive operator valued measure elements. The discrepancy between the two measures of information defines the quantum discord [141, 101]:

$$D_A(\rho) = I(\rho) - Q_A(\rho). \tag{2.16}$$

The discord is always nonnegative [141] and reaches zero for the classically correlated states [101]. Note that discord is not a symmetric quantity $D_A(\rho) \neq D_B(\rho)$ and D_A refers to the "left" discord, while D_B refers to the "right" discord. The state ρ for which $D_A(\rho) = D_B(\rho) = 0$ is *completely* classically correlated in a sense of [142, 136] From now on, when we refer to the discord we mean the "left" discord D_A.

To give an example of a state with non-vanishing discord consider the two-qubit separable state in which four nonorthogonal states of one qubit are correlated with four nonorthogonal states of the second qubit:

$$\begin{aligned}&\frac{1}{4}(|0\rangle\langle 0| \otimes |+\rangle\langle +| + |1\rangle\langle 1| \otimes |-\rangle\langle -| + |+\rangle\langle +| \otimes |1\rangle\langle 1| \\ &+|-\rangle\langle -| \otimes |0\rangle\langle 0|).\end{aligned} \tag{2.17}$$

Unlike the state above, one can show that the state ρ is of zero-discord if and only if there exist a von Neumann measurement $\{\Pi_k = |\psi_k\rangle\langle\psi_k|\}$ such that [51]

$$\sum_k (\Pi_k \otimes \mathbb{1}_{\mathrm{B}})\rho(\Pi_k \otimes \mathbb{1}_{\mathrm{B}}) = \rho, \tag{2.18}$$

In other words the zero-discord state is of the form $\rho = \sum_k p_k|\psi_k\rangle\langle\psi_k| \otimes \rho_k$ where $\{|\psi_k\rangle\}$ is some orthonormal basis set, ρ_k are the quantum states in B and p_k are non-negative numbers such that $\sum_k p_k = 1$.

2.3.2 An easily implementable necessary and sufficient condition

Let us choose basis sets in local Hilbert-Schmidt spaces of Hermitian operators, $\{A_n\}$ and $\{B_m\}$ where $n = 1 \ldots d_{\mathrm{A}}^2$ and $m = 1 \ldots d_{\mathrm{B}}^2$. We decompose the state ρ of composite system into $\rho = \sum_{nm} r_{nm} A_n \otimes B_m$. The coefficients r_{nm} define $d_{\mathrm{A}}^2 \times d_{\mathrm{B}}^2$ real matrix R which we call the correlation matrix. We can find its singular value decomposition (SVD), $URW^{\mathrm{T}} = \mathrm{diag}[c_1, c_2, \ldots]$ where U and W are $d_{\mathrm{A}}^2 \times d_{\mathrm{A}}^2$ and $d_{\mathrm{B}}^2 \times d_{\mathrm{B}}^2$ orthogonal matrices, respectively, while $\mathrm{diag}[c_1, c_2, \ldots]$ is $d_{\mathrm{A}}^2 \times d_{\mathrm{B}}^2$ diagonal matrix. SVD defines new basis in local Hilbert-Schmidt spaces $S_n = \sum_{n'} U_{nn'} A_{n'}$ and $F_m = \sum_{m'} W_{mm'} B_{m'}$. The state ρ in the new basis is of the form $\rho = \sum_{n=1}^{L} c_n S_n \otimes F_n$ where $L = \mathrm{rank}R$ is the rank of correlation matrix R (the number of non-zero eigenvalues c_n).

The necessary and sufficient condition (2.18) becomes $\sum_{n=1}^{L} c_n(\sum_k \Pi_k S_n \Pi_k) \otimes F_n = \sum_{n=1}^{L} c_n S_n \otimes F_n$ and it is equivalent to the set of conditions:

$$\sum_k \Pi_k S_n \Pi_k = S_n, \quad n = 1 \dots L, \tag{2.19}$$

or equivalently $[S_n, \Pi_k] = 0$ for all k, n. This means that the set of operators $\{S_n\}$ have common eigenbasis defined by the set of projectors $\{\Pi_k\}$. Therefore, the set $\{\Pi_k\}$ exists if and only if:

$$[S_n, S_m] = 0, \quad n, m = 1 \dots L. \tag{2.20}$$

In order to show zero discord we have to check at most $L(L-1)/2$ commutators, where $L = \text{rank}R \leq \min\{d_A^2, d_B^2\}$. Now, recall that the state of zero discord is of the form $\rho = \sum_{k=1}^{d_A} p_k \Pi_k \otimes \rho_k$, therefore is a sum of at most d_A product operators. This bounds the rank of the correlation tensor to $L \leq d_A$. Thus, the rank of the correlation tensor is the simple discord witness: If $L > d_A$, the state has a non-zero discord.

Correlation matrix can be obtained directly by simple measurements usually involved in quantum state tomography. However, the detection of non-zero discord does not necessarily require measurement of all $(d_A d_B)^2$ elements of the correlation matrix (full state tomography). It is sufficient that the experimentalist measures that many elements of the correlation matrix until he finds $d_A + 1$ linearly independent rows (or columns) of the correlation matrix.

2.3.3 Geometric measure of discord

Evaluation of quantum discord given by equation (2.16) in general requires considerable numerical minimization. Different measures of quantum discord [33] and their extensions to multipartite systems [136] have been proposed. However, analytical expression are known only for certain classes of states [128, 59, 162, 5, 3, 79]. Here we propose a following geometric measure

$$D_A^{(2)}(\rho) = \min_{\chi \in \Omega_0} \|\rho - \chi\|^2, \tag{2.21}$$

where Ω_0 denotes the set of zero-discord states and $\|X - Y\|^2 = \text{Tr}(X - Y)^2$ is the square norm in the Hilbert-Schmidt space. We will show how to evaluate this quantity for an arbitrary two-qubit state.

Two-qubit case

Consider the case $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$. We write a state ρ in Bloch representation:

$$\rho = \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} + \sum_{i=1}^{3} x_i \sigma_i \otimes \mathbb{1} + \sum_{i=1}^{3} y_i \mathbb{1} \otimes \sigma_i + \sum_{i,j=1}^{3} T_{ij} \sigma_i \otimes \sigma_j), \tag{2.22}$$

where $x_i = \mathrm{Tr}\rho(\sigma_i \otimes \mathbb{1})$, $y_i = \mathrm{Tr}\rho(\mathbb{1} \otimes \sigma_i)$ are components of the local Bloch vectors, $T_{ij} = \mathrm{Tr}\rho(\sigma_i \otimes \sigma_j)$ are components of the correlation tensor, and σ_i, $i \in \{1, 2, 3\}$, are the three Pauli matrices. To each state ρ we associate the triple $\{\vec{x}, \vec{y}, T\}$. Now, we characterize the set Ω_0. A zero-discord state is of the form $\chi = p_1|\psi_1\rangle\langle\psi_1| \otimes \rho_1 + p_2|\psi_2\rangle\langle\psi_2| \otimes \rho_2$, where $\{|\psi_1\rangle, |\psi_2\rangle\}$ is a single-qubit orthonormal basis, $\rho_{1,2}$ are 2×2 density matrices, and $p_{1,2}$ are non-negative numbers such that $p_1 + p_2 = 1$. We define $t = p_1 - p_2$ and three vectors

$$\vec{e} = \langle\psi_1|\vec{\sigma}|\psi_1\rangle, \tag{2.23}$$

$$\vec{s}_\pm = \mathrm{Tr}(p_1\rho_1 \pm p_2\rho_2)\vec{\sigma}. \tag{2.24}$$

It can easily be shown that $t\vec{e}$ and $\vec{s}_+$ represent the local Bloch vectors of the first and second qubit, respectively, while the vector $\vec{s}_-$ is directly related to the correlation tensor which is of the product form $T = \vec{e}\vec{s}_-^{\mathrm{T}}$. Therefore, a state of zero-discord χ has Bloch representation $\vec{\chi} = \{t\vec{e}, \vec{s}_+, \vec{e}\vec{s}_-^{\mathrm{T}}\}$, where $\|\vec{e}\| = 1$, $\|\vec{s}_\pm\| \leq 1$ and $t \in [-1, 1]$. The distance between states ρ and χ is given by

$$\begin{aligned} \|\rho - \chi\|^2 &= \|\rho\|^2 - 2\mathrm{Tr}\rho\chi + \|\chi\|^2 \\ &= \frac{1}{4}(1 + \|\vec{x}\|^2 + \|\vec{y}\|^2 + \|T\|^2) \\ &- \frac{1}{2}(1 + t\vec{x}\vec{e} + \vec{y}\vec{s}_+ + \vec{e}T\vec{s}_-) \\ &+ \frac{1}{4}(1 + t^2 + \|\vec{s}_+\|^2 + \|\vec{s}_-\|^2), \end{aligned} \tag{2.25}$$

where $\|T\|^2 = \mathrm{Tr}T^{\mathrm{T}}T$. First, we optimize the distance over parameters $\vec{s}_\pm$ and t. The function of equation (2.25) is convex and quadratic in its variables $t, \vec{s}_\pm$. It is straightforward to see that its Hessian is a positive and non-singular matrix. Therefore the function has a unique global minimum. The minimum occurs when the derivative is zero:

$$\frac{\|\rho - \chi\|^2}{\partial t} = \frac{1}{2}(-\vec{x}\vec{e} + t) = 0, \tag{2.26}$$

$$\frac{\|\rho - \chi\|^2}{\partial \vec{s}_+} = \frac{1}{2}(-\vec{y} + \vec{s}_+) = 0, \tag{2.27}$$

$$\frac{\|\rho - \chi\|^2}{\partial \vec{s}_-} = \frac{1}{2}(-T^{\mathrm{T}}\vec{e} + \vec{s}_-) = 0, \tag{2.28}$$

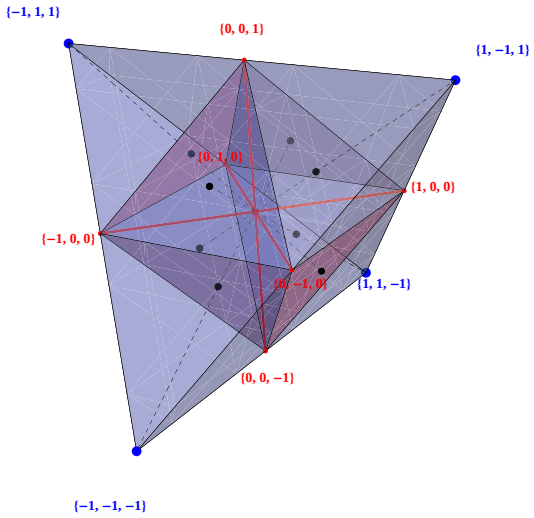

Figure 2.10: The set of two-qubit states with maximally mixed marginals (i.e. the reduced states of individual qubits are completely mixed). Physical states belong to the tetrahedron, among which separable ones are confined to the octahedron. The zero-discord states are labeled by the red lines (it is therefore clear that almost all states have non-zero discord [68]). The states with maximal value of discord correspond to the vertices of the tetrahedron (the four Bell states). Among the set of separable states, those which maximize discord are the centers of octahedron facets $(\pm 1, \pm 1, \pm 1)/3$ (black dots).

which gives the solution $t = \vec{x}\vec{e}$, $\vec{s}_+ = \vec{y}$ and $\vec{s}_- = T^{\mathrm{T}}\vec{e}$. Since the solution lies within the range of parameters, $|\vec{x}\vec{e}|, \|\vec{y}\|, \|T^{\mathrm{T}}\vec{e}\| \leq 1$ it represents the global minimum. After substituting the solution we obtain $\|\rho - \chi\|^2 = \frac{1}{4}\left(\|\vec{x}\|^2 + \|T\|^2 - \vec{e}(\vec{x}\vec{x}^{\mathrm{T}} + TT^{\mathrm{T}})\vec{e}\right)$ which attains the minimum when $\vec{e}$ is an eigenvector of matrix $K = \vec{x}\vec{x}^{\mathrm{T}} + TT^{\mathrm{T}}$ for the largest eigenvalue. Therefore, we have:

$$D_A^{(2)}(\rho) = \frac{1}{4}(\|\vec{x}\|^2 + \|T\|^2 - k_{\max}), \tag{2.29}$$

where $k_{\max}$ is the largest eigenvalue of matrix $K = \vec{x}\vec{x}^{\mathrm{T}} + TT^{\mathrm{T}}$. Next, we apply our criterion to a class of states.

States with maximally mixed marginals

We consider an example of two qubit states with maximally mixed marginals. Such a state is locally equivalent (under some local unitary transformation $U_1 \otimes U_2$) to a state $\rho(\vec{t}) = (\mathbb{1} \otimes \mathbb{1} + \sum_{i=1}^{3} t_i \sigma_i \otimes \sigma_i)/4$, where $\vec{t} = (t_1, t_2, t_3)$. The state $\rho(\vec{t})$ is physical if $\vec{t}$ belongs to the tetrahedron (Figure 2.10) defined by the set of vertices $(-1, -1, -1)$, $(-1, 1, 1)$, $(1, -1, 1)$ and $(1, 1, -1)$, while is separable if $\vec{t}$ belongs to the octahedron defined by the set of vertices $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$ and $(0, 0, \pm 1)$ [103]. Simple calculation

shows that $D_A^{(2)}(\vec{t}) = \frac{1}{4}(t_1^2 + t_2^2 + t_3^2 - \max\{t_1^2, t_2^2, t_3^2\})$. The zero-discord states have at most one non-zero component of vector $\vec{t}$ (Figure 2.10, red lines). The function $D_A^{(2)}(\vec{t})$ reaches its maximal value of $D_A^{(2)} = 1/2$ at the vertices of tetrahedron which represent the four Bell states. Within the set of separable states (octahedron) its maximal value of $D_A^{(2)} = 1/6$ is attained at the centers of octahedron facets $(\pm 1, \pm 1, \pm 1)/3$. They represent the states

$$\rho_{i_1 i_2 i_3} = \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} + \frac{1}{3}\sum_{k=1}^{3}(-1)^{i_k}\sigma_k \otimes \sigma_k), \tag{2.30}$$

where $i_k = \pm 1$, and can intuitively be understood as equal mixture of "maximally non-orthogonal" states. The states are symmetric under exchange of subsystems, thus they have the same value of "left" and "right" discord $D_A = D_B$.

2.3.4 DQC1 model

In [114], Knill and Laflamme introduced the model of mixed-state quantum computing which preforms the task of evaluating the normalized trace of a unitary matrix efficiently. The corresponding quantum circuit is shown in Figure 2.11. The input state is a highly mixed separable state and consists of a control qubit in the state $\frac{1}{2}(\mathbb{1} + \alpha\sigma_3)$, where α describes the purity, and a collection of n qubits in the maximally mixed state $\frac{1}{2^n}\mathbb{1}_n$, where $\mathbb{1}_n$ is the n-qubit identity. The DQC1 circuit consists of the Hadamard gate applied to the control qubit and a control n-qubit unitary gate U_n. The output state is:

$$\rho = \frac{1}{2^{n+1}}(\mathbb{1}_1 \otimes \mathbb{1}_n + \alpha|1\rangle\langle 0| \otimes U_n + \alpha|0\rangle\langle 1| \otimes U_n^\dagger). \tag{2.31}$$

We consider only the cases $\alpha \neq 0$, otherwise the state at the output is completely mixed and therefore cannot accomplish the task. After measuring the control qubit at the output in the eigenbasis of σ_1 and σ_2, we retrieve the normalized trace of the unitary matrix $\tau = \mathrm{Tr}U_n/2^n$ with the polynomial overhead scaling $1/\alpha^2$ [54].

The control qubit is completely separable from the rest of the qubits. The output state has vanishingly small entanglement across any bipartite split that groups the control qubit with some of the mixed qubits [114]. However, there is strong evidence that DQC1 task cannot be preformed efficiently using classical computation [55]. The question is what brings a "speed-up" in the considered task? The quantum discord was proposed as a figure of merit for characterizing the resources present in DQC1 model [54]. It has been shown that for almost every unitary matrix U_n (random unitary) the discord in the output state (2.31) is non-vanishing. Here we derive an explicit

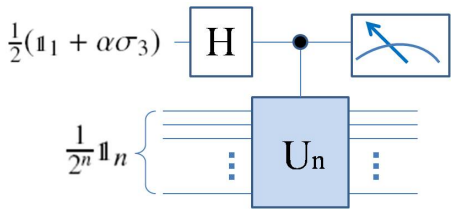

Figure 2.11: The quantum circuit for estimating the normalized trace of the unitary matrix U_n using the model of deterministic computing with one quantum bit (DQC1). H stands for the Hadamard gate. The control (top) qubit is measured in the σ_1 and σ_2 basis, and the expectation values give the real and imaginary part of normalized trace $\tau = \mathrm{Tr}U_n/2^n$ with the overhead scaling as $\frac{1}{\alpha^2}$ [54].

condition for characterizing the correlations in the output state and show that the discord is unlikely to be the source of speedup. We re-write it into a form:

$$\rho = \frac{1}{2^{n+1}}\left(\mathbb{1}_1 \otimes \mathbb{1}_n + \alpha\sigma_1 \otimes \frac{U_n + U_n^\dagger}{2} + \alpha\sigma_2 \otimes \frac{U_n - U_n^\dagger}{2i}\right). \tag{2.32}$$

Now, we apply the condition (2.20). The operators σ_1 and σ_2 do not commute, therefore, the state ρ is of the zero-discord if and only if the operators $\frac{U_n+U_n^\dagger}{2}$ and $\frac{U_n-U_n^\dagger}{2i}$ are linearly dependent, or equivalently $U_n^\dagger = kU_n$. This is possible if and only if $U_n = \mathrm{e}^{i\phi}A$, where $A^2 = \mathbb{1}$ is a binary observable. For such a unitary all the correlations at the output of DQC1 circuit are classical. However, it is very unlikely that the normalized trace of $\mathrm{e}^{i\phi}A$ can be evaluated efficiently on a classical computer, since all it's eigenvectors can be arbitrarily complex (random states).

We emphasize that our measure of discord is not monotonic under local operations. This, however, is not a shortcoming, as discord, unlike entanglement and mutual information, can in fact increase as well as decrease under local operations (even without the presence of classical correlations). A simple example of the local increase is to start from a zero-discord state $|00\rangle\langle 00| + |11\rangle\langle 11|$ and transform, say the first qubit, so that $|0\rangle \to |\psi_0\rangle$ and $|1\rangle \to |\psi_1\rangle$, such that $|\psi_0\rangle$ and $|\psi_1\rangle$ are not orthogonal. The resulting state, $|0\Psi_0\rangle\langle 0\Psi_0| + |1\psi_1\rangle\langle 1\psi_1|$ clearly has a non-vanishing discord. Finally, we point out that our method can be extended to any number of subsystems, though evaluating the measure of discord becomes progressively more difficult with increasing number of subsystems and their dimensionality.

Note added.—A related work was done by Datta [52].

Summary and Outlook

In the summary, I give a brief overview and outlook of the work presented here. There are six topics in total that are covered by the thesis:

- **Limited information content**, as a fundamental principle of nature was investigated from the operational perspective. Based on this principle the whole hierarchy of "quantum-like" theories is derived for an elementary system. The information encoded in the system supposed to be fundamentally limited to one bit, therefore no underlying hidden structure (in the form of hidden variables) is possible, and the results are irreducibly random. As a final remark, the examples of generalized theories are given which share some essential features with quantum mechanics but nevertheless differ from it. This perhaps suggests that either Nature admits additional principles that single out quantum theory from the more general class of theories or the alternatives are also realized in some domain that is still beyond our observations. The work is based on the following publication: B. Dakić, T. Paterek, and Č. Brukner, *Theories of systems with limited information content*, New J. Phys. **12**, 053037 (2010).

- **Mutually unbiased bases**, and their connection to orthogonal Latin squares was analyzed. Certain results for Latin squares can be applied to disprove the existence of certain classes of mutually unbiased bases when the system's dimensions is not a power of prime. Finally, using the Latin squares, the hidden-variable model are constructed that efficiently reproduce the measurement statistics of MUBs. The work is based on the following publication: T. Paterek, B. Dakić, and Č. Brukner, *Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models* , Phys. Rev. A **79**, 012109 (2009).

- **Reconstruction of quantum theory** is the procedure of recovering quantum formalism from a set of physically motivated assumptions (principles or axioms). In the work presented here such a task was accomplished by employing three simple physical principles: information capacity, locality and reversibility. In such a framework there was a room for quantum and classical probability theory, the only two theories for which we have an empirical evidences. A significant result that follows from the reconstruction is that no probability theory other than quantum theory can exhibit entanglement without contradicting one or more axioms. Perhaps, this suggest that going beyond quantum theory in a

"reasonable" way would require some new physical concepts that may go even beyond probabilistic description of Nature. The work is based on the following publication: B. Dakić, and Č. Brukner, *Quantum Theory and Beyond: Is Entanglement Special?*, in "Deep Beauty: Understanding the Quantum World through Mathematical Innovation", Eds. H. Halvorson, (Cambridge University Press, 2011), 365-392.

- **The expense of classical simulation of quantum statistics** was investigated. An interesting result has been found that only polynomial number Poly(N) of classical states (hidden-variables) is needed to reproduce the quantum statistics based on N measurement settings for an arbitrary quantum state. The model in the limit of continuous number of measurement settings converges to the model where each quantum state is a hidden-variable itself (a non-deterministic model). In the conclusion, we could say that quantum mechanics is indeed the most efficient description of itself. The work is based on the following publication: B. Dakić, M. Šuvakov, T. Paterek, and Č. Brukner, *Efficient Hidden-Variable Simulation of Measurements in Quantum Experiments*, Phys. Rev. Lett. **101**, 190402 (2008).

- **Quantum simulation** of a frustrated spin tetramer was investigated. The tetramer was experimentally realized using polarization of four entangled photons. The adiabatic evolution was achieved by employing a tunable gate capable of creating exotic states such as valence bond liquid. In the conclusion we could say that the field of quantum information greatly benefits from small-scale quantum simulators, such as one presented here in a way that they provide a technological and innovation insights towards building universal quantum simulator. The work is based on the following publication: X. Ma, B. Dakić, W. Naylor, A. Zeilinger, P. Walther, *Quantum simulation of the wavefunction to probe frustrated Heisenberg spin systems*, Nat. Phys. **7**, 399–405 (2011).

- **Quantum correlations** captured by quantum discord were analyzed. A handy necessary and sufficient condition for non-zero discord is found. Based on this, the presence of quantum discord can be verified directly from the measurement results. The geometric measure of quantum discord is introduced, with the significant difference to other measures, i.e. easy evaluation without need of minimization procedures. At the end, the resources in mixed-state computation setup were analyzed. What was found is that quantum discord is unlikely to be the reason of speedup in such a model. The work is based on the following publica-

tion: B. Dakić, V. Vedral, and Č. Brukner, *Necessary and sufficient condition for non-zero quantum discord*, Phys. Rev. Lett. **105**, 190502 (2010).

Bibliography

[1] S. Aaronson. Quantum computing and hidden variables. *Phys. Rev. A*, 71(3):032325, 2005.

[2] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. In *Logic in Computer Science, 2004. Proceedings of the 19th Annual IEEE Symposium on*, pages 415 – 425, 2004.

[3] G. Adesso and A. Datta. Quantum versus classical correlations in gaussian states. *Phys. Rev. Lett.*, 105(3):030501, Jul 2010.

[4] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki. Rigorous results on valence-bond ground states in antiferromagnets. *Phys. Rev. Lett.*, 59(7):799–802, Aug 1987.

[5] M. Ali, A. R. P. Rau, and G. Alber. Quantum discord for two-qubit x states. *Phys. Rev. A*, 81(4):042105, Apr 2010.

[6] J. Ambjørn, J. Jurkiewicz, and R. Loll. Reconstructing the universe. *Phys. Rev. D*, 72(6):064014, Sep 2005.

[7] L. Amico, R. Fazio, A. Osterloh, and V. Vedral. Entanglement in many-body systems. *Rev. Mod. Phys.*, 80(2):517–576, May 2008.

[8] P. Anderson. The resonating valence bond state in La_2CuO_4 and superconductivity. *Science*, 235(4793):1196, 1987.

[9] A. Aspuru-Guzik, A. Dutoi, P. Love, and M. Head-Gordon. Simulated quantum computation of molecular energies. *Science*, 309(5741):1704, 2005.

[10] W. Bakr, A. Peng, M. Tai, R. Ma, J. Simon, J. Gillen, S. Foelling, L. Pollet, and M. Greiner. Probing the superfluid–to–mott insulator transition at the single-atom level. *Science*, 329(5991):547, 2010.

[11] W. S. Bakr, J. I. Gillen, A. Peng, S. Fölling, and M. Greiner. A quantum gas microscope for detecting single atoms in a Hubbard-regime optical lattice. *Nature*, 462:74–77, 2009.

[12] L. Balents. Spin liquids in frustrated magnets. *Nature*, 464(7286):199–208, 2010.

[13] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34:512–528, 2008.

[14] H. Barnum, J. Barrett, M. Leifer, and A. Wilce. Cloning and Broadcasting in Generic Probabilistic Theories. *ArXiv e-prints*, 2006.

[15] H. Barnum, J. Barrett, M. Leifer, and A. Wilce. Generalized no-broadcasting theorem. *Phys. Rev. Lett.*, 99(24):240501, 2007.

[16] H. Barnum and A. Wilce. Information processing in convex operational theories. *ArXiv e-prints*, 2009.

[17] H. Barnum and A. Wilce. Ordered linear spaces and categories as frameworks for information-processing characterizations of quantum and classical theory. *ArXiv e-prints*, 2009.

[18] J. Barrett. Information processing in generalized probabilistic theories. *Phys. Rev. A*, 75(3):032304, 2007.

[19] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.

[20] I. Bengtsson. MUBs, Polytopes, and Finite Geometries. In A. Khrennikov, editor, *Foundations of Probability and Physics - 3*, volume 750 of *American Institute of Physics Conference Series*, pages 63–69, Feb. 2005.

[21] I. Bengtsson, W. Bruzda, A. Ericsson, J. Larsson, W. Tadej, and K. Życzkowski. Mutually unbiased bases and hadamard matrices of order six. *Journal of mathematical physics*, 48:052106, 2007.

[22] I. Bialynicki-Birula and J. Mycielski. Nonlinear wave mechanics. *Annals of Physics*, 100(1-2):62 – 93, 1976.

[23] J. Biamonte, V. Bergholm, J. Whitfield, J. Fitzsimons, and A. Aspuru-Guzik. Adiabatic quantum simulators. *Arxiv preprint arXiv:1002.0368*, 2010.

[24] H. Boerner. *Representations of groups*. Amsterdam: North- Holland publishing company, 1963.

[25] D. Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. I. *Phys. Rev.*, 85(2):166–179, Jan 1952.

[26] D. Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. II. *Phys. Rev.*, 85(2):180–193, Jan 1952.

[27] A. Bohr and O. Ulfbeck. Primary manifestation of symmetry. origin of quantal indeterminacy. *Rev. Mod. Phys.*, 67(1):1–35, Jan 1995.

[28] M. Born and V. Fock. Beweis des Adiabatensatzes. *Zeitschrift fur Physik*, 51:165–180, Mar. 1928.

[29] P. O. Boykin, M. Sitharam, P. H. Tiep, and P. Wocjan. Mutually Unbiased Bases and Orthogonal Decompositions of Lie Algebras. *ArXiv Quantum Physics e-prints*, June 2005.

[30] C. Brans and R. H. Dicke. Mach's principle and a relativistic theory of gravitation. *Phys. Rev.*, 124(3):925–935, Nov 1961.

[31] 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.*, 96(25):250401, Jun 2006.

[32] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for nmr quantum computing. *Phys. Rev. Lett.*, 83(5):1054–1057, Aug 1999.

[33] A. Brodutch and D. R. Terno. Quantum discord, local operations, and Maxwell's demons. *Phys. Rev. A*, 81(6):062103, Jun 2010.

[34] Č. Brukner, M. Aspelmeyer, and A. Zeilinger. Complementarity and information in "delayed-choice for entanglement swapping". *Foundations of Physics*, 35(11):1909–1919, 2005.

[35] Č. Brukner and V. Vedral. Macroscopic Thermodynamical Witnesses of Quantum Entanglement. *ArXiv Quantum Physics e-prints*, June 2004.

[36] Č. Brukner and A. Zeilinger. Operationally invariant information in quantum measurements. *Phys. Rev. Lett.*, 83(17):3354–3357, Oct 1999.

[37] Č. Brukner and A. Zeilinger. Encoding and decoding in complementary bases with quantum gates. *Journal of Modern Optics*, 47(12):2233–2246, 2000.

[38] Č. Brukner and A. Zeilinger. Young's experiment and the finiteness of information. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 360(1794):1061–1069, 2002.

[39] Č. Brukner and A. Zeilinger. Information and Fundamental Elements of the Structure of Quantum Theory. In L. Castell & O. Ischebeck, editor, *Time, Quantum and Information*, 2003.

[40] Č. Brukner and A. Zeilinger. Information Invariance and Quantum Probabilities. *Foundations of Physics*, 39:677–689, July 2009.

[41] Č. Brukner and A. Zeilinger. Information Invariance and Quantum Probabilities. *Foundations of Physics*, 39:677–689, July 2009.

[42] I. Buluta and F. Nori. Quantum simulators. *Science*, 326(5949):108, 2009.

[43] A. Caticha. Consistency, amplitudes, and probabilities in quantum theory. *Phys. Rev. A*, 57(3):1572–1582, Mar 1998.

[44] R. Clifton, J. Bub, and H. Halvorson. Characterizing quantum theory in terms of information-theoretic constraints. *Foundations of Physics*, 33:1561–1591, 2003.

[45] V. Coffman, J. Kundu, and W. K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61(5):052306, Apr 2000.

[46] C. J. Colbourn and J. H. Dinitz. *The CRC Handbook of Combinatorial Designs*. CRC Press, Boca Raton, Florida, 1996.

[47] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs*. CRC Press, 2007.

[48] B. Dakić and Č. Brukner. Quantum theory and beyond: Is entanglement special? In H. Halvorson, editor, *Deep Beauty: Understanding the Quantum World Through Mathematical Innovation*. Cambridge University Press, 2011.

[49] B. Dakić, M. Šuvakov, T. Paterek, and Č. Brukner. Efficient hidden-variable simulation of measurements in quantum experiments. *Phys. Rev. Lett.*, 101(19):190402, Nov 2008.

[50] G. M. D'Ariano. Probabilistic theories: What is special about quantum mechanics? In A. Bokulich and G. Jaeger, editors, *Philosophy of Quantum Information and Entanglement*. Cambridge University Press, 2010.

[51] A. Datta. *Studies on the role of entanglement in mixed-state quantum computation*. PhD thesis, The University of New Mexico, 2008.

[52] A. Datta. A Condition for the Nullity of Quantum Discord. *ArXiv e-prints*, Mar. 2010.

[53] A. Datta, S. T. Flammia, and C. M. Caves. Entanglement and the power of one qubit. *Phys. Rev. A*, 72(4):042316, Oct 2005.

[54] A. Datta, A. Shaji, and C. M. Caves. Quantum discord and the power of one qubit. *Phys. Rev. Lett.*, 100(5):050502, Feb 2008.

[55] A. Datta and G. Vidal. Role of entanglement and correlations in mixed-state quantum computation. *Phys. Rev. A*, 75(4):042310, Apr 2007.

[56] K. A. Dennison and W. K. Wootters. Entanglement sharing among quantum particles with more than two orthogonal states. *Phys. Rev. A*, 65(1):010301, Dec 2001.

[57] D. Deutsch. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[58] D. Deutsch and R. Jozsa. Rapid Solution of Problems by Quantum Computation. *Royal Society of London Proceedings Series A*, 439:553–558, Dec. 1992.

[59] R. Dillenschneider. Quantum discord and quantum phase transition in spin chains. *Phys. Rev. B*, 78(22):224413, Dec 2008.

[60] L. Diósi. Models for universal reduction of macroscopic quantum fluctuations. *Phys. Rev. A*, 40(3):1165–1174, Aug 1989.

[61] J. Du, N. Xu, X. Peng, P. Wang, S. Wu, and D. Lu. NMR implementation of a molecular hydrogen quantum simulation with adiabatic state preparation. *Phys. Rev. Lett.*, 104(3):030502, Jan 2010.

[62] S. Dürr, T. Nonn, and G. Rempe. Fringe visibility and which-way information in an atom interferometer. *Phys. Rev. Lett.*, 81(26):5705–5709, Dec 1998.

[63] T. Durt. About mutually unbiased bases in even and odd prime power dimensions. *Journal of Physics A: Mathematical and General*, 38(23):5267, 2005.

[64] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935.

[65] B.-G. Englert. Fringe visibility and which-way information: An inequality. *Phys. Rev. Lett.*, 77(11):2154–2157, Sep 1996.

[66] L. Euler. On magic squares. *Comm. Arithm.*, 2, 1849.

[67] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Quantum Computation by Adiabatic Evolution. *ArXiv Quantum Physics e-prints*, Jan. 2000.

[68] A. Ferraro, L. Aolita, D. Cavalcanti, F. M. Cucchietti, and A. Acín. Almost all quantum states have nonclassical correlations. *Phys. Rev. A*, 81(5):052318, May 2010.

[69] R. Feynman. Quantum mechanical computers. *Foundations of physics*, 16(6):507–531, 1986.

[70] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 1982.

[71] D. I. Fivel. How interference effects in mixtures determine the rules of quantum mechanics. *Phys. Rev. A*, 50(3):2108–2119, Sep 1994.

[72] A. Friedenauer, H. Schmitz, J. Glueckert, D. Porras, and T. Schätz. Simulating a quantum magnet with trapped ions. *Nature Physics*, 4(10):757–761, 2008.

[73] C. A. Fuchs. Quantum mechanics as quantum information (and only a little more). In A. Khrenikov, editor, *Quantum Theory: Reconstruction of Foundations*. Växjo University Press, 2003.

[74] C. A. Fuchs. Private communication, 2007.

[75] R. Gähler, A. G. Klein, and A. Zeilinger. Neutron optical tests of nonlinear wave mechanics. *Phys. Rev. A*, 23(4):1611–1617, Apr 1981.

[76] R. Gerritsma, G. Kirchmair, F. Zähringer, E. Solano, R. Blatt, and C. Roos. Quantum simulation of the dirac equation. *Nature*, 463(7277):68–71, 2010.

[77] G. C. Ghirardi, A. Rimini, and T. Weber. Unified dynamics for microscopic and macroscopic systems. *Phys. Rev. D*, 34(2):470–491, Jul 1986.

[78] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters. Discrete phase space based on finite fields. *Phys. Rev. A*, 70(6):062101, Dec 2004.

[79] P. Giorda and M. G. A. Paris. Gaussian quantum discord. *Phys. Rev. Lett.*, 105(2):020503, Jul 2010.

[80] V. Giovannetti, S. Lloyd, and L. Maccone. Quantum-enhanced measurements: Beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004.

[81] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1):145–195, Mar 2002.

[82] P. Goyal. Information-geometric reconstruction of quantum theory. *Phys. Rev. A*, 78(5):052120, Nov 2008.

[83] P. Goyal, K. H. Knuth, and J. Skilling. Origin of complex quantum amplitudes and Feynman's rules. *Phys. Rev. A*, 81(2):022109, Feb 2010.

[84] P. Grangier. Contextual objectivity: a realistic interpretation of quantum mechanics. *European Journal of Physics*, 23(3):331, 2002.

[85] P. Grangier. Contextual objectivity and the quantum formalism. *International Journal of Quantum Information*, 3:17–22, 2005.

[86] M. Grassl. Private communication.

[87] M. Grassl. On SIC-POVMs and MUBs in Dimension 6. *ArXiv Quantum Physics e-prints*, June 2004.

[88] D. Greenberger, M. A. Horne, and A. Zeilinger. Going beyond Bell's theorem. In M. Kafatos, editor, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*. Kluwer Academic, Dordrecht, 1989.

[89] M. Greiner, O. Mandel, T. Esslinger, T. Hänsch, and I. Bloch. Quantum phase transition from a superfluid to a mott insulator in a gas of ultracold atoms. *Nature*, 415(6867):39–44, 2002.

[90] A. Grinbaum. Reconstruction of Quantum Theory. *The British Journal for the Philosophy of Science*, 58:387–408, 2001.

[91] A. Grinbaum. Elements of information-theoretic derivation of the formalism of quantum theory. *International Journal of Quantum Information*, 1:289–300, 2003.

[92] S. Gröblacher, T. Paterek, R. Kaltenbaek, Č. Brukner, M. Żukowski, M. Aspelmeyer, and A. Zeilinger. An experimental test of non-local realism. *Nature*, 446:871–875, Apr. 2007.

[93] B. Groisman, S. Popescu, and A. Winter. Quantum, classical, and total amount of correlations in a quantum state. *Phys. Rev. A*, 72(3):032317, Sep 2005.

[94] D. Gross, M. Müller, R. Colbeck, and O. C. O. Dahlsten. All reversible dynamics in maximally nonlocal theories are trivial. *Phys. Rev. Lett.*, 104(8):080402, Feb 2010.

[95] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2):325–328, Jul 1997.

[96] L. Hardy. Quantum Theory From Five Reasonable Axioms. *ArXiv e-prints*, Jan. 2001.

[97] L. Hardy. Quantum ontological excess baggage. *Studies In History and Philosophy of Science Part B: Studies In History and Philosophy of Modern Physics*, 35(2):267 – 276, 2004.

[98] N. Harrigan and T. Rudolph. Ontological models and the interpretation of contextuality. *ArXiv e-prints*, Sept. 2007.

[99] N. Harrigan, T. Rudolph, and S. Aaronson. Representing probabilistic data via ontological models. *ArXiv e-prints*, Sept. 2007.

[100] A. Hayashi, M. Horibe, and T. Hashimoto. Mean king's problem with mutually unbiased bases and orthogonal latin squares. *Phys. Rev. A*, 71(5):052331, May 2005.

[101] L. Henderson and V. Vedral. Classical, quantum and total correlations. *Journal of Physics A: Mathematical and General*, 34(35):6899, 2001.

[102] A. S. Holevo. Some estimates for the amount of information transmittable by a quantum communication channel. *Problems Inf. Transmission*, 9:177–183, 1973.

[103] R. Horodecki and M. Horodecki. Information-theoretic aspects of inseparability of mixed states. *Phys. Rev. A*, 54(3):1838–1843, Sep 1996.

[104] D. I. Ivanović. Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, 14(12):3241, 1981.

[105] D. Jaksch and P. Zoller. The cold atom Hubbard toolbox. *Annals of Physics*, 315:52–79, Jan. 2005.

[106] D. James, P. Kwiat, W. Munro, and A. White. Measurement of qubits. *Physical Review A*, 64(5):052312, 2001.

[107] N. S. Jones and N. Linden. Parts of quantum states. *Phys. Rev. A*, 71(1):012324, Jan 2005.

[108] H. Kaiser, E. A. George, and S. A. Werner. Neutron interferometric search for quaternions in quantum mechanics. *Phys. Rev. A*, 29(4):2276–2279, Apr 1984.

[109] F. Károlyházy. Gravitation and quantum mechanics of macroscopic bodies. *Magyar Fizikai Folyóirat*, 22:33. Thesis, in Hungarian.

[110] F. Károlyházy. Gravitation and quantum mechanics of macroscopic objects. *Nuovo Cimento A Serie*, 42:390–402, Mar. 1966.

[111] I. Kassal, S. Jordan, P. Love, M. Mohseni, and A. Aspuru-Guzik. Polynomial-time quantum algorithm for the simulation of chemical dynamics. *Proceedings of the National Academy of Sciences*, 105(48):18681, 2008.

[112] K. Kim, M. Chang, S. Korenblit, R. Islam, E. Edwards, J. Freericks, G. Lin, L. Duan, and C. Monroe. Quantum simulation of frustrated ising spins with trapped ions. *Nature*, 465(7298):590–593, 2010.

[113] A. Klappenecker and M. Rötteler. Constructions of mutually unbiased bases. *Finite fields and applications*, pages 262–266, 2004.

[114] E. Knill and R. Laflamme. Power of one bit of quantum information. *Phys. Rev. Lett.*, 81(25):5672–5675, Dec 1998.

[115] E. Knill, R. Laflamme, and G. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[116] S. Kochen and E. Specker. The problem of hidden variables in quantum mechanics. *Indiana Univ. Math. J.*, 17:59–87, 1968.

[117] B. P. Lanyon, M. Barbieri, M. P. Almeida, and A. G. White. Experimental quantum computing without entanglement. *Phys. Rev. Lett.*, 101(20):200501, Nov 2008.

[118] B. P. Lanyon, J. D. Whitfield, G. G. Gillett, M. E. Goggin, M. P. Almeida, I. Kassal, J. D. Biamonte, M. Mohseni, B. J. Powell, M. Barbieri, A. Aspuru-Guzik, and A. G. White. Towards quantum chemistry on a quantum computer. *Nature Chemistry*, 2:106–111, Feb. 2010.

[119] J. Lawrence, Č. Brukner, and A. Zeilinger. Mutually unbiased binary observable sets on n qubits. *Phys. Rev. A*, 65(3):032320, Feb 2002.

[120] A. Leggett. Nonlocal hidden-variable theories and quantum mechanics: An incompatibility theorem. *Foundations of Physics*, 33:1469–1493, 2003.

[121] D. Leibfried, B. DeMarco, V. Meyer, M. Rowe, A. Ben-Kish, J. Britton, W. Itano, B. Jelenković, C. Langer, T. Rosenband, et al. Trapped-ion quantum simulator: experimental application to nonlinear interferometers. *Physical review letters*, 89(24):247901, 2002.

[122] M. Lewenstein, A. Sanpera, V. Ahufinger, B. Damski, A. Sen, and U. Sen. Ultracold atomic gases in optical lattices: mimicking condensed matter physics and beyond. *Advances in Physics*, 56(2):243–379, 2007.

[123] E. Lieb and D. Mattis. Ordering Energy Levels of Interacting Spin Systems. *Journal of Mathematical Physics*, 3:749–751, July 1962.

[124] N. Linden, S. Popescu, A. J. Short, and A. Winter. Quantum nonlocality and beyond: Limits from nonlocal computation. *Phys. Rev. Lett.*, 99(18):180502, Oct 2007.

[125] S. Lloyd. Universal quantum simulators. *Science*, 273(5278):1073–1073, 1996.

[126] C.-Y. Lu, W.-B. Gao, O. Gühne, X.-Q. Zhou, Z.-B. Chen, and J.-W. Pan. Demonstrating anyonic fractional statistics with a six-qubit quantum simulator. *Phys. Rev. Lett.*, 102(3):030502, Jan 2009.

[127] S. Luo. Maximum shannon entropy, minimum fisher information, and an elementary game. *Foundations of Physics*, 32:1757–1772, 2002.

[128] S. Luo. Quantum discord for two-qubit systems. *Phys. Rev. A*, 77(4):042303, Apr 2008.

[129] G. W. Mackey. Quantum mechanics and hilbert space. *The American Mathematical monthly*, 64(8):pp. 45–57, 1957.

[130] H. F. MacNeish. Euler squares. *The Annals of Mathematics*, 23(3):pp. 221–227, 1922.

[131] M. Mambrini, A. Läuchli, D. Poilblanc, and F. Mila. Plaquette valence-bond crystal in the frustrated Heisenberg quantum antiferromagnet on the square lattice. *Phys. Rev. B*, 74(14):144422, Oct. 2006.

[132] W. Marshall. Antiferromagnetism. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences*, 232(1188):48–68, 1955.

[133] L. Masanes, A. Acin, and N. Gisin. General properties of nonsignaling theories. *Phys. Rev. A*, 73(1):012112, Jan 2006.

[134] P. McMullen. The maximum number of faces of a convex polytope. *Mathematika*, 17:179, 1970.

[135] D. A. Meyer. Sophisticated quantum search without entanglement. *Phys. Rev. Lett.*, 85(9):2014–2017, Aug 2000.

[136] K. Modi, T. Paterek, W. Son, V. Vedral, and M. Williamson. Unified view of quantum and classical correlations. *Phys. Rev. Lett.*, 104(8):080501, Feb 2010.

[137] A. Montina. Condition for any realistic theory of quantum systems. *Phys. Rev. Lett.*, 97(18):180401, Oct 2006.

[138] A. Montina. Exponential complexity and ontological theories of quantum mechanics. *Phys. Rev. A*, 77(2):022104, Feb 2008.

[139] M. Navascues and H. Wunderlich. A glance beyond the quantum model. *Royal Society of London Proceedings Series A*, 466:881–890, Nov. 2009.

[140] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 1 edition, Jan. 2000.

[141] H. Ollivier and W. H. Zurek. Quantum discord: A measure of the quantumness of correlations. *Phys. Rev. Lett.*, 88(1):017901, Dec 2001.

[142] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki. Thermodynamical approach to quantifying quantum correlations. *Phys. Rev. Lett.*, 89(18):180402, Oct 2002.

[143] T. Osborne and F. Verstraete. General monogamy inequality for bipartite qubit entanglement. *Physical review letters*, 96(22):220503, 2006.

[144] J. K. Pachos, W. Wieczorek, C. Schmid, N. Kiesel, R. Pohlner, and H. Weinfurter. Revealing anyonic features in a toric code quantum simulation. *New Journal of Physics*, 11(8):083010, 2009.

[145] T. Paterek, B. Dakić, and Č. Brukner. Mutually unbiased bases, orthogonal latin squares, and hidden-variable models. *Phys. Rev. A*, 79(1):012109, Jan 2009.

[146] T. Paterek, B. Dakić, and Č. Brukner. Theories of systems with limited information content. *New Journal of Physics*, 12(5):053037, 2010.

[147] T. Paterek, J. Kofler, R. Prevedel, P. Klimek, M. Aspelmeyer, A. Zeilinger, and Č. Brukner. Logical independence and quantum randomness. *New Journal of Physics*, 12(1):013019, 2010.

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

[149] P. Pearle. Reduction of the state vector by a nonlinear Schrödinger equation. *Phys. Rev. D*, 13(4):857–868, Feb 1976.

[150] X. Peng, J. Zhang, J. Du, and D. Suter. Quantum simulation of a system with competing two-and three-body interactions. *Physical review letters*, 103(14):140501, 2009.

[151] R. Penrose. On gravity's role in quantum state reduction. *General Relativity and Gravitation*, 28:581–600, 1996.

[152] A. Peres. Proposed test for complex versus quaternion quantum theory. *Phys. Rev. Lett.*, 42(11):683–686, Mar 1979.

[153] A. Peres. Two simple proofs of the Kochen-Specker theorem. *Journal of Physics A: Mathematical and General*, 24(4):L175, 1991.

[154] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, 1995.

[155] A. Peres. Quaternionic quantum interferometry. In F. De Martini, G. Denardo, and A. Zeiliger, editors, *Quantum Interferometry*, pages 431–437. VCH Publ., 1996.

[156] M. Piani, P. Horodecki, and R. Horodecki. No-local-broadcasting theorem for multipartite quantum correlations. *Phys. Rev. Lett.*, 100(9):090502, Mar 2008.

[157] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24:379–385, 1994.

[158] C. A. Rodríguez-Rosario, K. Modi, A. meng Kuah, A. Shaji, and E. C. G. Sudarshan. Completely positive maps and classical correlations. *Journal of Physics A: Mathematical and Theoretical*, 41(20):205301, 2008.

[159] C. Rovelli. Relational quantum mechanics. *International Journal of Theoretical Physics*, 35:1637–1678, Aug. 1996.

[160] T. Rudolph. Ontological Models for Quantum Mechanics and the Kochen-Specker theorem. *ArXiv Quantum Physics e-prints*, Aug. 2006.

[161] M. Saniga, M. Planat, and H. Rosu. Mutually unbiased bases and finite projective planes. *Journal of Optics B: Quantum and Semiclassical Optics*, 6(9):L19, 2004.

[162] M. S. Sarandy. Classical correlation and quantum discord in critical systems. *Phys. Rev. A*, 80(2):022108, Aug 2009.

[163] V. Scarani and N. Gisin. Quantum communication between *n* partners and bell's inequalities. *Phys. Rev. Lett.*, 87(11):117901, Aug 2001.

[164] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31(04):555–563, 1935.

[165] E. Schrödinger. Probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 32(03):446–452, 1936.

[166] A. Shabani and D. A. Lidar. Vanishing quantum discord is necessary and sufficient for completely positive maps. *Phys. Rev. Lett.*, 102(10):100402, Mar 2009.

[167] A. Shimony. Proposed neutron interferometer test of some nonlinear variants of wave mechanics. *Phys. Rev. A*, 20(2):394–396, Aug 1979.

[168] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. IEEE, 1994.

[169] C. G. Shull, D. K. Atwood, J. Arthur, and M. A. Horne. Search for a nonlinear variant of the Schrödinger equation by neutron interferometry. *Phys. Rev. Lett.*, 44(12):765–768, Mar 1980.

[170] U. Sinha, C. Couteau, Z. Medendorp, I. Söllner, R. Laflamme, R. Sorkin, and G. Weihs. Testing Born's Rule in Quantum Mechanics with a Triple Slit Experiment. In L. Accardi, G. Adenier, C. Fuchs, G. Jaeger, A. Y. Khrennikov, J.-. Larsson, & S. Stenholm, editor, *American Institute of Physics Conference Series*, volume 1101 of *American Institute of Physics Conference Series*, pages 200–207, Mar. 2009.

[171] S. Somaroo, C. Tseng, T. Havel, R. Laflamme, and D. Cory. Quantum simulations on a quantum computer. *Physical review letters*, 82(26):5381–5384, 1999.

[172] R. D. Sorkin. Quantum Mechanics as Quantum Measure Theory. *Modern Physics Letters A*, 9:3119–3127, 1994.

[173] R. Spekkens. Private communication.

[174] R. W. Spekkens. Contextuality for preparations, transformations, and unsharp measurements. *Phys. Rev. A*, 71(5):052108, May 2005.

[175] R. W. Spekkens. Evidence for the epistemic view of quantum states: A toy theory. *Phys. Rev. A*, 75(3):032110, Mar 2007.

[176] J. Summhammer. Maximum predictive power and the superposition principle. *International Journal of Theoretical Physics*, 33:171–178, 1994.

[177] J. Summhammer. Quantum Theory as Efficient Representation of Probabilistic Information. *ArXiv e-prints*, Jan. 2007.

[178] G. Tarry. Comptes rendu de l'association. *Francaise pour l'-Avancement de Science Naturel*, 1(122), 1900.

[179] S. Trebst, U. Schollwöck, M. Troyer, and P. Zoller. *d*-wave resonating valence bond states of fermionic atoms in optical lattices. *Phys. Rev. Lett.*, 96(25):250402, Jun 2006.

[180] S. Trotzky, L. Pollet, F. Gerbier, U. Schnorrberger, I. Bloch, N. V. Prokof'Ev, B. Svistunov, and M. Troyer. Suppression of the critical temperature for superfluidity near the Mott transition. *Nature Physics*, 6:998–1004, Dec. 2010.

[181] L. Vaidman, Y. Aharonov, and D. Z. Albert. How to ascertain the values of σ_x, σ_y, and σ_z of a spin-1/2 particle. *Phys. Rev. Lett.*, 58(14):1385–1387, Apr 1987.

[182] W. van Dam. Implausible Consequences of Superstrong Nonlocality. *ArXiv e-prints*, Jan. 2005.

[183] G. Ver Steeg and S. Wehner. *Quant. Inf. Comput.*, 9:801, 2009.

[184] F. Verstraete, J. Cirac, and J. Latorre. Quantum circuits for strongly correlated quantum systems. *Physical Review A*, 79(3):032316, 2009.

[185] C. F. von Weizsäcker. *Aufbau der Physik*. Carl Hanser, München, 1958.

[186] S. Weinberg. *Dreams of a Final Theory*. New York: Vintage, 1994.

[187] J. Wheeler. Law without Law in Quantum Theory and Measurement. In J. Wheeler and W. Zurek, editors, *Quantum Theory and Measurement*, page 182. Princeton: Princeton University Press, 1983.

[188] A. White, D. James, P. Eberhard, and P. Kwiat. Nonmaximally entangled states: Production, characterization, and utilization. *Physical review letters*, 83(16):3103–3107, 1999.

[189] P. Wocjan and T. Beth. New Construction of Mutually Unbiased Bases in Square Dimensions. *ArXiv Quantum Physics e-prints*, July 2004.

[190] M. Wojtas. Five mutually orthogonal latin squares of order 35. *Journal of Combinatorial Designs*, 4(2):153–154, 1996.

[191] W. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Physical Review Letters*, 80(10):2245–2248, 1998.

[192] W. Wootters. Quantum measurements and finite geometry. *Foundations of Physics*, 36:112–126, 2006. 10.1007/s10701-005-9008-x.

[193] W. K. Wootters. Statistical distance and hilbert space. *Phys. Rev. D*, 23(2):357–362, Jan 1981.

[194] W. K. Wootters. Quantum mechanics without probability amplitudes. *Found. Phys.*, 16(4):391, 1986.

[195] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363 – 381, 1989.

[196] G. Zauner. *Quantendesigns – Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, Universität Wien, 1999.

[197] A. Zeilinger. A foundational principle for quantum mechanics. *Foundations of Physics*, 29:631–643, 1999. 10.1023/A:1018820410908.

[198] P. Zoller, T. Beth, D. Binosi, R. Blatt, H. Briegel, D. Bruss, T. Calarco, J. Cirac, D. Deutsch, J. Eisert, et al. Quantum information processing and communication. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 36(2):203–228, 2005.

[199] K. Zyczkowski. Quartic quantum theory: an extension of the standard quantum mechanics. *Journal of Physics A: Mathematical and Theoretical*, 41(35):355302, 2008.

Curriculum vitae

Faculty of Physics,
University of Vienna
Boltzmanngasse 5
A-1090 Vienna
Austria
Phone: +43-(0)1-4277-51336
Fax: +43-(0)1-4277-9552
E-mail: borivoje.dakic@univie.ac.at
Website: http://quantumfoundations.weebly.com

Personal Information

Name	Borivoje Dakić
Date and place of birth	October 30, 1980, Šabac, Serbia
Citizenship	Serbian

Education

2007-present	PhD studies Faculty of Physics, University of Vienna supervisor: Prof. Dr. Časlav Brukner
2004-2007	M.Sc. in Physics Faculty of Physics, University of Belgrade thesis: *Symmetry adapted generalized Bloch functions of monoperiodic systems* supervisor: Prof. Dr. Ivanka Milošević
1999-2004	B.Sc. in Physics Faculty of Physics, University of Belgrade thesis: *Vibrational Spectra of* MoS_2 *Nanotubes* supervisor: Prof. Dr. Milan Damnjanović

Work experience

2011-present	Research Assistant Faculty of Physics, University of Vienna
05/2011	Teaching Assistant course on “Quantum foundations and quantum information theory” Faculty of Physics, University of Belgrade
2010-2011	Research Assistant Institute for Quantum Optics and Quantum Information, Austrian Academy of Sicences
2007-2010	Research Assistant Faculty of Physics, University of Vienna
2004-2007	Research Assistant Nanostructures Laboratory, Faculty of Physics, University of Belgrade
2006-2007	Teaching Assistant course on “Quantum mechanics” Faculty of Physics, University of Belgrade

Awards & Honors

2010	Harvard University Fellow, CoQuS Secondment Program supported by FWF (Austrian Science Foundation)
2007	FWF (Austrian Science Foundation) Fellow, CoQuS Doctoral Program
2005	“Ljubomir Ćirković” Award for the best Diploma Thesis for the year 2004/2005
2002	Royal Norwegian Government Award for one of the 500 best students in Serbia
2001	Ministry of Science Republic of Serbia Scholarship