Quantum Correlations: On their Detection, Applications, and Foundations

INAUGURAL-DISSERTATION

submitted in partial fulfillment of the requirements
for the degree of

Dr. rer. nat

in the Faculty of Mathematics and Natural Sciences
at the Heinrich-Heine Universität Düsseldorf

presented by

Jochen Szangolies
from Hachenburg

Düsseldorf, October 4, 2016

from the Institute for Theoretical Physics III
at the Heinrich-Heine Universität Düsseldorf

printed by permission of the
Faculty of Mathematics and Natural Sciences at the
Heinrich-Heine Universität Düsseldorf

Supervisor: Prof. Dr. Dagmar Bruß

Co-Supervisor: PD Dr. Hermann Kampermann

Date of the oral examination:

Declaration of Authorship

Ich versichere an Eides Statt, dass die Dissertation von mir selbständig und ohne unzulässige fremde Hilfe unter Beachtung der “Grundsätze zur Sicherung guter wissenschaftlicher Praxis an der Heinrich-Heine-Universität Düsseldorf" erstellt worden ist.

Signed:

Date:

"The aim of science is not to open the door to infinite wisdom, but to set a limit to infinite error."

Bertolt Brecht, *The Life of Galileo* (1939, 1994), scene 9, 74.

Abstract

In quantum mechanics, systems may exhibit correlations that go beyond those possible in classical theories. The classical correlations form a convex polytope uniquely characterized by finitely many vertices, such that every classically achievable distribution of measurement probabilities can be written as a convex combination of these vertices. Consequently, any correlation that cannot be decomposed in this way is incompatible with a classical statistical theory.

Such incompatibilities manifest themselves in different ways. One example is the Kochen-Specker theorem, which asserts that quantum correlations, in general, cannot be understood as correlations between hidden parameters whose values are independent of other, simultaneously performed measurements. The experimental verification of quantum mechanical predictions in this case is faced with the so-called problem of compatibility: in general, real measurements are never perfectly compatible, and thus, the assumptions underlying the Kochen-Specker theorem cannot be straightforwardly implemented.

To address this issue, we present a formulation of the theorem, combining it with ideas behind Leggett-Garg inequalities, that is well-defined even for imperfectly compatible observables, and which reduces to the usual formulation in the limit of perfect compatibility.

Another important aspect of quantum correlations is the phenomenon of entanglement. Many methods to detect the entanglement of arbitrary quantum states have to be specifically taylored to that state, or else, quickly become infeasibly resource intensive. We present a novel method to detect any given state's entanglement content by performing a sequence of random measurements on different subsystems, and constructing appropriate witness operators from these measurement by semidefinite programming. We furthermore show that this method scales favorably as compared to other methods, such as quantum state tomography.

Quantum correlations can be used as a resource to perform certain tasks not classically feasible, or indeed, impossible. The third main result of this thesis is to present a novel such task: the certification of lower bounds to detector efficiencies in a device-independent scenario, where neither the quantum state nor the characterization of the measurement devices is known. To do so, we develop a method to derive Bell inequalities given only the observed measurement data, such that the violation of these inequalities allows us to derive a minimum efficiency that the detectors must exceed in order to produce this violation. Furthermore, we discuss applications of this method to (device-independent) entanglement detection, nonlocality certification without a shared reference frame, and quantum key distribution.

Finally, we outline a program to recast quantum theory as a so-called principle theory, whose empirical content derives from (ideally) intuitive physical postulates. We identify the notion of an epistemic restriction, that is, a restriction on the amount of information that can be gathered about a system, as a possible foundation for this program. We then discuss how such an epistemic restriction emerges via logical constraints on the predictability of measurement outcomes due to considerations of consistency.

Zusammenfassung

Systeme in der Quantenmechanik können Korrelationen aufweisen, die über die in klassischen Theorien möglichen hinaus gehen. Die klassischen Korrelationen bilden einen konvexen Polytopen, der durch Angabe von endlich vielen Vertices eindeutig charakterisiert werden kann, so dass jede klassisch mögliche Verteilung von Messergebnissen als konvexe Summe dieser Vertices geschrieben werden kann. Jede Korrelation die nicht in solcher Weise darstellbar ist, ist somit nicht mit einer klassischen statistischen Theorie vereinbar.

Derartige Unvereinbarkeiten manifestieren sich in verschiedener Weise. Ein Beispiel ist das Kochen-Specker Theorem, welches aussagt, dass Quantenkorrelationen im Allgemeinen nicht als Korrelationen versteckter Parameter, deren Wert unabhängig von anderen, gleichzeitig durchgefḧrten Messungen ist, verstanden werden können. Die experimentelle Überprüfbarkeit der quantenmechanischen Vorhersagen in diesem Fall sieht sich mit dem sogenannten Kompatibilitätsproblem konfrontiert: im Allgemeinen sind real durchgeführte Messungen niemals absolut kompatibel, und daher können die Annahmen des Kochen-Specker Theorems nicht direkt in den experimentellen Kontext übersetzt werden.

Um dieses Problem zu lösen, schlagen wir eine Formulierung des Theorems vor, indem wir einige Ideen, die den Leggett-Garg Ungleichungen zugrunde liegen, hinzuziehen, welche auch für nicht perfekt kompatible Observablen wohldefiniert ist, und welche für den Fall perfekter Kompatibilität auf die ursprüngliche Formulierung reduziert.

Ein weiterer wichtiger Aspekt der Quantenkorrelationen ist das Phänomen der Verschränkung. Viele Methoden zur Detektion der Verschränkung beliebiger Quantenzustände müssen spezifisch auf diese Zustände abgestimmt sein, oder benötigen andernfalls unerreichbare Resourcen. Wir demonstrieren eine neue Methode zur Detektion des Verschränkungsinhaltes beliebiger Zustände, indem eine Abfolge zufälliger Messungen an verschiedenen Untersystemen durchgeführt wird, woraus dann ein semidefinites Programm einen geeigneten Verschränkungszeugen konstruiert. Weiterhin zeigen wir, dass diese Methode im Vergleich mit Methoden wie etwa Quantenzustandstomographie ein besseres Skalierungsverhalten an den Tag legt.

Quantenkorrelationen können als Resourcen für Aufgaben, die klassisch praktisch undurchführbar oder sogar unmöglich sind, dienen. Der dritte Beitrag dieser Dissertation legt eine neuartige Aufgabe aus diesem Bereich dar: die Zertifizierung unterer Schranken an Detektoreffizienzen im geräteunabhängigen Szenario, in welchem weder der Quantenzustand noch die Charakterisierung der Messapparatur bekannt ist. Dafür entwickeln wir eine Methode, um Bellungleichungen lediglich aus den Messdaten zu konstruieren, so dass die Verletzung dieser Ungleichungen es uns erlaubt, die minimale Effizienz, welche die Detektoren überschreiten müssen um diese Verletzung hervorzubringen, abzuleiten. Weiterhin diskutieren wir Anwendungen dieser Methode auf die geräteunabhängige Detektion

von Verschränkung, die Feststellung nichtlokaler Korrelationen ohne gemeinsames Bezugssystem, und die Quantenschlüsselverteilung.

Schließlich beschreiben wir ein Programm, die Quantenmechanik in die Form einer Prinzipientheorie zu bringen, deren empirischer Inhalt von (idealerweise) intuitiv einsichtigen physikalischen Postulaten ableitbar ist. Wir identifizieren den Begriff der epistemischen Einschränkung, bei der es sich um eine Einschränkung der über ein System verfügbaren Information handelt, als mögliche Grundlage für dieses Programm. Wir geben an, wie solch eine epistemische Einschränkung aus logischen Bedingungen bezüglich der Vorhersagbarkeit von Messergebnissen aus Konsistenzüberlegungen folgt.

Acknowledgements

The printed end result of a large project (such as, for example, the writing of a doctoral thesis) often starts out with a fat lie: right there, on the cover, below the title, stands only a single name. Nothing could be further from the truth.

I have benefited greatly from the kindness of heart and the generosity of spirit of those who accompanied me on my journey to this point. In compiling this thesis and the results presented therein, my first and foremost gratitude lies with Prof. Dr. Dagmar Bruß, my advisor, whose guidance and experience proved invaluable, and whose patience and resolve were instrumental in shaping the unique experience that working within her group was. I will always be thankful for being given this opportunity, and I will cherish these memories for years to come.

No less thanks are due to PD Dr. Hermann Kampermann, whom I could always count upon to help give my vague notions a more precise and sharp formulation. I am grateful to have been able to rely on his great insight and knowledge, and derive from it many new approaches and ideas.

I also wish to express heartfelt thanks to Prof. Dr. Otfried Gühne, whose encouragement got me started down this path, and likewise Dr. Matthias Kleinmann, for support and many fruitful discussions.

I have been fortunate to share this journey with some of the best fellow travelers one could wish for: my colleagues here in Düsseldorf, Dr. Silvestre Abruzzo, Dr. Alexander Streltsov, Dr. Sylvia Bratzik, Dr. Junyi Wu, Dr. Michael Epping, Felix Bischof and Timo Holz—thank you for making this the rewarding experience it was. A special thanks also to Jens Bremer and his patience in sorting out my various computer troubles. To Christian Keller and Felix Bischof I owe thanks for comments and corrections on this manuscript.

Many thanks also go out to my former colleagues at the University of Siegen. I thank Dr. Costantino Budroni, Dr. Tobias Moroder, Dr. Martin Hofmann, and Roope Uola for many valuable discussions.

Reaching this point would not have been possible without the loving support of my family. My mother, Barbara, whose love and encouragement are what got me started on this trajectory, and whose courage and strength I will always carry with me in my heart, to lean on when my own is failing. My father, Bernhard, who kept belief in me when my path got difficult, and whose support I know I can rely on blindly. My two sisters, Inka and Gisa, and their wonderful families, whom I both admire, and who have time and again through their examples provided a light to guide my own path.

Finally, I do not know what I did to deserve the kindness, love, and understanding shown to me by my wife, Constance. I thank her for being by my side, for her strength, her warmth, and her compassion. And whatever whim of fate or chance it was that led her down the aisle with me: I thank that most of all.

Contents

List of Figures

List of Tables

To my wife, Constance

Chapter 1

Introduction

In the most basic sense, a physical theory consists of a mathematical formalism, combined with a prescription connecting the elements of this formalism to observable physical quantities. Thus, classical physics in its Lagrangian formulation contains:

- The *configuration space* Σ_s, i.e. the vector space spanned by the system's (generalized) coordinates $\boldsymbol{q}$ (subject to certain kinematical constraints), representing the physical system s
- The system's *state* $\boldsymbol{q}(t)$, representing the instantaneous (at time t) values of the generalized coordinates
- The *Lagrangian* $\mathcal{L}(\boldsymbol{q}, \dot{\boldsymbol{q}}, t)$, which is related to the difference between kinetic and potential energy of the system
- The *action* $S = \int \mathrm{d}t\mathcal{L}$, whose variation according to the principle of least action $\delta S = 0$ yields the system's trajectory, that is, the explicit functional form of $\boldsymbol{q}(t)$

Using these ingredients, classical mechanics can be used to derive predictions of empirical observables using a simple algorithm: we simply compute the time evolution of the system's generalized coordinates $\boldsymbol{q}(t)$ using the principle of least action, and then use our knowledge of the system's state at all times to compute the observable quantities we are interested in.

Note that it is not necessarily the case that the formulation of a theory must be unique: for instance, in the case of classical mechanics, an equivalent formulation is given by the Hamiltonian formalism, where a system S is described in *phase space* Π_s, spanned by its generalized coordinates $\boldsymbol{q}$ and momenta $\boldsymbol{p}$, with the *Hamiltonian* $\mathcal{H}(\boldsymbol{q}, \boldsymbol{p}, t)$ corresponding to its total energy, and where the time evoltion of the generalized coordinates and momenta (i.e. the system's state) is given by Hamilton's equations,

$$\begin{aligned}\frac{\mathrm{d}\boldsymbol{q}}{\mathrm{d}t} &= \frac{\partial\mathcal{H}(\boldsymbol{q}, \boldsymbol{p}, t)}{\partial\boldsymbol{p}} \\ \frac{\mathrm{d}\boldsymbol{p}}{\mathrm{d}t} &= -\frac{\partial\mathcal{H}(\boldsymbol{q}, \boldsymbol{p}, t)}{\partial\boldsymbol{q}}.\end{aligned} \tag{1.1}$$

Now, in order for a physical theory to be *complete*, any well-defined empirically accessible quantity ought to be matched with a corresponding element of the formalism, and predictions made using this formalism ought to match empirical observation in all cases. In this sense, classical mechanics as described above fails to be complete in several respects: in the regime of high velocities $|\dot{\boldsymbol{q}}| \sim c$, where c is the speed of light, classical mechanical predictions cease to be valid due to corrections from special relativity; likewise, for strong gravitational fields, the general theory of relativity becomes necessary; and finally, and most importantly for the purposes of this thesis, in the regime of small action $S \sim \hbar$, where $\hbar$ is the reduced Planck's constant, quantum mechanical effects must be taken into account.

From this point of view, quantum mechanics can be viewed as a completion of classical mechanics within a domain where the latter ceases to apply. Now, the question presents itself: is quantum mechanics itself complete? Since it, like Newtonian mechanics, fails to account for the effects of large velocities and gravitational fields, it is just as incomplete in this regimes. Furthermore, while a completion of quantum mechanics for large velocities has been formulated in the form of quantum field theory, completion to the gravitational sector, that is, formulating a theory of quantum gravity, is still an outstanding problem.

However, concerns were raised early on that quantum mechanics might fail to be complete even in its stated domain of applicability. Einstein, Podolsky, and Rosen (1935) formulated an argument, now famous as the so-called 'EPR-argument' after the initials of its authors, designed to show that there exist measurable quantities that have no corresponding representative in the formalism.

The form of the argument most familiar today is due to Bohm and Aharonov (1957), considering two particles whose spin degrees of freedom are described by an entangled wave function. Since spins along orthogonal axes are described by non-commuting quantities in the formalism of quantum mechanics, there exists an uncertainty principle dictating that complete knowledge of the spin along one direction entails complete ignorance along the orthogonal direction.

Now, consider performing a spin measurement on particle I. Due to the nature of the entangled state, whatever outcome is obtained dictates that the spin of particle II must be oppositely aligned. Hence, after obtaining a spin along the positive x-direction for particle I, we know that the spin of particle II must be aligned in negative x-direction. However, by the uncertainty principle, we also must conclude that the spin along e.g. the y-direction of particle II must be absolutely unknown—that is, measurement along this axis yields a positive or negative alignment with 50% probability each.

Yet, if we had instead performed a measurement along the y-direction of particle I, we can run the same argument again: since the y-spin of particle II is perfectly determined via this measurement, it follows that the spin along the x-direction is completely undetermined, with quantum mechanics again predicting a probability of 50% to yield either value. However, if both particles are sufficiently far removed from one another (far enough that no signal travelling at c could traverse their distance during the time the experiment takes), there ought to be no influence between the particles. But then, how does the second particle 'know' whether to have an exactly determined spin along the x- or y-direction?

From this apparent paradox, EPR concluded that, there being no mechanism to influence the spin orientation of particle II, there must be a definite fact of the matter regarding this orientation at all times, and hence, since quantum mechanics cannot predict this direction in all cases, the theory must be incomplete—there exists an observable quantity that does not have a representative within the formalism.

The argument sparked a great amount of controversy, most notably due to Bohr (1935), who used the notion of complementarity to argue that quantum mechanics should be considered a complete theory (within its domain), after all. It was not until three decades later that Bell, in a seminal paper, showed that the EPR-requirements of non-interaction of spacelike separated systems and simultaneous values for conjugate observables are, in fact, jointly irreconcilable with the predictions of quantum mechanics (Bell 1964). Experimental investigations due to Freedman and Clauser (1972), the groups of Aspect (Aspect, Dalibard, and Roger 1982; Aspect, Grangier, and Roger 1981, 1982) and Zeilinger (Weihs et al. 1998) have provided strong evidence favoring the quantum mechanical predictions. However, only recently has it become possible to perform a test of Bell's predictions free from certain loopholes (Giustina et al. 2015; Hensen et al. 2015; Shalm et al. 2015).

A main motivation behind the suspicion of quantum mechanics' incompleteness was the fact that the theory only yields probabilistic predictions in the general case. In classical meachanics, such a situation always signals an incompleteness regarding the knowledge of a given physical system, and given the requisite additional knowledge, deterministic predictions are in principle possible for any given system. But in quantum mechanics, due to the uncertainty principle, such additional knowledge is not attainable. Indeed, controversy regarding quantum mechanics and its interpretation continues to this day.

However, whatever else quantum mechanics may be, it is certainly an algorithm capable of producing some of the most well-confirmed predictions, making it one of the most successful physical theories available. Hence, in the following, we will take an operational approach: rather than considering contentious interpretational matters, we will try to understand quantum mechanics simply as a means of generating experimentally verifiable predictions. To this end, in the following section, we will introduce the framework of generalized probabilistic theories (GPTs), which proposes a set of reasonable constraints a physical theory aimed at (probabilistically) predicting measurement outcomes should fulfill. Since this turns out rather broad, afterwards, we will narrow our scope, locating quantum mechanics within this class of theories, and provide a brief introduction of its formalism.

1.1 Generalized Probabilistic Theories

The framework of generalized probabilistic theories arose out of the attempt to understand quantum theory in operational terms. The roots of this view can be traced back to pioneering works by Mackey (1963), Ludwig (1983), and Kraus et al. (1983) (see also the review (Janotta and Hinrichsen 2014)). Instead of focusing on the theory's interpretation, it marks a shift in perspective towards considering its empirical predictions, as well as allowed operations.

In the following, we will introduce the GPT-framework first on the example of single systems, and then move on to consider the case of composite systems, and consequently, of possible correlations.

1.1.1 Single Systems

In the setting of generalized probabilistic theories, a physical system is considered to be a 'black box', which can receive inputs and, based on these inputs, produces certain outcomes.

Commonly, one requires that these black box systems can be manipulated in three distinct ways: via preparations, transformations, and measurements. However, since any manipulation can be either thought of as part of the preparation process, or a measurement, it largely suffices to think exclusively about preparations and measurements.

The role of a preparation is, as the name implies, to prepare a physical system in a given (although not necessarily known) state; that is, a preparation fixes a system's disposition to react to certain inputs (due to the settings of a measurement apparatus) in certain ways. Measurement, then, interrogates the system, producing certain outcomes according to its setting. In the GPT context, these outcomes are usually referred to as *effects*.

In principle, the output of a measurement system may be either digital, yielding a finite number of distinct values, or analog. However, due to unavoidable inaccuracies in e.g. reading a value off of a scale, it is sufficient here to restrict ourselves to a finite number of outcomes. Thus, any measurement is associated with a finite number of effects, albeit different measurements can share some of the same effects.

This allows us now to introduce the concept of a *state* in the GPT framework: a state is simply the set of probabilities assigned to all effects. Thus, any two systems that assign the same probabilities to all effects are in the same state—this encapsulates the operational character of the framework. In general, this list of probabilities might well be infinite. To circumvent this, one postulates the existence of a finite number of *fiducial effects*, which suffice to specify the state uniquely.

Consider thus the set $\{M_i\}$ of k possible (fiducial) measurements, each of which has l_i possible outcomes, leading to the set $\{i|M_j\}$ of all possible effects. A state is then the list of probabilities assigned to these effects, given a certain preparation procedure P, i.e.

$$\omega_P = \begin{pmatrix} \mathrm{Pr}(1|M_1, P) \\ \mathrm{Pr}(2|M_1, P) \\ \vdots \\ \mathrm{Pr}(l_1|M_1, P) \\ \vdots \\ \mathrm{Pr}(1|M_2, P) \\ \vdots \\ \mathrm{Pr}(l_k|M_k, P) \end{pmatrix}. \tag{1.2}$$

Here, $\mathrm{Pr}(i|M_j, P)$ denotes the probability of observing the ith outcome, if the jth measurement is performed following preparation procedure P.

Different preparation procedures may assign the same probabilities to all effects; in this case, the states are equivalent, and thus, any given state is an equivalence class of preparations. Furthermore, we may consider the case of a preparation device probabilistically performing different preparations P and P'. Then, for a given measurement M_j, we will obtain the ith outcome with probability $p\mathrm{Pr}(i|M_j, P) + (1-p)\mathrm{Pr}(i|M_j, P')$, if the probability for preparation procedure P is p. Consequently, any convex combination of states must again be a state, and thus, the *state space* Ω must be convex. Any state ω that can be written as a convex combination of other states, i.e. in the form

$$\omega = \sum_i \lambda_i \omega_i \tag{1.3}$$

with $0 < \lambda_i \leq 1$ and $\sum_i \lambda_i = 1$ is called *mixed*; consequently, states that have no convex decomposition are called *pure*.

By means of example, let us look at the classical bit, or cbit, and the generalized bit, or gbit for short. For the cbit, there exists a single measurement M with two outcomes 1 and 0. Its state is completely specified by the two outcome probabilities:

$$\omega_c = \begin{pmatrix} \mathrm{Pr}(0|M) \\ \mathrm{Pr}(1|M) \end{pmatrix}, \tag{1.4}$$

with $\mathrm{Pr}(0|M) + \mathrm{Pr}(1|M) = 1$.

The gbit is a system for which there exist two measurement devices M_x and M_y, each of which has two outcomes, ↑ and ↓. Thus, the state of the gbit is given by

$$\omega_g = \begin{pmatrix} \mathrm{Pr}(\uparrow|M_x) \\ \mathrm{Pr}(\downarrow|M_x) \\ \mathrm{Pr}(\uparrow|M_y) \\ \mathrm{Pr}(\downarrow|M_y) \end{pmatrix}. \tag{1.5}$$

Normalization enforces that $\mathrm{Pr}(\uparrow|M_x) + \mathrm{Pr}(\downarrow|M_x) = \mathrm{Pr}(\uparrow|M_y) + \mathrm{Pr}(\downarrow|M_y) = 1$. Hence, the state space of the gbit is the unit square. Fig. 1.1 shows the state spaces of the cbit and gbit.

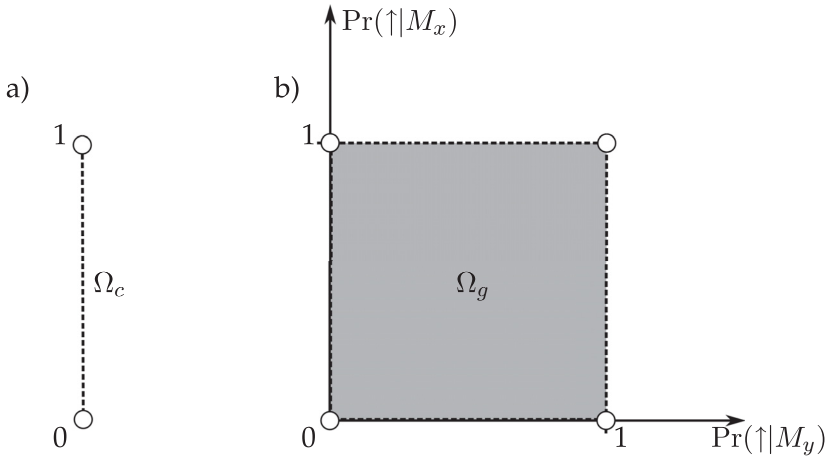


FIGURE 1.1: a) State space of the cbit, with pure states highlighted by white circles. b) State space of the gbit, pure states again highlighted by white circles.

We have seen that states ω in a GPT form a convex subset Ω of a vector space V. Now, we can model effects as linear functionals $e : V \to [0,1]$ (elements of the dual space V^*) which associate a real number in the interval $[0,1]$ to every state $\omega \in \Omega$. We identify this number with the probability of obtaining a given outcome, i.e.

$$\Pr(i|M) = e_i(\omega). \tag{1.6}$$

Then, linearity follows from the following argument: suppose we have a preparation procedure that prepares each of the states ω_i with probability p_i, that is, prepares the state $\omega = \sum_i p_i\omega_i$. Then, we will observe the j-th outcome with probability $\Pr(j|M) = e_j(\omega) = e_j(\sum_i p_i\omega_i)$.

However, after the preparation, we have the i-th state with probability p_i—that is, with probability p_1, we have the state ω_1, with probability p_2 the state ω_2, and so on. Now, if the state is ω_1, then the probability of obtaining the j-th outcome is $\Pr(j|M) = e_j(\omega_1)$; likewise, if the state is ω_2, then the probability will be $\Pr(j|M) = e_j(\omega_2)$, and so on.

Each of these cases happens now with probability p_i. Thus, since both are equivalent descriptions of the same situation, we must have:

$$e_j\left(\sum_i p_i\omega_i\right) = \sum_i p_i e_j(\omega_i) \tag{1.7}$$

for all effects e_j.

For an l-outcome measurement M, there then exist l effects $\{e_1, \dots, e_l\}$ such that

$$\sum_{i=1}^{l} e_i(\omega) = 1 \tag{1.8}$$

for all ω.

Both states and effects may be *unreliable*: a preparation procedure may fail to produce a system, or an experiment may yield no outcome, even though a system is present. If the preparation procedure for a system in the state ω succeeds with probability p (and consequently, fails with probability $1-p$), then, for instance, an effect e_i that yields outcome i on the system in state ω with probability 1, will now yield that outcome with probability p, instead. Conversely, if instead we have an unreliable effect e_i that produces the correct outcome with probability q, we will observe the outcome i with a probability of $qe_i(\omega)$.

Thus, we can represent unreliable states as subnormalized vectors $p\omega \in V$, and unreliable effects likewise as $qe \in V^*$. This extends the convex set of states Ω in V to the (truncated) *convex cone*

$$V_+ = \{p\omega \in V | 0 \leq p \leq 1, \omega \in \Omega\}. \tag{1.9}$$

Conversely, effects can be considered to be elements of the *dual cone*

$$V_+^* = \{qe \in V^* | 0 \leq q \leq 1,\, e(\omega) \geq 0\, \forall \omega \in \Omega\}. \tag{1.10}$$

Finally, there exists a special effect, the so-called *unit effect* u, which is defined by $u(\omega) = 1$ for all $\omega \in \Omega$; that is, this effect can be viewed as merely determining whether a system is present, and thus, the preparation procedure was successful. For any given collection of effects e_i of an l-outcome measurement, we have that

$$\sum_{i=1}^{l} e_i = u, \tag{1.11}$$

as the sum of all possible outcome probabilities must equal one.

Since we want the effects to yield probabilities if applied to all states, we must have, for all effects e and states ω,

$$0 \leq e(\omega) \leq 1. \tag{1.12}$$

The lower bound is already obeyed by restricting the set of effects to the (positive) dual convex cone V_+^*. To implement the upper bound, we note that with any effect e, also its complement $e^\perp = u - e$ must be included in the set of effects, since $e^\perp(\omega) \geq 0$ implies $(u-e)(\omega) \geq 0$, and hence, $e(\omega) \leq 1$ for all ω. Thus, the allowed set of effects E can be considered as the intersection of the convex cone V_+^* with the set of complement effects, i.e.

$$E = V_+^* \cap (u - V_+^*). \tag{1.13}$$

In general, not all effects may be jointly measurable. Here, *joint measurability* means the following. Consider two effects e_i and e_j, yielding a one-bit outcome each if applied to an arbitrary state ω. Now, for these effects to be jointly measurable means that there exists a third effect, $e_{i\wedge j}$, such that, applied to the same ω, it yields two bits with the same statistical distribution as the two bits obtained from measuring the effects e_i and e_j individually (cf. Janotta and Hinrichsen 2014).

For the full measurement, we need three additional effects $e_{i\wedge\bar{j}}$, $e_{\bar{i}\wedge j}$ and $e_{\bar{i}\wedge\bar{j}}$ such that the condition in Eq. 1.11 holds, i.e.

$$e_{i\wedge j} + e_{i\wedge\bar{j}} + e_{\bar{i}\wedge j} + e_{\bar{i}\wedge\bar{j}} = u. \tag{1.14}$$

Furthermore, the original effects must be obtainable as the mariginals of the joint measurement:

$$\begin{aligned} e_i &= e_{i\wedge j} + e_{i\wedge\bar{j}} \\ e_j &= e_{i\wedge j} + e_{\bar{i}\wedge j} \end{aligned} \tag{1.15}$$

The joint effect $e_{i\wedge j}$ can now be obtained in the following ways:

$$\begin{aligned} e_{i\wedge j} &= e_i - e_{i\wedge\bar{j}} \\ &= e_j - e_{\bar{i}\wedge j} \\ &= e_i + e_j - u + e_{\bar{i}\wedge\bar{j}} \end{aligned} \tag{1.16}$$

Thus, a joint effect exists if the intersection of sets

$$E \cap (e_i - E) \cap (e_j - E) \cap (e_i + e_j - u + E) \tag{1.17}$$

is not empty.

The machinery introduced so far suffices to describe measurements on single systems. In the following section, we will introduce the necessary tools to handle composite systems, which will then enable us to move on to our main topic, the possible correlations allowed by a given GPT. However, for completeness, we will have a short look at the allowed transformations—modeling, for instance, the possible physical evolutions of a system—below.

A transformation T is a mapping from a state space Ω_A to a state space Ω_B, $T : \Omega_A \to \Omega_B$. By an analogous argument to the one used for effects, we obtain that they must act linearly on states, that is,

$$T\left(\sum_i p_i\omega_i\right) = \sum_i p_i T(\omega_i). \tag{1.18}$$

Furthermore, we require transformations to be positive and normalization-nonincreasing, meaning that

$$e_i(T(\omega)) \geq 0 \tag{1.19}$$

and

$$\sum_{i=1}^{l} e_i(T(\omega)) \leq 1 \tag{1.20}$$

for all ω and l-outcome measurements with effects e_i.

If a transformation is invertible, that is, there exists a T^{-1} such that $TT^{-1} = \mathbb{1}$, and if T^{-1} is a transformation as well, we call the transformation *reversible*. The reversible transformations of a system form a compact Lie group. In the case of the gbit described above, this group of transformations is the dihedral group D_4, that is, the group of rotations through an angle $\frac{n\pi}{2}$, where $n \in \mathbb{N}$. In the quantum mechanical description of a d-dimensional system, this group is the group of $d \times d$ unitary matrices, $U(d)$.

1.1.2 Composite Systems

Having now compiled the necessary tools for the description of single systems in the GPT framework, we proceed to the case of composite systems and their correlations, which will be the main concern of this thesis.

Consider thus two systems A and B, whose state spaces Ω_A and Ω_B form convex subsets of vector spaces V_A and V_B, respectively. We are now looking for a construction that yields a physically reasonable definition for a combined state space Ω_{AB}, which we anticipate to be again a convex subset of a vector space V_{AB}.

To do so, we will make two physical assumptions. The first assumption is *local tomography*: essentially, we want to assume that we can learn all there is to know about a system by performing local measurements on its subsystems. Thus, suppose we have a collection of effects e^A on system A, and a collection of effects e^B on system B. Local tomography then means that for any two states ω_{AB} and ω'_{AB} of the joint system, if it holds that $e^{AB}(\omega_{AB}) = e^{AB}(\omega'_{AB})$, then $\omega_{AB} = \omega'_{AB}$. Here, we use the notation e^{AB} to denote the joint effect of a simultaneous measurement on both subsystems, and suppress the outcome indices to avoid clutter. It can be shown that this assumption mandates a tensor product structure for the theory, that is, the joint vector space is the tensor product of the subsystem vector spaces:

$$V_{AB} = V_A \otimes V_B. \tag{1.21}$$

The reason for this is that the number of parameters to determine an element of $V_A \otimes V_B$ is equal to the product of the number of parameters to determine an element of V_A and the number of parameters to determine an element of V_B (Barrett 2007).

This assumption is nontrivial: in fact, theories have been proposed in which it is violated. The most well-known such theory is the so-called *real-vector-space quantum theory* (Hardy and Wootters 2012), where the complex Hilbert space of standard quantum mechanics is replaced by a vector space over the real numbers, and where in general measurements on pairs of subsystems are necessary to fully determine the state of a system.

The second physical constraint we require is the *no-signalling principle*. This principle intuitively demands that there is no instantaneous action at a distance between two systems, and as such, is motivated by the fact that in special relativity, all influences propagate with a speed that is bounded by that of light (in vacuum, i.e. c).

The framework as introduced so far has no notions of space and time, and hence, no concept of distance. However, we can implement this principle in an operational way by demanding that for each system, there must exist local states $\omega_A \in \Omega_A$ and $\omega_B \in \Omega_B$ that completely suffice to determine the local measurement statistics. Thus, for any l-outcome measurement M_A on subsystem A and m-outcome measurement M_B on subsystem B, we require that

$$\Pr(i|M_A, M_B) = \Pr(i|M_A) \tag{1.22}$$

$$\Pr(j|M_A, M_B) = \Pr(j|M_B), \tag{1.23}$$

where $i \in \{0, \ldots, l\}$ ($j \in \{0, \ldots, m\}$) enumerates the measurement outcomes of M_A (M_B). Thus, the choice of measurement on A (B) does not influence the probability of obtaining the outcome j (i) on B (A).

We start with the simplest scenario: independent, locally prepared systems A and B in the states ω_A and ω_B respectively. In this case, for any joint measurement, we expect that the probabilities factorize, that is

$$\Pr(i, j|M_A, M_B) = \Pr(i|M_A) \cdot \Pr(j|M_B), \tag{1.24}$$

and hence, if the joint state of the system is ω_{AB},

$$e_{ij}^{AB}(\omega_{AB}) = e_i^A(\omega_A) e_j^B(\omega_B) \tag{1.25}$$

This situation can be represented using the tensor product $\otimes$, yielding $\omega_{AB} = \omega_A \otimes \omega_B$ and $e_{ij}^{AB} = e_i^A \otimes e_j^B$.

A natural generalization is to allow arbitrary convex combinations of states of the above form. This corresponds to the situation in which the two parties, A and B, produce a certain joint state $\omega_A^i \otimes \omega_B^j$ with a given probability p_{ij}—that is, it allows us to include (classical) correlations into our framework. Here, we speak of a correlation whenever knowledge of the state of one party increases the knowledge of the state of the other party—in the extreme case, if e.g. either the joint state $\omega_A^1 \otimes \omega_B^1$ or $\omega_A^2 \otimes \omega_B^2$, knowledge of A's state determines B's state completely, and we have perfect correlation.

Such a state can then always be written as

$$\omega_{AB} = \sum_{ij} p_{ij} \omega_A^i \otimes \omega_B^j. \tag{1.26}$$

This now allows us to find a first definition for the states of the joint system AB. This definition is given by the *minimal tensor product*, $\otimes_{\min}$, and yields

$$V_+^A \otimes_{\min} V_+^B = \left\{ \omega_{AB} = \sum_{ij} p_{ij} \omega_A^i \otimes \omega_B^j | \omega_A^i \in V_+^A, \omega_B^i \in V_+^B, p_{ij} \geq 0 \right\} \tag{1.27}$$

$$V_+^{A*} \otimes_{\min} V_+^{B*} = \left\{ e^{AB} = \sum_{ij} q_{ij} e_i^A \otimes e_j^B | e_i^A \in V_+^{A*}, e_i^B \in V_+^{B*}, q_{ij} \geq 0 \right\}. \tag{1.28}$$

However, this is not the only possible way to generate a joint state space; and in fact, this definition would be inadequate to capture the phenomena of quantum mechanics, as there exist (entangled) states that cannot be written in the form of Eq. 1.26.

Thus, we need to allow different definitions of the joint state space, if we are to capture the phenomena of quantum mechanics. A feature of the above definition is that if system A has k extremal (pure) states, and system B has l such states, the joint system will have $k \cdot l$ extremal states; hence, to include states that cannot be written as in Eq. 1.26, we need to add further extremal states to the state space (while obeying the physical constraints of local tomography and no-signalling).

There is a natural limit to this procedure of adding states to the tensor product: it can be shown that there exists a trade-off between the additional states available (as compared to the minimal tensor product) in the joint system, and the measurements that can be performed on it (Short and Barrett 2010). In fact, the maximum number of additional states is attained, if the set of joint effects is minimal (and vice versa); thus, we define the *maximal tensor product* as the set of all states which give nonnegative results for all effects contained in the minimal tensor product:

$$V_+^A \otimes_{\max} V_+^B = \{\omega_{AB} \in V^A \otimes V^B | e^A \otimes e^B(\omega_{AB}) \geq 0 \, \forall e^A \in V^{A*}, e^B \in V^{B*}\} \tag{1.29}$$

The requirement of nonnegativity in the above ensures that there exist local reduced states ω_A and ω_B that reproduce the local measurement statistics independently of the actions of the other party, and thus, enforces the no-signalling condition.

The minmal and maximal tensor products give a range of possible joint state spaces, and thus, a range of theories. A priori, each of these could yield a physical theory compatible with the desiderata formulated so far; however, in practice, only one of them can be realized in nature. It is therefore interesting to mention that the case of quantum mechanics corresponds, in a sense, to the most symmetrical one: the quantum tensor product sits right 'in between' the minimal and maximal tensor products in the sense that there exists a symmetry between entangled states and effects—the convex cones of states and effects can both be identified with the set of positive semidefinite operators on Hilbert space (Janotta, Gogolin, et al. 2011).

We have now assembled the requisite toolkit to treat composite systems and their correlations within the framework of generalized probabilistic theories. In the next section, we will bring the formalism to bear, by developing from it the notions of standard quantum mechanics.

1.2 Quantum Mechanics

Quantum mechanics can be viewed as an example of the generalized probabilistic theories discussed in the previous section. Thus, we now have to specialize the general framework presented there to the more familiar elements comprising the quantum mechanical description of nature—that is, we have to find the appropriate mathematical representations of quantum states, effects, and transformations, as well as choose a tensor product structure describing system composition.

We will follow the same basic structure as in the previous section, and start out with a description of single systems, which we then generalize to allow for system composition.

1.2.1 Single Systems

The quantum description of a system A proceeds as follows. First, states are elements of the vector space of Hermitian (self-adjoint) $n \times n$ matrices over $\mathbb{C}$, that is, matrices $M \in \mathbb{C}^{n\times n}$ such that $M^\dagger = M$, where the operation † refers to Hermitian conjugation. This vector space can be understood as the space of bounded linear operators over a (complex, and for the purposes of this thesis, finite-dimensional) Hilbert space $\mathcal{H}_A$, denoted $\mathcal{B}(\mathcal{H}_A)$. Within this space, *unnormalized* states are elements of the convex cone of positive semidefinite operators, i.e. operators ρ such that for all $|\psi\rangle \in \mathcal{H}_A$, it holds that

$$\langle\psi|\,\rho\,|\psi\rangle \geq 0, \tag{1.30}$$

where $\langle\psi| = |\psi\rangle^\dagger$. For brevity, we will denote this as $\rho \geq 0$. Adding the normalization condition $\mathrm{tr}\,(\rho) = 1$, we obtain the quantum state space

$$\Omega = \{\rho \in \mathcal{B}(\mathcal{H}_A)|\rho \geq 0, \mathrm{tr}\,(\rho) = 1\}. \tag{1.31}$$

A normalized, positive semidefinite operator ρ is called a *density operator* or, in particular when the underlying Hilbert space is finite dimensional (as it will be for most purposes in this thesis), *density matrix*.

The space $\mathcal{B}(\mathcal{H}_A)$ comes equipped with an inner product $\langle A, B\rangle = \mathrm{tr}\left(A^\dagger B\right)$. As any (normalized) state must have inner product 1 with the unit effect, it is simply the identity $\mathbb{1}$. Thus, quantum mechanically possible effects E_i associated to an l-outcome measurement must satisfy

$$\sum_{i=1}^{l} E_i = \mathbb{1}. \tag{1.32}$$

Then, the probability of observing the outcome i is simply given by the inner product of E_i and the state ρ:

$$\Pr(i|\rho) = \mathrm{tr}\left(E_i^\dagger \rho\right) \equiv \mathrm{tr}\left(E_i \rho\right), \tag{1.33}$$

where we have used that $E_i^\dagger = E_i$. This implies that $E_i \geq 0$, as probabilities must be positive. This encapsulates the most general description of measurement in quantum theory, the so-called *positive operator valued measures*, or POVMs.

A special important case are the so-called *projection-valued measures*, or PVMs, where effects Π_i obey the additional condition that

$$\Pi_i \Pi_j = \delta_{ij} \Pi_j. \tag{1.34}$$

A projection $\Pi_{|\psi\rangle}$ onto a vector $|\psi\rangle \in \mathcal{H}_A$ is a positive semidefinite operator such that

$$\Pi_{|\psi\rangle}^2 = \Pi_{|\psi\rangle}, \tag{1.35}$$

with $\Pi_{|\psi\rangle} |\psi\rangle = |\psi\rangle$. Using the scalar product $\langle\phi|\psi\rangle = \langle\phi| \cdot |\psi\rangle$ on $\mathcal{H}_A$, we see that we can write

$$\Pi_{|\psi\rangle} = |\psi\rangle\!\langle\psi|, \tag{1.36}$$

since

$$|\psi\rangle\!\langle\psi|^2 = |\psi\rangle\!\langle\psi|, \tag{1.37}$$

and

$$|\psi\rangle\!\langle\psi| \, |\psi\rangle = |\psi\rangle \underbrace{\langle\psi|\psi\rangle}_{=1} = |\psi\rangle. \tag{1.38}$$

We can then diagonalize any density matrix ρ, yielding

$$\rho = \sum_i \lambda_i \, |i\rangle\!\langle i|, \tag{1.39}$$

where $\{|i\rangle\}$ is a basis on $\mathcal{H}_A$. Let now $\{\lambda_i^\downarrow\}$ denote the collection of eigenvalues λ_i in descending order. Then, any density matrix with $\mathrm{rank}(\rho) \geq 2$ can be written as a mixture

$$\rho = \lambda_1^\downarrow \underbrace{|1\rangle\!\langle 1|}_{\rho_1} + (1-\lambda_1^\downarrow) \underbrace{\left(\sum_i \frac{\lambda_i^\downarrow}{1-\lambda_1^\downarrow} |i\rangle\!\langle i|\right)}_{\rho_2}. \tag{1.40}$$

Hence, all pure density matrices are rank-one projections.

Thus, for any pure density matrix ρ there exists a $|\psi\rangle \in \mathcal{H}_A$ such that ρ can be written as

$$\rho = |\psi\rangle\!\langle\psi|. \tag{1.41}$$

This means that pure states are in one-to-one correspondence with (normalized, $\langle\psi|\psi\rangle = 1$) vectors $|\psi\rangle$ in the Hilbert space $\mathcal{H}_A$, and consequently, such vectors can alternatively be used for their representation. However, this representation is not unique: the transformation

$$|\psi\rangle \to |\psi'\rangle = e^{i\phi} |\psi\rangle, \tag{1.42}$$

with $\phi \in [0, 2\pi]$, leaves the resulting density matrix invariant:

$$\rho = e^{i\phi} |\psi\rangle\langle\psi| e^{-i\phi} = |\psi\rangle\langle\psi| \,. \tag{1.43}$$

Hence, a pure state is given by the equivalence class (or *ray*) of vectors $|\psi\rangle \in \mathcal{H}_A$ that differ only by the above global phase transformation.

For an l-outcome measurement whose associated effects are given by the projection operators Π_i, we can define a (Hermitian) *measurement operator O* as

$$O = \sum_{i=1}^{l} o_i \Pi_i, \tag{1.44}$$

where o_i is the outcome associated with the projector Π_i. From this definition, we immediately see that the inner product of such an operator with a density matrix ρ yields the expectation value of the associated measurement, given the state ρ:

$$\begin{aligned}
\langle O, \rho \rangle &= \mathrm{tr}\left(O\rho\right) && (1.45)\\
&= \sum_{i=1}^{l} o_i \mathrm{tr}\left(\Pi_i \rho\right) && (1.46)\\
&= \sum_{i=1}^{l} o_i \mathrm{Pr}\left(o_i | \rho\right) && (1.47)\\
&\equiv \langle O \rangle && (1.48)
\end{aligned}$$

If the system is in a state $|\psi_i\rangle$ such that $\Pi_i |\psi_i\rangle = |\psi_i\rangle$ for some i, and consequently, $\Pi_j |\psi_i\rangle = 0$ for $i \neq j$, then $\langle O \rangle = o_i$, i.e. we will see the outcome o_i with certainty. Hence, the eigenvalues of O yield the possible measurement outcomes. Furthermore, we want measurements to be repeatable: that is, an immediate re-measurement of the same observable should yield the same outcome. Thus, it follows that if measuring O yielded outcome o_i, in order to yield the same outcome again, after the first measurement, the system must be in an eigenstate $|\psi_i\rangle$ of outcome o_i, even if it was in an arbitrary state before the first measurement. This is sometimes called the *projection postulate*.

As we have seen, effects may fail to be jointly observable in GPTs. In quantum mechanics, this occurs whenever two measurement operators O_1 and O_2 fail to have common eigenstates. In this case, for any $|\psi\rangle$, we have

$$O_1 O_2 |\psi\rangle \neq O_2 O_1 |\psi\rangle \,, \tag{1.49}$$

and consequently,

$$[O_1, O_2] = O_1 O_2 - O_2 O_1 \neq 0, \tag{1.50}$$

where the object $[O_1, O_2]$ defined by this equation is called the *commutator* of O_1 and O_2. This implies that the value of O_1 and O_2 cannot be known simultaneously to arbitrary precision, as after the measurement of O_1, the system fails to be in an eigenstate of O_2, and vice versa. The uncertainties

$$\Delta O_i = \sqrt{\langle O_i^2 \rangle - \langle O_i \rangle^2} \tag{1.51}$$

are connected by the *Schrödinger-Robertson uncertainty relation* (Robertson 1929)

$$\Delta O_1 \Delta O_2 = \frac{|\langle [O_1, O_2] \rangle|}{2}. \tag{1.52}$$

Jointly measurable observables are often called *compatible*.

In this formulation, joint measurability is thus synonymous with commutativity. This is, however, only the case for measurement operators of the form of Eq. 1.44, defined in terms of projections. For the more general case of POVMs, this equivalence breaks down: for two POVM-elements E_i and E_j, it may be that $[E_i, E_j] \neq 0$, yet still, there may exists a joint effect E_{ij} such that the effects E_i and E_j can be obtained as its marginals (Lahti and Pulmannová 1997). However, in the following, we will generally understand observables as being of the form of Eq. 1.44, and thus, use commutativity and joint measurability interchangeably.

Finally, the allowed transformations of quantum theory can be derived by requiring that they preserve the norm, and hence, the scalar product on $\mathcal{H}_A$, ensuring that valid states are taken to valid states. Thus, for a transformation $|\psi\rangle \to |\psi'\rangle = U|\psi\rangle$, we have

$$\langle \psi | \psi \rangle \overset{!}{=} \langle \psi' | \psi' \rangle \tag{1.53}$$

$$= \langle \psi | U^\dagger U | \psi \rangle , \tag{1.54}$$

and hence, $U^\dagger U = \mathbb{1} = UU^\dagger$. Matrices obeying this condition are called *unitary*.

As in the preceding section, it is instructive to look at an example of a quantum mechanical system. The simplest nontrivial such system is the qubit. Its Hilbert space is two-dimensional, and consequently, pure states can be written in the form

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle , \tag{1.55}$$

where α and β are complex parameters fulfilling the normalization condition $|\alpha|^2 + |\beta|^2 = 1$, and $\{|0\rangle, |1\rangle\}$ is an orthonormal basis, the so-called *computational basis*, of the qubit Hilbert space.

The arbitrary overall phase implies that we can choose α real, and write the general qubit state as

$$|\psi\rangle = z|0\rangle + (x + iy)|1\rangle , \tag{1.56}$$

with the real parameters x, y and z now fulfilling the normalization condition $x^2 + y^2 + z^2 = 1$, which parametrizes a 2-sphere. Thus, any pure qubit state lies on the surface of a three dimensional ball, the so-called *Bloch sphere*. In spherical coordinates, we can then write this state as

$$|\psi\rangle = \cos\left(\frac{\vartheta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\vartheta}{2}\right)|1\rangle , \tag{1.57}$$

where the half-angle ensures that orthogonal states get mapped to antipodal points on the sphere. The Bloch sphere is shown in Fig. 1.2.

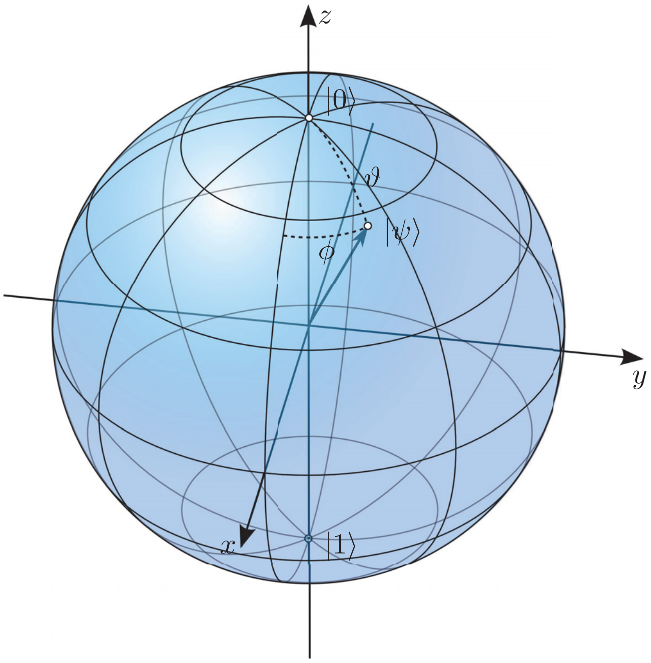


FIGURE 1.2: The bloch sphere of single qubit states. Indicated are the computational basis states $|0\rangle$ and $|1\rangle$, as well as an arbitrary state $|\psi\rangle$ with azimuth ϑ and phase ϕ.

This picture can be extended to mixed states, as well. Any state ρ can be written in the form

$$\rho = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \tag{1.58}$$

$$= \frac{1}{2}(\mathbb{1} + x\sigma_x + y\sigma_y + z\sigma_z) \tag{1.59}$$

$$\equiv \frac{1}{2}(\mathbb{1} + \boldsymbol{s}\cdot\boldsymbol{\sigma}), \tag{1.60}$$

where we have introduced the *Pauli matrices*

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{1.61}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{1.62}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1.63}$$

the *Pauli vector* $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)^T$, and finally, the Bloch vector $\boldsymbol{s} = (x, y, z)^T$. In the bloch picture, the mixed states are then those with $|\boldsymbol{s}| < 1$, that is, they form the interior of the Bloch ball.

Measurements can be represented on the Bloch sphere by the projectors

$$\Pi_\pm = \frac{\mathbb{1} \pm \boldsymbol{a}\cdot\boldsymbol{\sigma}}{2}, \tag{1.64}$$

whose eigenstates corresponding to the eigenvalues ± 1 are given by the states with Bloch vectors $\pm\boldsymbol{a}$.

1.2.2 Composite Systems

To introduce the tensor product structure of composite systems in quantum mechanics, it is simplest to start with pure states of two systems A and B, respectively their Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$.

Let thus $\{|a_i\rangle\}$ be a basis of $\mathcal{H}_A$, and $\{|b_j\rangle\}$ a basis of $\mathcal{H}_B$. Then, a basis of the composite space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ is given by $\{|a_i\rangle \otimes |b_j\rangle\}$. For brevity, we will often write $|a_i b_j\rangle$ for tensor products of vectors, whenever there is no danger of confusion. If $\mathcal{H}_A$ has dimension d_A (and thus, d_A elements in its basis), and $\mathcal{H}_B$ has dimension d_B, this means that the dimension of $\mathcal{H}_{AB}$ must be $d_A \cdot d_B$.

As before, the simplest case of independently locally prepared systems in states $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$ simply is the *product state*

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \equiv |\psi_A \psi_B\rangle\,. \tag{1.65}$$

However, the most general element of $\mathcal{H}_{AB}$ can be written as

$$|\psi_{AB}\rangle = \sum_{ij} c_{ij}\,|a_i b_j\rangle\,, \tag{1.66}$$

where $c_{ij} \in \mathbb{C}$, $\sum_{ij} |c_{ij}|^2 = 1$.

This state in general cannot be brought into the form of Eq. 1.65, and in that case, it is not an element of the minimal tensor product. We call such states *entangled*. A famous example of entangled states for the case of a two-qubit system are the *Bell states* (Bell 1964)

$$\begin{aligned} |\Phi^+\rangle &= \tfrac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \quad |\Psi^+\rangle = \tfrac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \\ |\Phi^-\rangle &= \tfrac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \quad |\Psi^-\rangle = \tfrac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right). \end{aligned} \tag{1.67}$$

The above notions readily generalize to mixed states. As before, elements of the minimal tensor product, that is, elements of the form

$$\rho_{AB} = \sum_{ij} p_{ij} \rho_A^i \otimes \rho_B^j \tag{1.68}$$

with $p_{ij} \geq 0$, $\sum_{ij} p_{ij} = 1$ are called separable; they can be interpreted as describing a preparation that yields either of the product states $\rho_A^i \otimes \rho_B^j$ with probability p_{ij}. Conversely, the general density matrices describing a joint state of the systems A and B,

$$\rho_{AB} = \sum_i p_i\,|\psi_i\rangle\!\langle\psi_i| \tag{1.69}$$

where $|\psi_i\rangle \in \mathcal{H}_{AB}$, that cannot be brought into the form of Eq. 1.68 are called entangled.

Finally, the density matrix of the joint system ρ_{AB} allows the construction of local states ρ_A and ρ_B such that these states yield the same statistics for local measurements as the joint state, independently of manipulations on the other system, as required by the no-signalling principle. The construction of these local states uses the *partial trace* operation. For a state

$\rho = \sum_{ijkl} c_{ijkl} \, |a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l|$, the partial trace over subsystem B is defined as the linear operation

$$\mathrm{tr}_B \left(\sum_{ijkl} c_{ijkl} \, |a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l| \right) = \sum_{ijklm} c_{ijkl} \, |a_i\rangle\langle a_j| \, \langle b_m|b_k\rangle \langle b_l|b_m\rangle. \quad (1.70)$$

The definition for the partial trace over subsystem A is analogous.

Chapter 2

Quantum Correlations

A central topic of this thesis is the study of correlations. Intuitively, a correlation between two random variables X and Y means that knowledge of the value of one variable increases the probability of correctly guessing the value of the other. Thus, formally, the two variables are independent if

$$\begin{aligned} \mathrm{Pr}(X^x|Y^y) &= \mathrm{Pr}(X^x) \\ \mathrm{Pr}(Y^y|X^x) &= \mathrm{Pr}(Y^y), \end{aligned} \tag{2.1}$$

where X^x (Y^y) denotes the value of X being x (Y being y), and $\mathrm{Pr}(X^x|Y^y)$ is the conditional probability that X yields the value x, given that Y yields the value y. This implies that the joint probability distribution is the product of the individual probabilities:

$$\mathrm{Pr}(X^x, Y^y) = \mathrm{Pr}(X^x) \cdot \mathrm{Pr}(Y^y). \tag{2.2}$$

A suitable measure for correlations then is any expression that measures the deviation of the joint distribution from a product form. One such measure that will be used throughout this thesis is the *correlator* $\langle XY \rangle$, defined as

$$\langle XY \rangle = \sum_{x,y} xy\mathrm{Pr}\left(X^x Y^y\right). \tag{2.3}$$

Whenever X and Y are independent, the correlator becomes merely the product of their average values:

$$\begin{aligned} \langle XY \rangle &= \sum_{x,y} xy\mathrm{Pr}\left(X^x\right)\mathrm{Pr}\left(Y^y\right) \\ &= \sum_{x} x\mathrm{Pr}\left(X^x\right) \sum_{y} y\mathrm{Pr}\left(Y^y\right) \\ &\equiv \langle X \rangle \langle Y \rangle. \end{aligned} \tag{2.4}$$

Thus, any deviation from this value indicates a nonvanishing correlation of X and Y.

An important factor in assessing the correlations possible in generalized probabilistic theories is the fact that certain effects may not be jointly measurable. Thus, for two random variables describing measurements performed on a physical system, it might be the case that no joint probability distribution exists. In fact, as we will see in the following section, the requirement of joint measurability implies certain constraints on the correlations available in a theory, and serves to delineate the classical correlations from those of post-classical theories like, for instance, quantum mechanics.

In order to properly compare correlations possible in various theories, we will first introduce a standard setting, which we will then analyze from the points of view of classical probability, quantum theory, and more general probabilistic theories. This setting is the one proposed by Clauser, Horne, Shimony, and Holt (CHSH) (Clauser, Horne, et al. 1969): two parties, Alice (A) and Bob (B) each perform two dichotomic ±1-valued measurements, $\{A_1, A_2\}$ and $\{B_1, B_2\}$ respectively, on two subsystems A and B of a joint system AB. The setup is schematically depicted in Fig. 2.1.

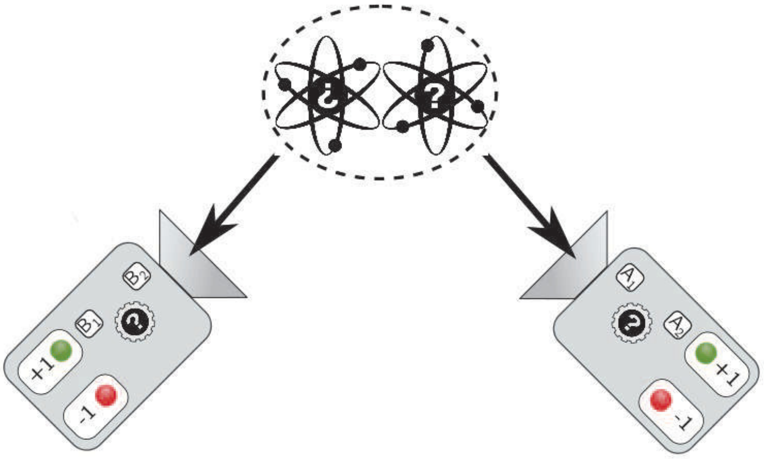


FIGURE 2.1: Schematic depiction of the CHSH setting used to analyze possible correlations. Two parties, A and B, can choose between two possible ±1-valued measurements to investigate the correlations between their subsystems.

In the following sections, we will analyze this setup, and find bounds on the allowed values for (linear combinations of) the correlators $\langle A_i B_j \rangle$ that depend on the possible correlations between the subsystems—classical, quantum, and post-quantum (i.e. given by a non-quantum GPT). After this analysis, we introduce three famous 'no-go' theorems due to Bell (1964), Kochen and Specker (1969), and Leggett and Garg (1985), concerning the impossibility of replicating correlations of quantum theory within a classical theory obeying certain empirically motivated restrictions.

2.1 Correlations: Classical, Quantum, and Beyond

Different physical theories may differ widely in the allowed correlations between subsystems. Fundamentally, this is an assertion about the probability distributions that have a model—in terms of appropriate states and effects—within the theory. As we will see, classical correlations can be defined by the requirement that all probability distributions that can be obtained within a given experimental setting must be obtainable as the marginals of a joint probability distribution. This is due to the fact that, in such theories, all effects are jointly measurable.

The situation differs in theories in which this is not the case, which includes, in particular, quantum mechanics. In the following, we will first introduce the set of classically allowed correlations for a given experimental setting, and then study the novel possibilities that arise when we consider probabilistic theories in which not all effects are jointly measurable.

2.1.1 The Polytope of Classical Correlations

In classical theories, all effects are jointly measurable. This implies that there exists a well-defined joint probability distribution $\mathrm{Pr}(A_1^{a_1}, A_2^{a_2}, B_1^{b_1}, B_2^{b_2})$ for the CHSH-scenario, and that we can interprete measurements as simply revealing the value of a given observable quantity. Thus, any classical theory must assign probabilities p_i to each of the 16 possible outcomes, as shown in Table 2.1.

TABLE 2.1: The classical probability distribution must assign values to each of the possible outcome combinations in the CHSH setting.

a_1	a_2	b_1	b_2	$\mathrm{Pr}\left(A_1^{a_1}, A_2^{a_2}, B_1^{b_1}, B_2^{b_2}\right)$
$+$	$+$	$+$	$+$	p_1
$+$	$+$	$+$	$-$	p_2
$+$	$+$	$-$	$+$	p_3
$+$	$+$	$-$	$-$	p_4
$+$	$-$	$+$	$+$	p_5
$+$	$-$	$+$	$-$	p_6
$+$	$-$	$-$	$+$	p_7
$+$	$-$	$-$	$-$	p_8
$-$	$+$	$+$	$+$	p_9
$-$	$+$	$+$	$-$	p_{10}
$-$	$+$	$-$	$+$	p_{11}
$-$	$+$	$-$	$-$	p_{12}
$-$	$-$	$+$	$+$	p_{13}
$-$	$-$	$+$	$-$	p_{14}
$-$	$-$	$-$	$+$	p_{15}
$-$	$-$	$-$	$-$	p_{16}

From this assignment of values, all other probabilities can be obtained by marginalization, e.g. $\mathrm{Pr}\left(A_1^+\right) = \sum_{i=1}^{8} p_i$, or, more importantly in the following discussion, $\mathrm{Pr}\left(A_1^+, B_1^+\right) = p_1 + p_2 + p_5 + p_6$.

Now, let us consider the CHSH-combination of correlators (Clauser, Horne, et al. 1969):

$$\langle \mathcal{C}_{\mathrm{CHSH}} \rangle = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle. \tag{2.5}$$

This can be rewritten using the values from Table 2.1 in two ways (Cereceda 2000):

$$\begin{aligned} \langle \mathcal{C}_{\mathrm{CHSH}} \rangle &= 2 - 4(p_4 + p_5 + p_6 + p_8 + p_9 + p_{11} + p_{12} + p_{13}) \\ &= 4(p_1 + p_2 + p_3 + p_7 + p_{10} + p_{14} + p_{15} + p_{16}) - 2 \end{aligned} \tag{2.6}$$

Due to the normalization condition $\sum_i p_i = 1$, the terms in parentheses are bounded between 0 and 1. Hence, we obtain the following bound on the CHSH-expression:

$$-2 \leq \langle \mathcal{C}_{\mathrm{CHSH}} \rangle \leq 2. \tag{2.7}$$

Thus, we conclude that for any theory in which there exists a joint probability distribution for the CHSH-observables, the absolute value of the CHSH-quantity is bounded by two. It is important to note here that in order to conclude whether the set of observables $\{A_1, A_2, B_1, B_2\}$ admits a joint probability distribution, we never have to measure all of them simultaneously; it is sufficient to measure the pairs present in the expression in Eq. 2.5.

The bound in Eq. 2.7 provides a necessary and sufficient condition for the existence of a joint probability distribution for the observables $\{A_1, A_2, B_1, B_2\}$. It would be useful to have a general technique to generate such conditions, based only on the number of local observables per party. Such a technique was, in fact, introduced already by Boole (1862), and applied to the case of finding inequalities of the type of Eq. 2.7 by Pitowsky (1989, 1994).

The CHSH-inequality described above can be considered to be a hyperplane dividing the space of probability distributions of the pairs of observables A_iB_j: those that obey it, and that consequently possess a joint distribution, lie on one side, while those that fail to be consistent marginals of a joint distribution lie on the other. The minus sign in Eq. 2.5 can be distributed among the four possible places, which, together with the upper and lower bounds, in total yields eight hyperplanes bounding the set of classical correlations.

An equivalent way to describe the convex polytope circumscribed by these planes is to consider its vertices $\boldsymbol{v_i}$. In order to derive these vertices, we merely need to note that the fundamental condition for the existence of a joint probability distribution is the existence of a population such that the relative frequencies of values for the observables A_i and B_j approaches that of Table 2.1. We may imagine this as an urn model: each ball comes decorated with values for A_1, A_2, B_1 and B_2.

In order to check whether such a model exists, we can simply rely on conditions of logical consistency—within a population of balls that may be red or green, and wooden or made from metal, each ball that is both red and wooden must also possess the joint property 'red and wooden'. (Compare this with the condition for joint measurability in Eq. 1.17.)

Thus, for the simple case in which we have two observables A and B with outcomes ±1, as well as their conjunction $A \wedge B$, we require that their $+1$-outcomes obey the truth table of the Boolean and, as shown in Table 2.2.

TABLE 2.2: Truth table of the and-function.

A^+	B^+	$A^+ \wedge B^+$
0	0	0
0	1	0
1	0	0
1	1	1

The rows of this truth table now represent the logically possible outcomes: say, that the ball is neither red nor wooden, red but not wooden, and so on. We can associate to each of these possibilities a probability λ_i; then, the probabilities for the different outcomes, $\Pr(A^+)$, $\Pr(B^+)$, and

$\Pr(A^+B^+)$, where A^+ can be read as 'has property A', e.g. 'is red', can be obtained by the combination:

$$\begin{pmatrix}\Pr(A^+)\\ \Pr(B^+)\\ \Pr(A^+B^+)\end{pmatrix} = \lambda_1\begin{pmatrix}0\\0\\0\end{pmatrix} + \lambda_2\begin{pmatrix}0\\1\\0\end{pmatrix} + \lambda_3\begin{pmatrix}1\\0\\0\end{pmatrix} + \lambda_4\begin{pmatrix}1\\1\\1\end{pmatrix} = \begin{pmatrix}\lambda_2+\lambda_4\\ \lambda_3+\lambda_4\\ \lambda_4\end{pmatrix}, \tag{2.8}$$

with $0 \leq \lambda_i \leq 1$ and $\sum_i \lambda_i = 1$. Thus, all valid probability distributions $\boldsymbol{p} = (\Pr(A^+), \Pr(B^+), \Pr(A^+B^+))^T$ for this population can be written as a convex combination of the rows of Table 2.2, which therefore form the vertices $\boldsymbol{v_i}$ of a convex polytope:

$$\boldsymbol{p} = \sum_i \lambda_i \boldsymbol{v_i} \tag{2.9}$$

This polytope is depicted in Fig. 2.2.

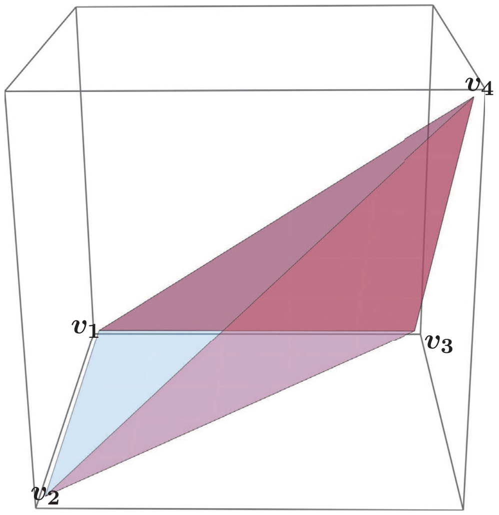


FIGURE 2.2: Polytope of allowed probability distributions consistent with the logical constraints in Table 2.2.

It is straightforward to extend this description to less trivial settings. For the CHSH-setting discussed above, the vertices of the polytope of classical correlations are obtained as the 16 rows of Table 2.3.

From these vertices, one can now once again obtain the facets of the polytope, which will take the form of inequalities $\boldsymbol{h} \cdot \boldsymbol{p} \leq x_0$, where $\boldsymbol{h}$ is the normal of the hyperplane corresponding to a facet, and x_0 is a scalar offset. Among the nontrivial (that is, not given from simple consistency conditions

TABLE 2.3: Vertices of the polytope of classical correlations in the CHSH-setting.

A_1	A_2	B_1	B_2	$A_1 \wedge B_1$	$A_1 \wedge B_2$	$A_2 \wedge B_1$	$A_2 \wedge B_2$
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0
0	0	1	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	0	0	0	0	0
0	1	0	1	0	0	0	1
0	1	1	0	0	0	1	0
0	1	1	1	0	0	1	1
1	0	0	0	0	0	0	0
1	0	0	1	0	1	0	0
1	0	1	0	1	0	0	0
1	0	1	1	1	1	0	0
1	1	0	0	0	0	0	0
1	1	0	1	0	1	0	1
1	1	1	0	1	0	1	0
1	1	1	1	1	1	1	1

on the probabilities) inequalities, one finds the set (Pitowsky 1989):

$$\begin{aligned}
-1 \leq \Pr\left(A_1^+ B_1^+\right) + \Pr\left(A_1^+ B_2^+\right) + \Pr\left(A_2^+ B_1^+\right) & - \Pr\left(A_2^+ B_2^+\right) \\
& - \Pr\left(A_1^+\right) - \Pr\left(B_1^+\right) \leq 0 \\
-1 \leq \Pr\left(A_1^+ B_1^+\right) + \Pr\left(A_1^+ B_2^+\right) - \Pr\left(A_2^+ B_1^+\right) & + \Pr\left(A_2^+ B_2^+\right) \\
& - \Pr\left(A_1^+\right) - \Pr\left(B_2^+\right) \leq 0 \\
-1 \leq \Pr\left(A_1^+ B_1^+\right) - \Pr\left(A_1^+ B_2^+\right) + \Pr\left(A_2^+ B_1^+\right) & - \Pr\left(A_2^+ B_2^+\right) \qquad (2.10) \\
& - \Pr\left(A_2^+\right) - \Pr\left(B_1^+\right) \leq 0 \\
-1 \leq \Pr\left(A_1^+ B_1^+\right) + \Pr\left(A_1^+ B_2^+\right) + \Pr\left(A_2^+ B_1^+\right) & - \Pr\left(A_2^+ B_2^+\right) \\
& - \Pr\left(A_2^+\right) - \Pr\left(B_2^+\right) \leq 0
\end{aligned}$$

These inequalities were first proposed by Clauser and Horne (1974), and are thus generally referred to as CH-inequalities. Analogous inequalities hold after exchanging some subset of $+1$ outcomes for -1 outcomes; adding those inequalities containing only $+1$ or only -1 outcomes to -1 times those containing mixed outcomes, one obtains the CHSH-inequalities from above.

We have now introduced a method of bounding the correlations obtainable in classical theories, that is, in theories where all effects are jointly observable. However, since this is not the case in quantum theory, or in more general GPTs, one might suspect that these bounds fail to hold in such theories. We will now proceed to put this intuition on more solid footing.

2.1.2 Quantum Correlations and Beyond

Imagine you have three coins, C_1, C_2 and C_3, each of which, when thrown in isolation, yields either heads (H) or tails (T) with 50% probability. You can throw either pair of coins simultaneously, and find the following correlations:

- whenever C_1 and C_2 are thrown together, the outcome is either both heads (HH) or both tails (TT), with equal probability
- whenever C_2 and C_3 are thrown together, the outcome is again either (HH) or (TT), with equal probability
- whenever C_1 and C_3 are thrown together, the outcome is either (HT) or (TH), with equal probability.

Clearly, these pairwise joint distributions are compatible, in the sense that the single-coin marginal distributions always yield either (H) or (T) with probability $\frac{1}{2}$. However, trying to throw all three coins simultaneously, we run into an inconsistency: if C_1 yields (H), then so must C_2; but then, likewise, C_3 must yield (H)—but from the anticorrelation between C_3 and C_1, this implies that C_1 must yield (T). Thus, there is no possible assignment of values to all three coins thrown together.

Now, can such a situation in fact occur in the real world? One might think that, due to the joint measurability of all effects, this situation is impossible in the classical realm. This is, however, not quite the case: for instance, it would be easy to program a computer such that it yields the above correlations. Moreover, a machine can be constructed distributing tokens marked (H) or (T) in accordance with these statistics, as long as it is forbidden to request all three tokens at once.

More in general, a failure to possess a joint distribution is possible if, for instance, the choice of pairs influences the probability distribution from which their values are drawn; that is, if the pair $\{C_1, C_3\}$ is chosen, the probability distribution for all three coins is

$$\Pr(C_1, C_2, C_3) = \lambda_1(HTT) + \lambda_2(HHT) + \lambda_3(THH) + \lambda_4(TTH). \quad (2.11)$$

Here, $\lambda_1 + \lambda_2 = \frac{1}{2} = \lambda_3 + \lambda_4$ to yield the correct probability for the outcomes of C_1 and C_3 (since the value of C_2 is unobservable in this setting, we can leave its probability open), while if the pair $\{C_2, C_3\}$ is chosen, the joint probability distribution is instead

$$\Pr(C_1, C_2, C_3) = \mu_1(HHH) + \mu_2(HTT) + \mu_3(THH) + \mu_4(TTT), \quad (2.12)$$

where now $\mu_1 + \mu_3 = \frac{1}{2} = \mu_2 + \mu_4$. Finally, for the pair $\{C_1, C_2\}$, we have

$$\Pr(C_1, C_2, C_3) = \nu_1(HHH) + \nu_2(HHT) + \nu_3(TTH) + \nu_4(TTT), \quad (2.13)$$

with again $\nu_1 + \nu_2 = \frac{1}{2} = \nu_3 + \nu_4$. Thus, allowing the choice of measurement to influence the outcome distribution, we can reproduce the correlations of the coins. This condition is commonly called (Shimony 1986) *parameter dependence* (where the parameter is the choice of pair to throw, or, more generally, the choice of measurement).

Another possibility is to have the outcome of the second coin throw depend on the outcome of the first (or vice versa): thus, if C_1 is thrown and lands (H), immediately it is fixed that if C_2 were thrown, it would yield (H), while C_3 would yield (T). This condition is known as *outcome dependence* (Shimony 1986). In the following, we will refer to the assumption that neither parameter- nor outcome-dependence is given as *nondisturbance assumption*.

A final possibility is that there simply is no joint probability distribution. In other words, events which cannot be observed—such as the simultaneous throwing of all three coins—do not possess a well-defined probability. This is equivalent to assuming that there does not, in general, exist an underlying definite value for all observables—since if there was such a value, and there is neither parameter- nor outcome dependence, the asymptotic relative frequencies of possible value assignments within a population would yield a probability distribution as in Table 2.1. The assumption that there is such an underlying definite value is generally called *value definiteness*, or sometimes simply *realism*.

In the classical realm, we can assume all observable quantities to be simultaneously definite, since there are joint effects for any collection of effects. Thus, we can think of measurement in classical mechanics as merely 'revealing' an a priori present value of a given quantity. Consequently, all violations of inequalities of the conditions for the existence of a joint probability distribution must be due to either of the first two conditions—that is, either the choice of measurement, or its outcome, must influence, or disturb, the probability distribution from which measurement outcomes are drawn.

However, due to the possible non-existence of joint effects in GPTs, the situation here is less clear-cut. It is, in fact, possible to find GPT-systems which lead to a violation of the bounds in Eq. 2.7. In this section, we will merely introduce this possibility, leaving questions of interpretation for the next section.

Such a setup is given by the so-called *Popescu-Rohrlich (PR) box* (Popescu and Rohrlich 1994). Popescu and Rohrlich take the CHSH-setting in Fig. 2.1, and imagine a system that, upon measurement of a pair of local observables $\{A_{i+1}, B_{j+1}\}$, returns an answer according to the following probability distribution:

$$\Pr\left(A_{i+1}^{a_k}, B_{j+1}^{b_l}\right) = \begin{cases} \frac{1}{2} & \text{if } i \cdot j = k \oplus l \\ 0 & \text{otherwise} \end{cases} \tag{2.14}$$

Here, $i, j, k, l \in \{0, 1\}$, the operator $\oplus$ denotes addition modulo 2, and the indices k and l yield the outcomes $a_k = (-1)^k$ and $b_l = (-1)^l$. This implies perfect anticorrelation in the case of measuring the pair $\{A_2, B_2\}$, since $k \oplus l = 1$ implies $k \neq l$, but perfect correlation for the pairs $\{A_1, B_1\}$, $\{A_1, B_2\}$, and $\{A_2, B_1\}$. Nevertheless, outcome probabilities on one side are independent of the settings on the other, thus satisfying the no-signalling principle (see Sec. 1.1.2). Thus, the correlations defined in this way are often referred to as *no-signalling correlations.* This yields for the CHSH-expression

$$\begin{aligned} \langle \mathcal{C}_{\mathrm{CHSH}} \rangle &= \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle \\ &= 1 + 1 + 1 - (-1) \\ &= 4 > 2. \end{aligned} \tag{2.15}$$

Thus, we have seen that GPTs contain correlations that cannot be the result of a joint probability distribution for all observable quantities. In fact, since the value 4 is the algebraic maximum of the CHSH-expression for ± 1-valued observables, we can say that such correlations yield a maximal violation of the CHSH-inequality.

As we have seen, in and of itself, that may not be surprising: failure of either parameter- or outcome-independence suffices to account for the observed violation. However, in the next section, we will introduce some assumptions that give us good *physical* reason to believe that these conditions are upheld, and nevertheless, the violation will persist; and in fact, as we will see, this violation is not just present in some abstract GPT, but rather, occurs in quantum mechanics as well.

2.2 Three No-Go Theorems

In order to make the connection between the abstract formalism introduced so far and physics, we need to specify a physical scenario in which we intend to perform experiments. Furthermore, we will introduce scenarios such that we have good physical reason to suppose that the nondisturbance assumption is fulfilled, and nevertheless show that violations of the bounds in Eq. 2.7 occur, leading to the conclusion that either, despite appearances, there is some influence of either the choice of measurements, or their outcomes, on one another—or that we must drop the assumption of value definiteness.

There are several possibilities to interpret correlators like $\langle AB\rangle$: they could pertain to the correlation of observables measured on distinct systems (or subsystems); the measurements could be performed simultaneously on one and the same system; or, they could be performed in sequence on a system. Each of these cases, as we will see in the following, leads to an interesting result. Since we are mainly concerned with the consequences of these in a real experimental setting, in the following, we will use the quantum formalism, on the presumption that quantum theory is indeed the correct description of real physical systems.

2.2.1 Bell: Locality

In order to ensure nondisturbance, the most stringent physical requirement is to carry out measurements on systems that cannot possibly influence each other. According to the special theory of relativity, information (or information-bearing physical carriers) propagate with a speed bounded by that of light in vacuum, c. Hence, performing measurements on two systems separated by a sufficient distance such that no signal could reach each from the other during the performance of the experiment seems to forestall any possibility of influence between the experiments.

This is, in fact, the assumption of *locality* made by Bell (1964). In our setup, this corresponds to assuming a joint system, described by a density operator ρ_{AB} in the joint Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, on which local measurements of the form $A_i \otimes \mathbb{1}$ and $\mathbb{1} \otimes B_j$ are performed. Thus, the CHSH-expression becomes

$$\langle \mathcal{C}_{\mathrm{CHSH}}\rangle = \langle A_1 \otimes B_1\rangle + \langle A_1 \otimes B_2\rangle + \langle A_2 \otimes B_1\rangle - \langle A_2 \otimes B_2\rangle. \tag{2.16}$$

If the locality-assumption now suffices to certify nondisturbance, and if we are furthermore justified in assigning definite values to these quantum mechanical observables, then the above expression should be bounded by 2.

However, if we take the state

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{2.17}$$

together with the observables

$$\begin{aligned} A_1 &= \sigma_x, \quad B_1 = \tfrac{1}{\sqrt{2}}(\sigma_x + \sigma_z), \\ A_2 &= \sigma_z, \quad B_2 = \tfrac{1}{\sqrt{2}}(\sigma_x - \sigma_z), \end{aligned} \tag{2.18}$$

a straightforward calculation of the expectation values

$$\langle A_i B_j \rangle = \operatorname{tr}\left(A_i \otimes B_j \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|\right) \tag{2.19}$$

shows that

$$\begin{aligned} \langle \mathcal{C}_{\mathrm{CHSH}} \rangle &= \langle A_1 \otimes B_1 \rangle + \langle A_1 \otimes B_2 \rangle + \langle A_2 \otimes B_1 \rangle - \langle A_2 \otimes B_2 \rangle \\ &= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - (-\frac{1}{\sqrt{2}}) \\ &= 2\sqrt{2} > 2. \end{aligned} \tag{2.20}$$

Which, as can be shown, is in fact the maximum value (Cirel'son 1980). Thus, despite the locality requirement, there are quantum mechanical measurements that do not possess a joint probability distribution. The impossibility to reconcile a *local realistic* picture with the predictions of quantum mechanics is the content of *Bell's theorem*. The reason for this irreconcilability does indeed lie with the failure of co-measurability of the observables: neither A_1 and A_2, nor B_1 and B_2 are jointly measurable, since both $[A_1, A_2]$ and $[B_1, B_2]$ are nonzero (cf. Eq. 1.52). The necessity of this requirement can be seen easily by taking the square of the CHSH-operator:

$$\mathcal{C}^2_{\mathrm{CHSH}} = 4 \cdot \mathbb{1} + (A_1A_2 - A_2A_1) \otimes (B_2B_1 - B_1B_2) = 4 \cdot \mathbb{1} - [A_1, A_2] \otimes [B_1, B_2], \tag{2.21}$$

where we have used that dichotomic observables square to the identity. Hence, a violation of the CHSH-inequality is only possible if both commutators are nonvanishing.

Note, however, that while this is a necessary condition, it is not alone sufficient: for a state of the form $\rho_{\mathrm{prod}} = |\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2|$, since the observables A_i act nontrivially only on $|\psi_1\rangle$, while the observables B_j act only on $|\psi_2\rangle$, the correlators factorize (cf. Eq. 2.4), yielding for the expectation value of the CHSH-operator

$$\begin{aligned} \langle \mathcal{C}_{\mathrm{CHSH}} \rangle &= \langle A_1 \rangle \langle B_1 \rangle + \langle A_1 \rangle \langle B_2 \rangle + \langle A_2 \rangle \langle B_1 \rangle - \langle A_2 \rangle \langle B_2 \rangle \\ &= \langle A_1 \rangle \left(\langle B_1 \rangle + \langle B_2 \rangle\right) + \langle A_2 \rangle \left(\langle B_1 \rangle - \langle B_2 \rangle\right) \\ &\leq 2, \end{aligned} \tag{2.22}$$

since $\langle A_i \rangle, \langle B_j \rangle \leq 1$. This extends to convex combinations $\rho_{\mathrm{sep}} = \sum_i p_i \rho^i_{\mathrm{prod}}$, since each of the terms in the combination is bounded by 2. Thus, separable states, i.e. states that can be written as a convex combination of product states, cannot violate the bound $|\langle \mathcal{C}_{\mathrm{CHSH}} \rangle| \leq 2$. It follows that, besides non-jointly measurable observables, entanglement is a critical resource for Bell inequality violation.

It is sometimes alleged that Bell's theorem implies that quantum mechanics is a non-local theory (see, e.g. Maudlin 2014b). This, as we have seen, is however only justified if one requires the existence of a probability table of the form of Table 2.1, assigning probabilities even to unobservable joint effects (s.a. (Werner 2014a), (Maudlin 2014a) for a reply, and (Werner 2014b) for a response to the reply). Dropping this assumption means that bounds of the form of Eq. 2.7 or 2.10 can no longer be derived, without resorting to any non-local influence of either measurement settings or outcomes.

There is another interesting consequence of the violation of Bell inequalities: in all theories (including, specifically, the generalized probabilistic theories of Sec. 1.1) that are no-signalling and that predict the violation of Bell inequalities, information cannot be perfectly copied—that is, in all such theories there exists a *no-cloning theorem* (Masanes, Acin, and N. Gisin 2006). Indeed, the quantum no-cloning theorem was first found in the context of a proposal (due to Herbert (1982)) for superluminal communication (Dieks 1982; Wootters and Zurek 1982): picture two parties, Alice and Bob, who share the $|\Phi^+\rangle$-Bell state (see Eq. 1.67). Both parties can carry out measurements in either the σ_x- or σ_z-basis. After Alice carries out her measurement, Bob's particle will be in an eigenstate of the basis Alice used, and hence, yield a deterministic outcome if Bob measures in the same basis, but a random one if he measures along an orthogonal direction.

Now suppose Bob uses a cloning machine in order to multiply his qubit, that is, he effects the transition

$$|\psi_B\rangle \otimes |r\rangle \rightarrow |\psi_B\rangle \otimes |\psi_B\rangle = U_C\,|\psi_B\rangle \otimes |r\rangle\,, \tag{2.23}$$

where $|\psi_B\rangle$ is the state of Bob's qubit, $|r\rangle$ is a qubit in some reference state, and U_C is a unitary matrix implementing the cloning operation. Then, if Bob performs this operation often enough, he ends up with an ensemble of identical quantum states which are eigenstates of either σ_x or σ_z. Now, he simply needs to measure half of his qubits in the σ_x-basis, and the other half in the σ_z-basis, to see which measurement yields a deterministic outcome, and thus, to find out which measurement was performed by Alice.

Since this protocol may be performed on a timescale shorter than the time a speed-of-light signal would need to reach Bob from Alice, provided both parties are sufficiently far removed from one another, and Alice can use her choice of measurement basis to communicate one bit of information to Bob, this thus constitutes faster-than-light communication. However, we had demanded just the impossibility of such FTL-signalling in establishing the GPT-framework; consequently, since quantum mechanics fits into this framework, no operation of the form in Eq. 2.23 can exist for general states.

2.2.2 Kochen-Specker: Noncontextuality

As Bell's theorem relies on locality in order to prevent influences between different measurements, so does the theorem by Kochen and Specker (1969) rely on the notion of *noncontextuality*: roughly, the idea that the value of an observable A, measured simultaneously with observables B or C (with which it hence must be jointly measurable), does not depend on whether it is measured simultaneously with B or C. This is a reasonable expectation in the classical world—for instance, we do not observe an object's color changing, depending on whether we measure it simultaneously with its shape, or with its mass.

It is again clear that this assumption holds whenever we have a joint probability distribution—as in this case, we can think of a population in which elements simply carry certain values for all observables within experimental interest, which do not mutually influence one another, and are simply revealed upon measurement. The assumption is, however, not justified in the case of our coin example: if we assume that, say, the outcome of throwing C_2 is always (H), independent of whether we throw the third or first coin simultaneously with it, we run into a contradiction—namely, we would deduce that both of these coins likewise always yield (H), contrary to their mutual anticorrelation.

To make these notions more precise, let us consider four observables $\{A, B, C, D\}$ on a four-dimensional Hilbert space $\mathcal{H}_4$. Among these observables, we have the following commutation (and hence, joint measurability) relations:

$$\begin{array}{ll} [A,B]=0 & [C,B]=0 \\ [A,D]=0 & [C,D]=0 \\ [A,C]\neq 0 & [B,D]\neq 0 \end{array} \tag{2.24}$$

Thus, in the expression

$$\langle \mathcal{C}_{\mathrm{CHSH}}^{\mathrm{KS}} \rangle = \langle AB\rangle + \langle BC\rangle + \langle CD\rangle - \langle DA\rangle, \tag{2.25}$$

only jointly measurable quantities enter in pairs. If we now assume that the value of each observable is independent of the context—that, for instance, the value of A does not depend on whether it is measured simultaneously with B or D—we again assume the presence of a joint probability distribution for all observables, and consequently, again obtain the bound $|\langle \mathcal{C}_{\mathrm{CHSH}}^{\mathrm{KS}} \rangle| \leq 2$.

Now, with the identifications $A_1 \otimes \mathbb{1} = C$, $A_2 \otimes \mathbb{1} = A$, $\mathbb{1} \otimes B_1 = D$ and $\mathbb{1} \otimes B_2 = B$, the observables in Eq. 2.18 fulfill exactly these relations. Consequently, we cannot assume that each of them yields its value independently of its context—and hence, any test of Bell's theorem is also a test of the Kochen-Specker theorem.

However, we need not appeal to entanglement, or indeed the bipartite Hilbert-space structure in order to test the Kochen-Specker theorem. For instance, we may take the observables (which are related to the observables in Eq. 2.18 by a unitary rotation)

$$\begin{aligned} A &= \sigma_x \otimes \sigma_x, \qquad B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \\ C &= \sigma_x \otimes \mathbb{1}, \quad D = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \end{aligned} \tag{2.26}$$

and the (product) state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle), \tag{2.27}$$

to again obtain the value $\left\langle \mathcal{C}_{\mathrm{CHSH}}^{\mathrm{KS}} \right\rangle = 2\sqrt{2}$. Hence, we can view the noncontextuality of Kochen and Specker as a relaxation of Bell's locality: for any set of local observables, the commutation relations in Eq. 2.24 will be automatically fulfilled, but not every set of observables fulfilling them consists of local observables on a bipartite Hilbert space.

2.2.3 Leggett-Garg: Macroscopic Realism

Finally, the third option to make the nondisturbance assumption plausible is the *macroscopic realism* of Leggett and Garg (1985). Macroscopic realism is the conjunction of two postulates:

- Any macroscopic system that has available to it two or more distinguishable states, is at any given time in exactly one of those states.
- It is possible, in principle, to determine which of these states the system is in at a given time, without disturbing the system or its dynamics.

Let us thus imagine a system that has exactly two states available to it, as well as a measurement Q (which we again assume to be ±1-valued) that is capable of differentiating between these states. Furthermore, we measure this observable at four different points in time $t_1 \ldots t_4$. Then, we observe the correlation between measurements at different points in time, and calculate the quantity

$$\left\langle \mathcal{C}_{\mathrm{CHSH}}^{\mathrm{LG}} \right\rangle = \langle Q(t_1)Q(t_2)\rangle + \langle Q(t_2)Q(t_3)\rangle + \langle Q(t_3)Q(t_4)\rangle - \langle Q(t_1)Q(t_4)\rangle. \tag{2.28}$$

Again, now, the assumption of macroscopic realism serves to shield a measurement at a later time from the influence of an earlier one; thus, again, we can assume a joint probability distribution for the value of Q at different times, and conclude that $\left|\left\langle \mathcal{C}_{\mathrm{CHSH}}^{\mathrm{LG}} \right\rangle\right| \leq 2$.

A difference to the previous two cases is now that at first sight, there is no problem with 'joint' measurability—after all, we just re-measure the same observable Q at different points in time. However, in general, there will be a non-trivial time-evolution of the system in between measurements. This time-evolution is mediated by some unitary $U(t)$, producing the transformation $|\psi(0)\rangle \to |\psi(t)\rangle = U(t)\,|\psi(0)\rangle$. To calculate the expectation value of an operator at time t, we can equally well use a time-evolved operator and the state at $t = 0$:

$$\begin{aligned} \langle A \rangle_t &= \mathrm{tr}\left(A\rho(t)\right) \\ &= \mathrm{tr}\left(AU(t)\rho(0)U^\dagger(t)\right) \\ &= \mathrm{tr}\left(U^\dagger(t)AU(t)\rho(0)\right) \\ &= \mathrm{tr}\left(A(t)\rho(0)\right). \end{aligned} \tag{2.29}$$

This is known as the *Heisenberg picture*, whereas the corresponding picture in which the time evolution acts on the states instead is the *Schrödinger picture*. Hence, we can keep the initial state fixed, and take $Q_i = U^\dagger(t_i - t_0)Q(t_0)U(t_i - t_0)$. However, this yields 'too much' incommensurability: in general, $[Q(t_i), Q(t_j)] \neq 0$ for any pair of indices, and consequently, we do not know how to define the correlator $\langle Q(t_i)Q(t_j)\rangle$, as the simple product of both operators will typically fail to be Hermitian.

Nevertheless, for projective qubit measurements, we can go back to the definition of the correlator

$$\langle Q_1 Q_2\rangle = \sum_{q_k, q_l} q_k q_l \mathrm{Pr}\,(Q_1^{q_k} Q_2^{q_l})\,, \tag{2.30}$$

where $q_k, q_l \in \{+1, -1\}$ are the outcomes of Q_1 and Q_2, respectively. To calculate these probabilities, the projection postulate yields

$$\mathrm{Pr}\,(Q_1^{q_k} Q_2^{q_l}) = \left\langle \frac{\mathbb{1} + q_k \boldsymbol{q_1}\cdot\boldsymbol{\sigma}}{2} \cdot \frac{\mathbb{1} + q_l \boldsymbol{q_2}\cdot\boldsymbol{\sigma}}{2} \cdot \frac{\mathbb{1} + q_k \boldsymbol{q_1}\cdot\boldsymbol{\sigma}}{2} \right\rangle, \tag{2.31}$$

where $\boldsymbol{q_i}$ is the Bloch vector associated to Q_i.

Using this to compute the correlator, one arrives at the expression (Fritz 2010)

$$\sum_{q_k, q_l} q_k q_l \mathrm{Pr}\,(Q_1^{q_k} Q_2^{q_l}) = \langle Q_1 \circ Q_2\rangle, \tag{2.32}$$

for the appropriate quantum analogue to the classical correlation functions in Eq. 2.28, where the symbol $\circ$ denotes the symmetric (Jordan) product

$$X \circ Y = \frac{XY + YX}{2}. \tag{2.33}$$

With this framework, it can again be shown that in quantum mechanics, a maximum of $\langle \mathcal{C}_{\mathrm{CHSH}}^{\mathrm{LG}}\rangle = 2\sqrt{2}$ is achievable.

Chapter 3

Their Detection

We have now introduced the main tools and concepts necessary for the study of quantum correlations. In this chapter, we aim to bring these tools to bear, with a particular focus on the experimental detection of these correlations.

One particular issue that needs to be addressed in translating the concepts developed so far to the laboratory is the fact that, in general, no experiment is free of noise. As a consequence, no state preparation is ever perfect: instead of some target state ρ, a real preparation procedure may end up producing, e.g., a state of the form

$$\rho' = p\rho + \frac{1-p}{d}\mathbb{1}_d, \tag{3.1}$$

where d is the Hilbert space dimension. This models the addition of white (unbiased) noise to the target state, and may result in its deterioration to such an extent that methods developed to test qualities of the state ρ—such as its degree of entanglement—are no longer applicable.

Furthermore, a realistic measurement never exactly corresponds to a given measurement operator O one set out to implement. Finite precision in, e.g., polarizer settings may result in a slightly different measurement being actually implemented. As an important consequence, measurements A and B that are formally jointly measurable, may fail to be so in their actual implementation—that is, $[A, B] = 0$ does not hold exactly. This raises issues, e.g., with the experimental testing of the predictions of the Kochen-Specker theorem.

It is not our purpose here to study these experimental imperfections in detail. Rather, we will instead propose methods robust to such unavoidable inaccuracies, which then may be experimentally applicable even in cases where the original methods fail to be, and thus, we aim to extend the reach of laboratory testing to novel phenomena.

In particular, in the following sections, we will introduce a method to test the Kochen-Specker predictions (or rather, a slight generalization) in experimentally realistic cases, where the usual definition of noncontextuality does not hold in general. Afterwards, we will turn our attention to the phenomenon of entanglement and its detection via so-called *witness operators*, where a witness is an operator W such that

$$\mathrm{tr}\,(W\rho)\begin{cases} \geq 0 & \text{if } \rho \,\text{is separable}, \\ < 0 & \text{for at least one entangled } \rho. \end{cases} \tag{3.2}$$

Here, it is the problem of detecting the entanglement of a completely unknown state ρ that will concern us, and we exhibit a construction capable of finding the optimal witness operator, given a set of local measurements and their outcomes. This construction makes use of the method of semidefinite programming, to which we give a brief introduction.

3.1 Testing Quantum Contextuality

As we have seen in Sec. 2.2.2, the Kochen-Specker theorem introduces a nondisturbance assumption based on the idea that jointly measurable observables, i.e. A and B such that $[A, B] = 0$, do not influence each other. However, in realistic experimental implementations, this condition does not hold in general. Hence, violations of the classical bound of inequalities such as

$$\left\langle \mathcal{C}^{\mathrm{KS}}_{\mathrm{CHSH}} \right\rangle = \langle AB \rangle + \langle BC \rangle + \langle CD \rangle - \langle DA \rangle \leq 2 \tag{3.3}$$

do not necessarily signal the contextuality of quantum theory; instead, it may be the case that measurement of A, say, influences the value of B and D, if they are imperfectly implemented.

Indeed, one can write down an explicit model where a measurement introduces a random state transition independently of which observable is measured, which allows a violation of inequality 3.3 up to (and beyond) quantum levels (Szangolies, Kleinmann, and Gühne 2013; s.a. Szangolies 2015).

3.1.1 Markov Models

To introduce this model, we again work in the CHSH-setting introduced before. Let us assume that each observable $O \in \{A, B, C, D\}$ can always be assigned a definite value $v(O) = \pm 1$. Clearly, this amounts to assuming a joint probability distribution, which simply states the probabilities for each possible value assignment to be present. Thus, each possible state of the model is a probability distribution of the form given in Table 2.1.

Such a probability distribution can be considered as a 16-dimensional vector spanning the set of possible probability assignments, that is, a convex combination of the basis states

$$\boldsymbol{\lambda_i} = (\underbrace{0, \ldots, 0}_{i\,\text{zeros}}, 1, \underbrace{0, \ldots, 0}_{15-i\,\text{zeros}})^T, \tag{3.4}$$

where $i \in \{0, \ldots, 15\}$, and each $\boldsymbol{\lambda_i}$ corresponds to one definite assignment of values ± 1 to the observables $\{A, B, C, D\}$. These values are sometimes called *hidden variables*, and the resulting state is the *hidden-variable state*. Thus, we can alternatively label the basis states by this value assignment, yielding e.g. $\boldsymbol{\lambda_0} = (+ + + +)$, $\boldsymbol{\lambda_1} = (+ + + -)$, and so on, where we have used the obvious abbreviations of $+$ and $-$ for the values $+1$ and -1 respectively. If we now consider

$$(+) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad (-) = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{3.5}$$

as a basis for the individual subspaces associated with each observable, we can write, e.g.,

$$\boldsymbol{\lambda_0} = (++++) = (+) \otimes (+) \otimes (+) \otimes (+), \tag{3.6}$$

and analogously for the other basis vectors. The general state is then of the form

$$\boldsymbol{P} = \sum_i p_i \boldsymbol{\lambda_i}, \tag{3.7}$$

with p_i being the probability of finding the system in state $\boldsymbol{\lambda_i}$.

Allowed transformations in this model are all linear transformations that take valid probability distributions to valid probability distributions, that is, transformations which preserve the 1-norm $||\boldsymbol{P}||_1 = \sum_i p_i = 1$. Thus, the condition for a matrix $M = (m_{ij})$ to represent a valid transformation $\boldsymbol{P} \rightarrow \boldsymbol{P'} = M\boldsymbol{P}$ follows from

$$\sum_i p'_i = \sum_{ij} m_{ij} p_j = 1, \tag{3.8}$$

which necessitates that $\sum_i m_{ij} = 1$. Such matrices are generally called *(left-)stochastic*.

The model now is a *Markov chain*, that is, a discrete random process that undergoes probabilistic state transitions without memory (Norris 1998). The states of the Markov chain are just the value-assignments to the observables, i.e., the hidden-variable states. Whenever a measurement is performed, the noise introduced into the system via its imperfect implementation may lead to a state change with a certain probability p. Note that the transition does not depend on which measurement is carried out—in this sense, the model is 'noncontextual'. Consider now the model given by the transition matrix (Szangolies, Kleinmann, and Gühne 2013)

$$\begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \otimes \mathbb{1}_2^{\otimes 3}, \tag{3.9}$$

which after the first measurement flips the value assigned to observable A with a probability of p, and leaves all other values invariant. Suppose $p = 1$, such that the value of A is flipped deterministically. Then, we can introduce the quantity

$$K_{ij} = A_i B_j + B_i C_j + C_i D_j - D_i A_j, \tag{3.10}$$

where the notation $A_i = A(\boldsymbol{\lambda_i})$ denotes the value of A given the hidden state $\boldsymbol{\lambda_i}$. For $p = 1$, e.g. the state $\boldsymbol{\lambda_0} = (++++)$ is taken to $\boldsymbol{\lambda_8} = (-+++)$ after each measurement; hence, since $K_{0,8} = 4$, this would violate the inequality maximally. For arbitrary p, starting in the state $\boldsymbol{\lambda_0}$, we have

$$\langle \mathcal{C}^{\mathrm{KS}}_{\mathrm{CHSH}} \rangle = pK_{0,8} + (1-p)K_{0,0} = 2 + 2p, \tag{3.11}$$

and hence, any $p \geq 0$ leads to a violation of the KS-CHSH inequality. In fact, it can be shown that such a violation exists for arbitrary starting states $\boldsymbol{P} = \sum_i p_i \boldsymbol{\lambda_i}$ (Szangolies, Kleinmann, and Gühne 2013).

3.1.2 Noncontextual Evolution

We have now exhibited a model capable of violating KS-inequalities, even though it may be said to be 'noncontextual' in the sense that its dynamics are unchanged, no matter which measurement (or set of measurements in more general cases) is performed. The reason for this is the failure of the KS-nondisturbance assumption: in realistic experiments, we do not have perfectly compatible observables; thus, we cannot conclude that measurement of one observable does not influence the value of the other, as in general, there exists an uncertainty principle between incompatible observables.

This severely hampers the experimental testability of the Kochen-Specker predictions. One way around this problem that has been proposed is by way of the use of error terms that seek to quantify the amount of disturbance introduced by the incompatibility of observables (Gühne et al. 2010). The KS-CHSH equation then assumes the form

$$\begin{aligned}\langle \mathcal{C}^{\mathrm{KS}}_{\mathrm{CHSH}}\rangle - 2p^{err}(B^1A^2B^3) - 2p^{err}(C^1B^2C^3)\\ -2p^{err}(D^1C^2D^3) - 2p^{err}(A^1D^2A^3) \leq 2,\end{aligned} \tag{3.12}$$

where e.g. $p^{err}(B^1A^2B^3)$ is the probability that the first and second measurements of the value of B disagree, given that A was measured in between. However, these error terms only hold in the case where additional measurements always increase the total disturbance to the system; yet, this assumption may not hold in models of the form discussed in the previous section, and thus, such models can lead to violations of inequality 3.12.

Hence, a different approach towards making the KS-predictions experimentally accessible was pursued in (Szangolies, Kleinmann, and Gühne 2013). This approach may be viewed as finding a new nondisturbance assumption that can be termed *noncontextual evolution*, consisting of the conjunction of two conditions:

- All of a system's observables have definite values at any given time.
- It is possible to uniquely attribute to each system a sequence of (hidden-variable) states $\boldsymbol{\lambda_i} \rightarrow \boldsymbol{\lambda_j} \rightarrow \boldsymbol{\lambda_k} \rightarrow \ldots$ (or probabilistic combinations thereof) that is independent of the measurements performed on the system.

In a sense, this can be viewed as a generalization and combination of both the Leggett-Garg and Kochen-Specker nondisturbance assumptions: taking the trivial evolution in which the hidden-variable state remains unchanged throughout the measurement procedure returns the KS-scenario; using measurements that merely check one single property at any given point in time yields the LG one. Taken together, we can now impose a time-ordering on the measurements: take, for instance, two dichotomic measurements Q_1 and Q_2, and evaluate them at two distinct points in time, t_1 and t_2. We can then propose the following inequality:

$$\langle Q_1(t_1)Q_2(t_2)\rangle + \langle Q_1(t_1)Q_1(t_2)\rangle + \langle Q_2(t_1)Q_1(t_2)\rangle - \langle Q_2(t_1)Q_2(t_2)\rangle \leq 2, \tag{3.13}$$

which holds again in all cases where there exists a joint probability distribution for all observables.

TABLE 3.1: The Peres-Mermin square of nine observables on a two-qubit system.

$A = \sigma_x \otimes \mathbb{1}$	$B = \mathbb{1} \otimes \sigma_x$	$C = \sigma_x \otimes \sigma_x$
$a = \mathbb{1} \otimes \sigma_y$	$b = \sigma_y \otimes \mathbb{1}$	$c = \sigma_y \otimes \sigma_y$
$\alpha = \sigma_x \otimes \sigma_y$	$\beta = \sigma_y \otimes \sigma_x$	$\gamma = \sigma_z \otimes \sigma_z$

Now, we can impose a similar time ordering on inequality 3.3, which yields

$$\left\langle \mathcal{C}_{\mathrm{CHSH}}^{\mathrm{NCE}} \right\rangle = \langle AB \rangle + \langle CB \rangle + \langle CD \rangle - \langle AD \rangle \leq 2, \tag{3.14}$$

where the ordering now indicates the measurement sequence. Note that the same observables are always measured at the same point in the sequence. This ensures now that the model proposed above no longer is capable of violating the inequality: the quantity $K_{ij} = A_i B_j + C_i B_j + C_i D_j - A_i D_j$ is bounded by two for all possible hidden-variable evolutions (as long as they are independent of which measurement is being performed). Thus, models obeying the new nondisturbance assumption can be ruled out, and moreover, since we do no longer need perfect compatibility between measurements, this possibility is in fact directly amenable to experimental testing. Furthermore, since the class of models ruled out includes the Kochen-Specker noncontextual ones, this opens up a perspective for testing the Kochen-Specker predictions in the laboratory.

The procedure outlined so far can be generalized to different settings. For instance, a conceptually insightful proof of the Kochen-Specker theorem is given by the Peres-Mermin square (Mermin 1990b; Peres 1990), as shown in Table 3.1.

In this table of observables, each row and each column yields a set of compatible observables (a context), and the product of every row, as well as the first two columns, is $\mathbb{1}$, while the product of the observables in the third column yields $-\mathbb{1}$. Each of the observables, measured individually, yields either the value $+1$ or -1. Thus, if we try to distribute values among the observables independently of the context in which they are measured, then, in order to obey the condition given by the row products, the product of all of these values needs to be $+1$, and hence, an even number of -1's must occur in the value assignment; however, looking at the columns, the product of all the values ought to be -1, necessitating an odd number of -1's. Hence, no context-independent assignment of values can reproduce the quantum mechanical predictions.

It is worthy of note that we have not needed to talk about the state on which the measurements are to be performed here: indeed, the phenomenon of contextuality is often said to be *state-independent*.

Collecting the observables present in rows and columns of Table 3.1, one may propose the following expression (Cabello 2008):

$$\left\langle \mathcal{C}_{\mathrm{PM}}^{\mathrm{KS}} \right\rangle = \langle ABC \rangle + \langle abc \rangle + \langle \alpha\beta\gamma \rangle + \langle Aa\alpha \rangle + \langle Bb\beta \rangle - \langle Cc\gamma \rangle \tag{3.15}$$

The reasoning above shows that classically, $\left\langle \mathcal{C}_{\mathrm{PM}}^{\mathrm{KS}} \right\rangle \leq 4$, while in quantum mechanics, $\left\langle \mathcal{C}_{\mathrm{PM}}^{\mathrm{KS}} \right\rangle = 6$ is possible.

However, this inequality suffers from the same issue as before: in a real experiment, perfect compatibility of observables is generally impossible to achieve; hence, there may be spurious violations of the classical bound due to disturbance. But as before, the inequality can be re-ordered to yield

$$\left\langle \mathcal{C}_{\mathrm{PM}}^{\mathrm{NCE}} \right\rangle = \langle ABC \rangle + \langle cab \rangle + \langle \beta\gamma\alpha \rangle + \langle Aa\alpha \rangle + \langle \beta Bb \rangle - \langle c\gamma C \rangle, \tag{3.16}$$

which can be shown to be bounded by 4 for the case of measurement-independent disturbances, and yields a maximum of 6 in quantum mechanics (Szangolies, Kleinmann, and Gühne 2013).

Not all inequalities can be directly modified this way. In certain cases, such as the inequality proposed by Klyachko, Can, Binicioğlu, and Shumovsky (KCBS) (Klyachko et al. 2008), a simple re-ordering is not enough. The original expression

$$\left\langle \mathcal{C}_{\mathrm{KCBS}}^{\mathrm{KS}} \right\rangle = \langle AB \rangle + \langle BC \rangle + \langle CD \rangle + \langle DE \rangle + \langle EA \rangle \tag{3.17}$$

with observables on a qutrit system is classically bounded (from below) by -3, and no re-ordering of observables as above is possible. However, one may introduce an additional term, $\langle AA \rangle$, and then modify the expression to

$$\left\langle \mathcal{C}_{\mathrm{KCBS}}^{\mathrm{NCE}} \right\rangle = \langle AB \rangle + \langle CB \rangle + \langle CD \rangle + \langle DE \rangle + \langle EA \rangle - \langle AA \rangle, \tag{3.18}$$

is classically bounded by -4: to minimize the expression, A_i must equal E_i, while A_j must equal $-E_i$; consequently, $A_i = -A_j$, and thus, $\langle AA \rangle = -1$, yielding the minimum -4. In quantum mechanics, however, a minimum of $4 - 4\sqrt{5}$ can be achieved (Szangolies, Kleinmann, and Gühne 2013).

Finally, an expression can be derived from the intriguing scenario proposed by Yu and Oh (2012), which takes the form (Kleinmann et al. 2012; Zhang et al. 2013)

$$\left\langle \mathcal{C}_{\mathrm{YO}}^{\mathrm{KS}} \right\rangle = \sum_i \Gamma_i \langle A_i \rangle + \sum_{ij} \Gamma_{ij} \langle A_i A_j \rangle, \tag{3.19}$$

where the coefficients Γ_i and Γ_{ij} are as follows:

$$\Gamma_i = \begin{cases} 1 & \forall i \in \{4, 7, 10, \ldots, 13\} \\ 2 & \forall i \in \{1, 5, 6, 8, 9\} \\ 3 & \forall i \in \{2, 3\} \end{cases}$$

$$\Gamma_{ij} = \begin{cases} -1 & \forall (i,j) \in \{(1,2), (1,3), (1,4), (1,7), (4,10), (8,10), (9,10), \\ & (5,11), (7,11), (9,11), (6,12), (7,12), (8,12), (4,13), \\ & (5,13), (6,13)\} \\ -2 & \forall (i,j) \in \{(2,3), (2,5), (2,8), (3,6), (3,9), (5,8), (6,9)\} \\ 0 & \text{else} \end{cases}$$

Classically, this inequality is bounded by 16. Using our method, we obtain the modified expression

$$\left\langle \mathcal{C}_{\mathrm{YO}}^{\mathrm{NCE}} \right\rangle = \sum_i \Gamma_i \langle A_i \rangle + \sum_{ij} \Gamma_{ij} \langle A_i A_j \rangle + 4 \sum_i \langle A_i A_i \rangle, \tag{3.20}$$

which is bounded by 68 for all noncontextually evolving hidden variable theories, while the maximum quantum value is $69 + \frac{1}{3}$ (Szangolies, Kleinmann, and Gühne 2013).

Thus, we have seen that the problematic failure of compatibility in real laboratory experiments can be overcome by generalizing the nondisturbance assumption of Kochen and Specker to the assumption of noncontextual evolution, where the hidden variables are allowed to undergo arbitrary evolution, as long as this evolution does not depend on the measurement context. Since this assumption contains Kochen-Specker noncontextuality in the limit of trivial evolutions, it is thus a proper generalization of the latter, and hence, its experimental implementation serves to exclude a set of hidden-variable theories including the Kochen-Specker noncontextual ones.

3.2 Semidefinite Programming Basics

Before we move on to the next main topic of this thesis, we first need to introduce a tool that has been gaining importance in quantum information theory, namely, *semidefinite programming* (Vandenberghe and Boyd 1996). Semidefinite programming is a subset of *convex optimization* (Boyd and Vandenberghe 2004), that is, the task of minimizing convex functions over convex sets. Many of the problems arising in quantum information theory are of this kind: entanglement distillation (Rains 2001), distinguishing separable and entangled states (Doherty, Parrilo, and Spedalieri 2002), and the unambiguous discrimination of non-orthogonal quantum states (Eldar 2003), to name just a few examples, can be aided by semidefinite methods.

To introduce the semidefinite programming framework, we will start by first recalling some basics of constrained optimization, with a particular focus on the relationship between primal and dual problems. Then, we will discuss the special case of semidefinite problems, and give an outline of the algorithmic methods used to solve them.

3.2.1 Constrained Optimization and Lagrange Duality

For simplicity, we will consider the case of a two-dimensional problem; all definitions straightforwardly generalize to the case of more complex problem spaces. The simplest case is an optimization problem with a single equality constraint:

$$\begin{aligned} \text{minimize:} \quad & f(x,y) \\ \text{subject to:} \quad & g(x,y) = c \end{aligned}$$

Here, the problem is to find a *feasible point* (x, y) such that the function $f(x, y)$ is minimized, given the constraint $g(x, y) = c$. A feasible point (x, y) is any point within the domain of $f(x, y)$ such that $g(x, y) = c$; the *optimal point* (x^*, y^*) is then that element of the set of feasible points such that $f(x, y)$ assumes its minimum p^*. The situation is depicted in Fig. 3.1.

At the optimal point, the constraint lies tangent to a contour of $f(x, y)$. Hence, we must have

$$\nabla f(x, y) = -\mu \nabla g(x, y). \tag{3.21}$$

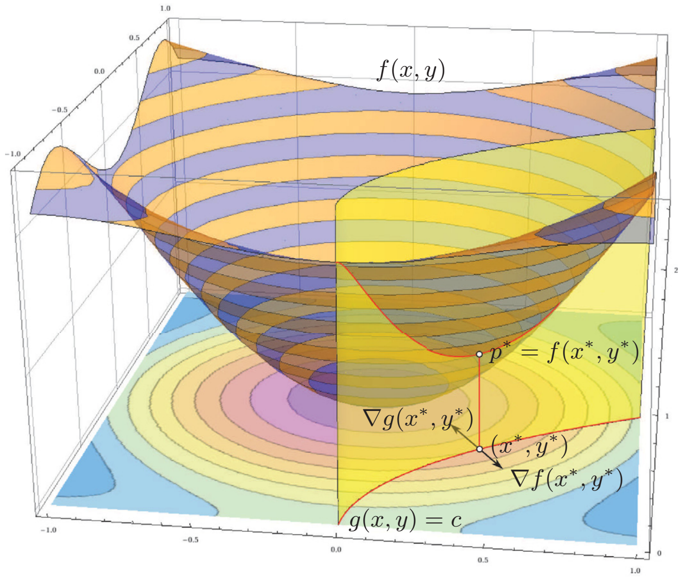


FIGURE 3.1: Plot of the objective function $f(x, y)$ together with its contours and the constraint $g(x, y) = c$. The optimal value lies on the intersection of the yellow surface with the objective function.

We can then define the *Lagrangian*

$$\mathcal{L}(x, y, \mu) = f(x, y) + \mu(c - g(x, y)), \tag{3.22}$$

where μ is a so-called *Lagrange multiplier*. The optimal point (x^*, y^*) is then given by a stationary point (x^*, y^*, μ) of this Lagrangian, that is, a point such that

$$\nabla\mathcal{L}(x, y, \mu) = 0, \tag{3.23}$$

where the gradient now includes partial differentiation with respect to x, y, and μ. This yields three equations with three unknowns, whose solution yields possible optimal points. Whether these candidate solutions are (local) extrema of the objective function can then be decided by computing the magnitude of the gradient.

For the general case, now, we allow problems with n objective variables, that is, objective functions $f(\boldsymbol{x})$ where $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)^T$, together with k equality constraints. These problems are of the form:

$$\begin{array}{ll} \text{minimize:} & f(\boldsymbol{x}) \\ \text{subject to:} & g_i(\boldsymbol{x}) = c_i,\ i \in \{1, \ldots, k\} \end{array}$$

To solve them, we formulate the Lagrangian

$$\mathcal{L}(\boldsymbol{x}, \boldsymbol{\mu}) = f(\boldsymbol{x}) + \sum_{i=1}^{k} \mu_i(c_i - g_i(\boldsymbol{x})), \tag{3.24}$$

where $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_k)$, and then again take the gradient as above.

Using the Lagrangian, we can then define the *dual function*

$$q(\boldsymbol{\mu}) = \inf_{\boldsymbol{x} \in X} \mathcal{L}(\boldsymbol{x}, \boldsymbol{\mu}), \tag{3.25}$$

where X is the domain of $f(\boldsymbol{x})$ (for instance, $\mathbb{R}^n$). This is a function depending only on the Lagrange multipliers, and we can then write the *dual problem* as:

$$\begin{array}{rl} \text{maximize:} & q(\boldsymbol{\mu}) \\ \text{subject to:} & \mu_i \geq 0,\, i \in \{1, \dots, k\} \end{array}$$

For all $\mu \geq 0$, $q(\boldsymbol{\mu}) \leq p^*$; hence, the maximization over $q(\boldsymbol{\mu})$ yields a lower bound for the optimal value of the primal problem. The difference between the optimal dual value d^* and the optimal primal value p^* is called the *duality gap*; if this gap is zero, one speaks of *strong duality*, otherwise, the problem is said to exhibit *weak duality*.

The case where there are, besides the k equality constraints, l inequality constraints can be treated similarly, by means of the *Karush-Kuhn-Tucker conditions* (Karush 1939; Kuhn and Tucker 1951).

3.2.2 Semidefinite Problems

Semidefinite problems form a special and interesting case of the above framework. We now consider only linear objective functions, that is, functions $f(\boldsymbol{x})$ that can be written in the form (following the notation of Vandenberghe and Boyd (1996))

$$f(\boldsymbol{x}) = \boldsymbol{c}^T \boldsymbol{x}, \tag{3.26}$$

where $\boldsymbol{x}, \boldsymbol{c} \in \mathbb{R}^n$ are the variable and the problem vector, respectively. Furthermore, we consider constraints of the form

$$F(\boldsymbol{x}) = F_0 + \sum_i x_i F_i \geq 0, \tag{3.27}$$

where $F_i \in \mathbb{R}^{m \times m}$, $F_i = F_i^T$, and $F(\boldsymbol{x}) \geq 0$ denotes positive semidefiniteness. This problem is called *convex*, since with $F(\boldsymbol{x}) \geq 0$ and $F(\boldsymbol{y}) \geq 0$, it follows that for any $0 \leq \mu \leq 1$

$$F(\mu \boldsymbol{x} + (1-\mu)\boldsymbol{y}) = \mu F(\boldsymbol{x}) + (1-\mu) F(\boldsymbol{y}) \geq 0, \tag{3.28}$$

i.e. the set of feasible points is convex. A schematic representation of such a problem is given in Fig. 3.2.

Roughly, one can interpret a convex optimization as the problem of moving as far as possible in the direction of $-\boldsymbol{c}$, while staying within the feasible set $\{\boldsymbol{x} | F(\boldsymbol{x}) \geq 0\}$. The general problem can then be written as:

$$\begin{array}{rl} \text{minimize:} & \boldsymbol{c}^T \boldsymbol{x} \\ \text{subject to:} & F(\boldsymbol{x}) = F_0 + \sum_i x_i F_i \geq 0,\, i \in 1, \dots, k \end{array}$$

From the primal problem, one can again derive the dual problem (for details, see (Boyd and Vandenberghe 2004))

$$\begin{array}{rl} \text{maximize:} & -\mathrm{tr}\,(F_0 Z) \\ \text{subject to:} & \mathrm{tr}\,(F_i Z) = c_i,\, i \in 1, \dots, k \\ & Z \geq 0, \end{array}$$

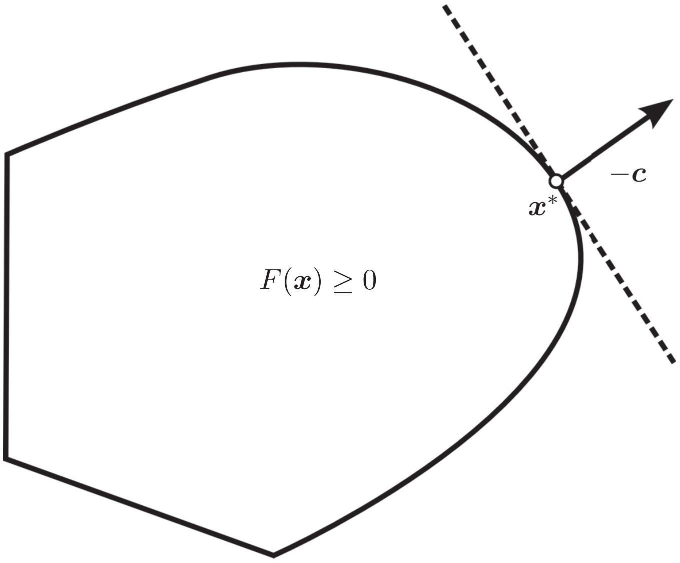


FIGURE 3.2: Schematic representation of a convex optimization problem.

where $Z \in \mathbb{R}^{m\times m}$ and $Z = Z^T$. It is straightforward to see that this dual indeed yields a lower bound on the primal problem, i.e. that $\boldsymbol{c}^T\boldsymbol{x} \geq -\mathrm{tr}\,(F_0 Z)$ for all feasible points $\boldsymbol{x}$ and Z. In general, for feasible $\boldsymbol{x}$ and Z, one has

$$\mathrm{tr}\,(ZF(\boldsymbol{x})) \geq 0, \tag{3.29}$$

since Z and $F(\boldsymbol{x})$ are both positive semidefinite. Using the constraints $\mathrm{tr}\,(F_i Z) = c_i$, this yields

$$0 \leq \mathrm{tr}\,(ZF(\boldsymbol{x})) = \mathrm{tr}\,(F_0 Z) + \sum_i \mathrm{tr}\,(ZF_i x_i) = \mathrm{tr}\,(F_0 Z) + \boldsymbol{c}^T\boldsymbol{x}. \tag{3.30}$$

Thus, for all feasible $\boldsymbol{x}$ and Z, we have

$$-\mathrm{tr}\,(F_0 Z) \leq \boldsymbol{c}^T\boldsymbol{x}. \tag{3.31}$$

In particular, this holds for the optimal value p^* of the primal, i.e.

$$-\mathrm{tr}\,(F_0 Z) \leq p^*. \tag{3.32}$$

Likewise, we have for the optimal value d^* of the dual that

$$d^* \leq \boldsymbol{c}^T\boldsymbol{x}. \tag{3.33}$$

Consequently, we have that $d^* \leq p^*$.

An advantage of the semidefinite programming framework is that strict conditions for *strong duality*, i.e. $p^* = d^*$, are known. Consider thus the optimal sets of the primal and dual programs,

$$\begin{aligned} X_{\mathrm{opt}} &= \{\boldsymbol{x}|F(\boldsymbol{x}) \geq 0,\, \boldsymbol{c}^T\boldsymbol{x} = p^*\} \\ Z_{\mathrm{opt}} &= \{T|Z \geq 0, \mathrm{tr}\,(F_i Z) = c_i,\, -\mathrm{tr}\,(F_0 Z) = d^*\}. \end{aligned} \tag{3.34}$$

If either of the following conditions hold, we have $p^* = d^*$:

1. The primal program is strictly feasible, i.e. there exists $\boldsymbol{x}$ with $F(\boldsymbol{x}) \geq 0$.
2. The dual program is strictly feasible, i.e. there exists $Z = Z^T \geq 0$ with $\operatorname{tr}(F_i Z) = c_i$.

If both conditions hold, both sets in Eq. 3.34 are nonempty.

This result is known as the *strong duality theorem*. A proof can be found, e.g., in (Rockafellar 2015).

3.2.3 Interior Point Methods

Another advantage of semidefinite programming is the fact that there exists effective numerical methods to find (arbitrarily close to) optimal solutions. In the following, we will only consider the case in which both conditions for strong duality hold, and hence, $d^* = p^*$. Then, the solution to a semidefinite problem can be found using *interior-point methods*, whose basic idea is to iteratively find candidate solutions $\boldsymbol{x}^{(k)}$ and $Z^{(k)}$ such that the duality gap is strictly decreasing, that is

$$\boldsymbol{c}^T \boldsymbol{x}^{(k)} + \operatorname{tr}\left(F_0 Z^{(k)}\right) > \boldsymbol{c}^T \boldsymbol{x}^{(k+1)} + \operatorname{tr}\left(F_0 Z^{(k+1)}\right). \tag{3.35}$$

Once the duality gap is smaller than some pre-defined tolerance ε, the algorithm terminates with a solution approximating the optimal point to the desired degree of accuracy. Such methods solve both the primal and dual problem, and are hence also referred to as *primal-dual methods*. The benefit of these methods compared to simply solving either the primal or dual on its own is that one may use information from the dual (i.e. $Z^{(k)}$) to find a good update for the primal variable $\boldsymbol{x}^{(k)}$ (Vandenberghe and Boyd 1996).

In the following, we briefly discuss the motivation behind one of the most common interior-point algorithms, the *central path following algorithm*. First, we define the *barrier function*

$$\phi(\boldsymbol{x}) = \begin{cases} \log \det F(\boldsymbol{x})^{-1} & \text{if } F(\boldsymbol{x}) > 0 \\ \infty & \text{otherwise,} \end{cases} \tag{3.36}$$

which can be thought of as a strongly repulsive potential diverging to infinity at the boundary of the feasible set $\{\boldsymbol{x} | F(\boldsymbol{x}) > 0\}$. The minimum of this barrier function yields the *analytic center*

$$\boldsymbol{x}^c = \operatorname{argmin} \phi(\boldsymbol{x}). \tag{3.37}$$

The analytic center of a linear matrix inequality $F(\boldsymbol{x}) \geq 0$ can be computed using the Newton method (Vandenberghe and Boyd 1996).

We can use the notion of analytic center to parametrize a curve through the feasible set, whose endpoint will yield the optimal value of the optimization problem. To do so, consider

$$\begin{aligned} \text{minimize:} \quad & \log \det F(\boldsymbol{x})^{-1} \\ \text{subject to:} \quad & F(x) > 0 \\ & \boldsymbol{c}^T \boldsymbol{x} = \gamma, \end{aligned}$$

where again the analytic center is the argument $\boldsymbol{x}^c$ minimizing the objective function. This essentially corresponds to calculating the minimum of the objective function that lies on a constraint surface $\boldsymbol{c}^T\boldsymbol{x} = \gamma$, where $p^* \leq \gamma \leq \bar{p} = \sup\{\boldsymbol{c}^T\boldsymbol{x}|F(\boldsymbol{x}) < 0\}$. This yields a path parametrized by γ through the feasible set, the so-called *central path* (see Fig. 3.3).

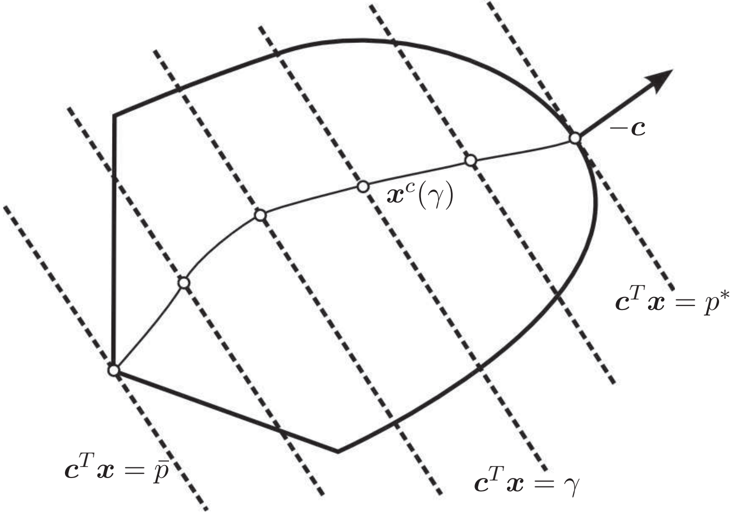

$-\boldsymbol{c}$
$\boldsymbol{x}^c(\gamma)$
$\boldsymbol{c}^T\boldsymbol{x} = p^*$
$\boldsymbol{c}^T\boldsymbol{x} = \bar{p}$
$\boldsymbol{c}^T\boldsymbol{x} = \gamma$

FIGURE 3.3: The central path is given by the minimum of the barrier function $\phi(\boldsymbol{x})$ intersecting the level surfaces of the constraint $\boldsymbol{c}^T\boldsymbol{x} = \gamma$, with $\gamma \in [p^*, \bar{p}]$.

The most common strategy to solve a semidefinite problem then is to choose points that lie either on, or close to, the central path. One possibility is, for instance, to introduce a measure of deviation from the central path,

$$\psi(\boldsymbol{x}) = \log\det F(\boldsymbol{x})^{-1} - \log\det F(\boldsymbol{x}^c(\boldsymbol{c}^T\boldsymbol{x}))^{-1}, \tag{3.38}$$

and keep this below a certain tolerance whenever choosing a new candidate optimal point.

In these algorithms, the most computationally expensive step is in general choosing the next candidate point, as the Newton method for finding the analytic center includes a least-squares problem in a large number of variables (Vandenberghe and Boyd 1996).

In order to implement semidefinite programming methods in this thesis, use was made of the freely available MATLAB-toolboxes YALMIP (Löfberg 2004) and SDPT3 (Toh, Todd, and Tütüncü 1999).

3.3 Random Measurements to Witness Entanglement

Having now availed us of the tool of semidefinite programming, we proceed to present the second main result of this thesis, namely, a procedure for detecting the entanglement of arbitrary (and unknown) quantum states ρ (Szangolies, Kampermann, and Bruß 2015).

The tool we use to approach this problem are the so-called entanglement witnesses, as briefy introduced at the beginning of this chapter. In general, detecting entanglement of an unknown state using such a witness is a hard task (Žnidarič et al. 2007). However, as we will show, it is possible to devise a protocol in which two parties carry out measurements, and then check, via a semidefinite program, whether a witness detecting the unknown state can be constructed from these measurements, in such a way that the number of measurements that have to be carried out is significantly smaller on average than the number of measurements needed, e.g., to reconstruct the full state, and then compute its entanglement.

3.3.1 Entanglement Witnesses

We first introduce entanglement witnesses and the concepts needed in the remainder of this section. As briefly mentioned, an entanglement witness W (Lewenstein et al. 2000; Terhal 2000) is a (Hermitian) operator such that

$$\mathrm{tr}\,(W\rho) \begin{cases} \geq 0 & \text{if } \rho \text{ is separable,} \\ < 0 & \text{for at least one entangled } \rho. \end{cases} \tag{3.39}$$

Thus, a negative expectation value of W certifies the presence of entanglement. The existence of witness operators follows from the *Hahn-Banach theorem* (see, e.g., (Hirzebruch and Scharlau 1971)): if there are two convex disjoint subsets S_1 and S_2 of a Banach space at least one of which is compact, then there always exists a bounded functional f separating them. Here, a Banach space simply is a vector space equipped with a norm, together with the completeness requirement that the limit of every Cauchy sequence of vectors lies within the space. In particular, all Hilbert spaces with the norm induced by the scalar product are examples of Banach spaces, as is the space of trace-class operators acting on a Hilbert space.

Now, take an arbitrary separable state ρ on some Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Such a state can always be written in the form

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i. \tag{3.40}$$

Hence, the separable states are the convex hull of the product states, i.e. states of the form $\rho_{AB} = \rho_A \otimes \rho_B$. As now any entangled state ρ_{ent} lies outside of this set, it follows immediately from the Hahn-Banach theorem that there must exist a bounded functional separating this state from the set of separable states, which we can identify with a Hermitian operator W.

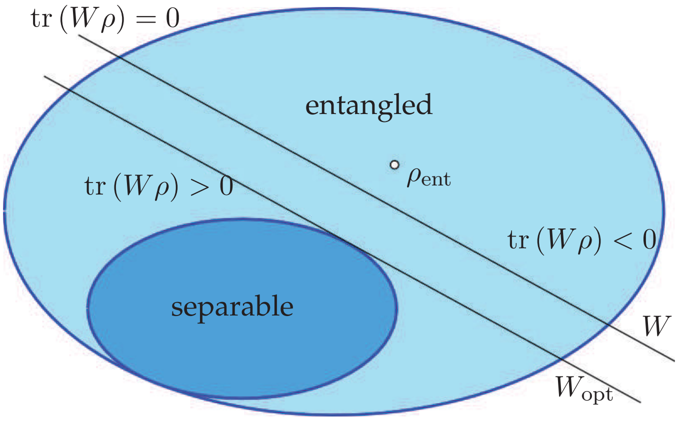
In fact, in general, there will exist more than one such witness operator. Let us introduce the *range* of a witness W as

$$R(W) = \{\rho | \mathrm{tr}\,(W\rho) < 0\}, \tag{3.41}$$

i.e. as the set of states that are detected by a given witness. Then, a witness W_2 is said to be *finer* than W_1 if $R(W_1) \subset R(W_2)$, that is, if W_2 detects all the states W_1 detects, and at least one additional state. We call a witness W_{opt} *optimal* if there is no finer witness detecting the same states. In this case, the witness directly bounds the set of separable states (see Fig. 3.4).

We will mostly be concerned with a special kind of witness, the so-called *decomposable witnesses*. A witness W is decomposable if it can be written as (Woronowicz 1976)

$$W = P + Q^{T_A}, \tag{3.42}$$



$\mathrm{tr}\,(W\rho) = 0$
entangled
ρ_{ent}
$\mathrm{tr}\,(W\rho) > 0$
$\mathrm{tr}\,(W\rho) < 0$
separable
W
W_{opt}

FIGURE 3.4: The set of separable states forms a convex subset within the set of quantum states. Witnesses can be understood as (affine) hyperplanes separating the set of states into detected entangled states and separable and undetected entangled states.

where P and Q are both positive semidefinite operators, and ^{T_A} denotes partial transposition with respect to subsystem A, i.e. the operation

$$A = \sum_{ijkl} a^{ij}_{kl} \left|i\right\rangle\!\left\langle j\right| \otimes \left|k\right\rangle\!\left\langle l\right| \rightarrow A^{T_A} = \sum_{ijkl} a^{ij}_{kl} \left|j\right\rangle\!\left\langle i\right| \otimes \left|k\right\rangle\!\left\langle l\right| . \tag{3.43}$$

To understand these particular witnesses, we first need to introduce the *partial transpose criterion*, which can be used to decide entanglement of a quantum state.

The partial transpose, PPT (for positive partial transpose), or Peres-Horodecki criterion (M. Horodecki, P. Horodecki, and R. Horodecki 1996; Peres 1996) provides a sufficient criterion for entanglement, that is also necessary in the case of 2 × 2 and 2 × 3-dimensional Hilbert spaces.

Consider any separable state

$$\rho_{AB} = \sum_i p_i \rho^i_A \otimes \rho^i_B. \tag{3.44}$$

Its partial transpose is

$$\rho^{T_A}_{AB} = \sum_i p_i (\rho^i_A)^T \otimes \rho^i_B, \tag{3.45}$$

i.e. the local components ρ^i_A are transposed individually. However, the transposition does not change the spectrum of an operator; thus, for all separable states, the spectrum of ρ_{AB} and $\rho^{T_A}_{AB}$ must be the same. In particular, both must be positive operators.

Thus, whenever we act on a state with the partial transpose, and find a nonpositive result—that is, the partial transpose has at least one negative eigenvalue in its spectrum—we know that this state cannot be separable. In fact, in dimensions 2 × 2 and 2 × 3, one finds that all entangled states lead to a nonpositive partial transpose, while in higher dimensions, entangled states having positive partial transpose (so-called *PPT entangled states*) exist (M. Horodecki, P. Horodecki, and R. Horodecki 1996).

Consider now a positive semidefinite operator Q. It holds that

$$\operatorname{tr}\left(Q^{T_A}\rho\right) = \operatorname{tr}\left(Q\rho^{T_A}\right), \tag{3.46}$$

and consequently, $\operatorname{tr}\left(Q^{T_A}\rho\right)$ may be negative, provided ρ^{T_A} is a nonpositive operator. Thus, if we obtain a negative expectation value upon measuring Q^{T_A}, we may conclude that the state ρ must be entangled—Q^{T_A} is an entanglement witness based on the PPT-criterion. To obtain the most general such witness, note that we can add an arbitrary positive operator P to obtain

$$\operatorname{tr}\left(\left[P + Q^{T_A}\right]\rho\right) = \operatorname{tr}\left(P\rho\right) + \operatorname{tr}\left(Q^{T_A}\rho\right), \tag{3.47}$$

where the first term in the sum is positive (or zero) for all ρ, while the second term may become negative for some entangled states. Hence, an operator of the form

$$W = P + Q^{T_A} \tag{3.48}$$

is the most general witness detecting states with nonpositive partial transpose.

Entanglement witnesses typically need to be tailored to the states they are intended to detect. For instance, consider a state ρ_{NPT} which has a negative partial transpose. Then, if $|\psi_-\rangle$ is the eigenvector of $\rho_{\mathrm{NPT}}^{T_A}$ to the negative eigenvalue λ_-, the operator

$$W = |\psi_-\rangle\langle\psi_-|^{T_A} \tag{3.49}$$

is an entanglement witness for the state ρ_{NPT}. Likewise, for any entangled pure state $|\psi_{\mathrm{ent}}\rangle$, one may take

$$W = \alpha\mathbb{1} - |\psi_{\mathrm{ent}}\rangle\langle\psi_{\mathrm{ent}}|, \tag{3.50}$$

where α can be computed as the maximal overlap of $|\psi_{\mathrm{ent}}\rangle$ with a separable state, that is,

$$\alpha = \max_{\rho_{\mathrm{sep}}} \operatorname{tr}\left(|\psi_{\mathrm{ent}}\rangle\langle\psi_{\mathrm{ent}}|\,\rho_{\mathrm{sep}}\right) = \max_{|\phi\rangle=|\phi_A\rangle\otimes|\phi_B\rangle} |\langle\psi_{\mathrm{ent}}|\phi\rangle|^2. \tag{3.51}$$

This maximum can be effectively computed by means of the Schmidt decomposition (Bourennane et al. 2004).

However, this has the disadvantage of necessitating prior knowledge of the state one wants to detect, and even then, if one uses a non-optimal witness, a noisy preparation may still lead to a failure of detecting the state, even though it is entangled. To see this, consider the Bell state $|\Psi^-\rangle$ (see Eq. 1.67), and the operator

$$W_{|\Psi^-\rangle} = \frac{2}{3}\mathbb{1} - \left|\Psi^-\right\rangle\!\left\langle\Psi^-\right|. \tag{3.52}$$

Since the maximal overlap of $|\Psi^-\rangle$ with the separable states is

$$\operatorname{tr}\left(\left|\Psi^-\right\rangle\!\left\langle\Psi^-\right|\rho_{\mathrm{sep}}\right) = \frac{1}{2}, \tag{3.53}$$

the operator yields a positive expectation value on all separable states, but

$$\mathrm{tr}\left(W_{|\Psi^-\rangle}\left|\Psi^-\middle\rangle\middle\langle\Psi^-\right|\right) = -\frac{1}{3}. \tag{3.54}$$

Hence, it is an entanglement witness detecting $|\Psi^-\rangle$.

Now assume that we have an imperfect preparation procedure yielding, due to the addition of white noise, instead the so-called *Werner state* (Werner 1989)

$$\rho_W = p\left|\Psi^-\middle\rangle\middle\langle\Psi^-\right| + \frac{1-p}{4}\mathbb{1}, \tag{3.55}$$

which is entangled for $p > \frac{1}{3}$. The expectation value of W given this state is

$$\mathrm{tr}\left(W_{|\Psi^-\rangle}\rho_W\right) = \frac{5-9p}{12}. \tag{3.56}$$

Thus, states with $\frac{1}{3} < p \leq \frac{5}{9}$ will not be detected by the witness, even though they are entangled. Hence, the unavoidable presence of noise in every real experiment may spoil an effort to detect entanglement, even though it is in fact present.

In a case such as this, of course, the problem can be avoided by simply using the optimal witness for the state $|\Psi^-\rangle$. However, this may no longer be the case for other preparation failures. Consider the optimal witness

$$W^{\mathrm{opt}}_{|\Psi^-\rangle} = \frac{1}{2}\mathbb{1} - \left|\Psi^-\middle\rangle\middle\langle\Psi^-\right|, \tag{3.57}$$

and a source that produces the mixture

$$\rho_M = p\left|\Psi^-\middle\rangle\middle\langle\Psi^-\right| + (1-p)\left|\Phi^-\middle\rangle\middle\langle\Phi^-\right|. \tag{3.58}$$

This state is separable only for $p = \frac{1}{2}$; however, the witness $W^{\mathrm{opt}}_{|\Psi^-\rangle}$ is only able to detect its entanglement in the regime $p > \frac{1}{2}$. Hence, even though the state ρ_M may be suitable for certain entanglement-based quantum information tasks, a test based on the witness $W^{\mathrm{opt}}_{|\Psi^-\rangle}$ may lead to the rejection of the source producing it as a viable device.

Thus, it would be interesting to have an efficient procedure capable of detecting entanglement in *arbitrary* states, should any entanglement be present. We now proceed to describe such a procedure.

3.3.2 Random States and Random Witnesses

If we have no knowledge about the state ρ we wish to detect, there is no way to choose an appropriate witness a priori. One approach then might be to simply choose a witness randomly, and attempt detection.

In order to gauge whether this might be an appropriate method, we first need to specify what exactly we mean by choosing a witness (or, more generally, a Hermitian operator) 'randomly'; likewise, in order to quantify its performance on random quantum states, we need to give a procedure for drawing a quantum state randomly. First, we need an appropriate probability measure. A requirement on such a measure is *translational invariance*:

if we look at integrals over $\mathbb{R}$, we have

$$\int_{\mathbb{R}} f(x)\,\mathrm{d}x = \int_{\mathbb{R}} f(x+a)\,\mathrm{d}x. \tag{3.59}$$

Note now that $(\mathbb{R}, +)$, that is, the real numbers equipped with the addition operation, forms a group. Hence, for our measure μ, we require that for arbitrary elements g of some group G, it holds that

$$\int_G f(x)\,\mathrm{d}\mu(x) = \int_G f(gx)\,\mathrm{d}\mu(x), \tag{3.60}$$

where we have now indicated the group operation simply by juxtaposition.

A measure μ is called *Haar measure* (Haar 1933) if it satisfies

$$\mu(gS) = \mu(Sg) = \mu(S), \tag{3.61}$$

with

$$\mu(S) = \int_{g\in S} \mathrm{d}\mu(g), \tag{3.62}$$

for arbitrary $S \subseteq G$ and $g \in G$. In addition, if $\mu(G) = 1$, then μ is a *probability measure* on G. Thus, we can define the probability of S, given a probability density function f such that $\mathrm{d}\mu(g) = f(g)\,\mathrm{d}g$ as

$$\mu(S) = \int_{g\in S} \mathrm{d}\mu(g) = \int_{g\in S} f(g)\,\mathrm{d}g. \tag{3.63}$$

This definition can now be applied to the groups of interest to us, which are the unitary groups $U(n)$. To build intuition, it may be helpful to consider the simple case $U(1)$. Any given element $U \in U(1)$ has the form $U = e^{i\phi}$. The measure $\mathrm{d}\mu(U) = \mathrm{d}\phi$ then measures the perimeter of the unit circle, and it holds that $\mathrm{d}\phi + \phi_0 = \mathrm{d}\phi$, for any fixed ϕ_0. Alternatively, this can be written as $\mathrm{d}\mu(UU_0) = \mathrm{d}\mu(U)$, with $U_0 = e^{i\phi_0}$, which yields the required translational invariance in Eq. 3.61. Hence, generalization to $U(n)$ follows from taking U and U_0 from $U(n)$.

One should, however, be careful not to generalize the intuition gained from the simple case of $U(1)$—whose group manifold is simply the unit circle $\mathbb{S}^1$—too hastily. For instance, in the case of $SO(3)$, the group of rotations in three dimensions, whose group manifold is the unit sphere $\mathbb{S}_2$, naively drawing the angles θ and ϕ at random will fail to yield a uniformly distributed direction—rather, the points picked this way will tend to 'bunch' at the poles. The reason for this is that the measure in this case, $\sin(\theta)\,\mathrm{d}\theta\,\mathrm{d}\phi = \mathrm{d}\cos(\theta)\,\mathrm{d}\phi$ is a function of θ. Thus, one needs to draw values for $t = \cos(\theta)$ from the interval $[-1, 1]$, calculating $\theta = \arccos(t)$, and draw ϕ from $[0, 2\pi]$.

This gives us now a method for choosing random unitary matrices—we simply sample a distribution that is uniform with respect to the Haar measure. For $U(1)$, this amounts to choosing a random phase $\phi \in [0, 2\pi]$. For $n > 1$, a convenient method to draw Haar-random unitaries is to first create a matrix with uniformly random, bounded complex entries, and then to diagonalize it using the Gram-Schmidt method. This can be shown to guarantee Haar-randomness (Mezzadri 2007).

Using this method, we can thus effectively generate random unitary matrices. Since the rows and columns of an $n \times n$ unitary matrix form a basis of an n-dimensional Hilbert space, extracting a column from such a random unitary yields a random pure state. For random mixed states, if the dimension of the pure state generated this way is $n = k \times l$, we trace out the k-dimensional environment, yielding an l-dimensional mixed state randomly distributed according to the measure (Życzkowski, Penson, et al. 2011)

$$\mathrm{d}\mu(\rho) \propto \Theta(\rho)\delta(\mathrm{tr}\,(\rho) - 1)\mathrm{det}\rho^{k-n}, \tag{3.64}$$

where the Θ-function enforces positivity, and the dirac δ guarantees the normalization.

Finally, a random (normalized) Hermitian operator H can be produced by first generating a diagonal matrix D with uniformly distributed random real entries, then drawing a random unitary U according to the process outlined above, and forming

$$H = \frac{UDU^\dagger}{\mathrm{tr}\,(UDU^\dagger)}. \tag{3.65}$$

Now having a method of randomly drawing Hermitian operators, and thus, observables, we need to check whether a given operator W actually is an entanglement witness. The first check involves the spectrum of W: if W is either positive- or negative-definite, then W cannot possibly be an entanglement witness, as, per Eq. 3.39, W must have positive expectation value on separable states, but yield a negative value for at least one entangled state. Hence, any prospective witness operator must be indefinite.

Furthermore, an easy to check condition is whether W's partial transpose is positive. Since for any separable state ρ_{sep}, $\rho_{\mathrm{sep}}^{T_A}$ is again a separable density operator, we can find ρ'_{sep} such that $\rho'^{T_A}_{\mathrm{sep}} = \rho_{\mathrm{sep}}$, and hence, if $W^{T_A} \geq 0$, we have

$$\mathrm{tr}\,(W\rho_{\mathrm{sep}}) = \mathrm{tr}\left(W\rho'^{T_A}_{\mathrm{sep}}\right) = \mathrm{tr}\left(W^{T_A}\rho'_{\mathrm{sep}}\right) \geq 0, \tag{3.66}$$

and consequently, the expectation value of W is nonegative on all separable states. Since W however is an indefinite operator, there must exist at least one state such that W yields a negative expectation value, which cannot be separable and hence, must be entangled. Thus, the conditions of indefiniteness and positivity of the partial transpose suffice to identify W as a witness.

There are, however, witnesses that cannot be found in this way, due to the fact that there exist entangled states with a positive partial transpose in all Hilbert spaces of dimension greater than 2×3. These additional witnesses can be found using an overlap minimization algorithm, based on the one presented in (Kampermann et al. 2012).

The goal of the algorithm is to calculate the quantity

$$\min_{|\psi\rangle = |a\rangle|b\rangle} \mathrm{tr}\,(W\,|\psi\rangle\!\langle\psi|)\,, \tag{3.67}$$

i.e. the minimal expectation value of W on a separable pure state.

This is done using the following iterative procedure. First, a starting state $|b_0\rangle$ is chosen, and with it, the quantity

$$X_A = \mathrm{tr}_B(W\mathbb{1} \otimes |b_0\rangle\langle b_0|) \tag{3.68}$$

is calculated. Then, the eigenvector $|a_0\rangle$ to the smallest eigenvalue of X_A is chosen for the calculation of

$$X_B = \mathrm{tr}_B(W\,|a_0\rangle\langle a_0| \otimes \mathbb{1}). \tag{3.69}$$

The procedure is now iterated, with in the next step $|b_1\rangle$ being the eigenvector to the smallest eigenvalue of X_B, and so on.

In each step, the overlap $\mathrm{tr}\,(W\,|\psi_i\rangle\langle\psi_i|)$, with $|\psi_i\rangle = |a_i\rangle \otimes |b_i\rangle$, is calculated; if it is found to be negative, the procedure is terminated, as W is not an entanglement witness. Otherwise, the algorithm terminates if either a fixed number of iterations has been performed, or the difference between expectation values of W on successive states $|\psi_{i-1}\rangle$ and $|\psi_i\rangle$ differs by less than a predefined amount.

Note that, however, only the negative result of this iteration procedure is fully conclusive: even if no negative overlap with a separable state is found using the above procedure, this does not strictly imply that W is a witness, as the algorithm is not guaranteed to reach the global minimum in general. In order to increase the confidence in having found the global optimum, the procedure is repeated 10^3 times with different initial conditions.

We can now use these methods to quantify the chances of detecting a random state by measuring a random witness operator. The results of this are discouraging: among 10^5 candidate operators on a two-qubit Hilbert space, a fraction of $1.73 \pm 0.05\%$, where the uncertainty is due to finite statistics, were identified as witnesses via their positive partial transpose; a further $1.34 \pm 0.04\%$ were found using the overlap-minimization procedure. Furthermore, these witnesses are not typically very effective: even for maximally entangled states, only a fraction of $(1.094 \pm 0.007) \cdot 10^{-2}$ were detected using witnesses with positive partial transpose, while operators found using the overlap-minimization process detected $(1.092 \pm 0.008) \cdot 10^{-2}$ of all generated states. For general entangled states, the effectiveness is much lower, on the order of 10^{-5} (Szangolies, Kampermann, and Bruß 2015).

Hence, using the simple method of merely randomly measuring witnesses is not a feasible strategy to detect the entanglement of arbitrary states. However, there exists a better method, which rests on carrying out local measurements on a joint Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, and then using a semidefinite program to determine the best possible witness that can be generated using these measurements, and the observed experimental data. We discuss this method in the following.

3.3.3 Random States and Observables

In general, in order to measure an operator W on a joint Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, it has to be decomposed into local measurements on the subspaces $\mathcal{H}_A$ and $\mathcal{H}_B$, preferrably using some local basis that is simple to implement experimentally. For instance, the witness $W^{\mathrm{opt}}_{|\Psi^-\rangle}$ can be decomposed as

$$W^{\text{opt}}_{|\Psi^-\rangle} = \frac{1}{2}\mathbb{1} - |\Psi^-\rangle\langle\Psi^-| \\ = \frac{1}{4}(\mathbb{1} + \sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z). \tag{3.70}$$

Our approach now is, instead of starting with a witness $W \in \mathcal{B}(\mathcal{H}_{AB})$, to start with local observables $A_i \in \mathcal{B}(\mathcal{H}_A)$ and $B_j \in \mathcal{B}(\mathcal{H}_B)$, and then attempt to find a combination

$$W = \sum_{ij} c_{ij} A_i \otimes B_j, \tag{3.71}$$

such that W is a witness operator detecting the unknown state ρ. For the remainder of this chapter, we will exclusively consider the case of decomposable witnesses, that is, witnesses that can be written in the form of Eq. 3.42.

Thus, our task is now to find of coefficients c_{ij}, given the operators A_i, B_j, and their expectation values (as approximated via measurement) $\langle A_i \otimes B_j \rangle$, such that the operator formed according to Eq. 3.71 is a decomposable witness with minimal expectation value. If this expectation value then is negative, we have detected the entanglement of our unknown state.

We can collect the coefficients c_{ij} into a vector $\boldsymbol{c}$, and likewise, the expectation values into a vector $\boldsymbol{m}$. Consequently, the expectation value of the prospective witness can be written as

$$\langle W \rangle = \sum_{ij} c_{ij} \langle A_i \otimes B_j \rangle \\ = \boldsymbol{m}^T \boldsymbol{c}. \tag{3.72}$$

Then, the problem of finding a suitable witness can be cast into the form of a semidefinite program (see Sec. 3.2.2)

$$\begin{aligned} \text{minimize:}\quad & \boldsymbol{m}^T \boldsymbol{c} \\ \text{subject to:}\quad & W = \textstyle\sum_{ij} c_{ij} A_i \otimes B_j \\ & W = P + Q^{T_A} \\ & P \geq 0 \\ & Q \geq 0 \\ & \operatorname{tr}(W) = 1. \end{aligned}$$

Here, the trace constraint is merely to ensure normalization of the witness. The reason for this is that traceless operators cannot be witnesses: the expectation value of any traceless operator with the maximally mixed state vanishes. Hence, the hyperplane associated to a traceless operator necessarily contains the maximally mixed state. However, there always is a finite ball of separable states around the maximally mixed state, and consequently, this operator must have both positive and negative eigenvalues with at least some separable states, and hence, cannot be a witness.

If this program yields a negative optimal value, we know with certainty that the state ρ, which gave rise to the values $\langle A_i \otimes B_j \rangle$, must have been entangled.

There now remains the question of the effectiveness of this method. Clearly, if the number of measurements that have to be performed is not significantly smaller than the number of measurements needed to fully characterize the state, we have not gained much. In order to characterize a state of dimension $d = d_A \times d_B$, where d_A is the dimension of $\mathcal{H}_A$ (and analogously for d_B), one needs in total $(d_A^2 - 1) \cdot (d_B^2 - 1)$ measurements. Thus, this value yields an upper bound for our method, since having tomographically complete information about a state clearly suffices to decide its entanglement content.

3.3.4 Evaluation of the Method

Given the previous considerations, we need to evaluate the chances of success of our method. The simplest way to do so is to simulate enough experiments in order to gather meaningful statistics, and then to compute the average number of measurements needed in order to detect a state of a given entanglement content.

To do this, we first need a way to measure the entanglement content of a quantum state ρ. That is, we need a suitable *entanglement measure $E(\rho)$*, whose value yields information about, roughly, the 'amount' of entanglement in a given state. Such a measure must satisfy a number of conditions (Vedral et al. 1997):

1. First of all, it should vanish on all separable states, that is, $E(\rho_{\text{sep}}) = 0$ for all separable states ρ_{sep}.

2. Furthermore, it should be invariant under operations that do not change the entanglement content of the state. Operations of this type amount to a local change of basis, implemented by local unitary operations, i.e., for a state acting on a bipartite Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$,
$$E(\rho) = E(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger), \tag{3.73}$$
where U_A and U_B are unitary.

3. Entanglement cannot be created via local operations, together with classical communication between the parties sharing a state (LOCC). Thus, any entanglement measure should be nonincreasing under any map Λ^{LOCC} that can be implemented in this way:
$$E(\rho) \geq E\left(\Lambda^{LOCC}(\rho)\right) \tag{3.74}$$

4. Furthermore, it is often demanded that entanglement measures need to be convex, that is, that they should be nonincreasing under mixture:
$$\sum_i p_i E(\rho_i) \geq E\left(\sum_i p_i \rho_i\right). \tag{3.75}$$
This indicates that, if we have an ensemble of states ρ_i, and loose information about which state is present, entanglement should not increase.

An appropriate entanglement measure for our purposes is the so-called *negativity* (Vidal and Werner 2002; Życzkowski, P. Horodecki, et al. 1998). Essentially, the negativity measures the violation of the PPT-criterion (see

Eq. 3.45 and the discussion following it):

$$\mathcal{N}(\rho) = \frac{||\rho^{T_A}||_1 - 1}{2}, \tag{3.76}$$

where $||X||_1 = \operatorname{tr}\left(\sqrt{XX^\dagger}\right)$ denotes the trace norm. Equivalently, the negativity can be computed as

$$\mathcal{N}(\rho) = \sum_i \frac{|\lambda_i| - \lambda_i}{2}, \tag{3.77}$$

where the λ_i are the negative eigenvalues of ρ. Occasionally, also the *logarithmic negativity*

$$\mathcal{N}_L(\rho) = \log_2 ||\rho^{T_A}||_1 \tag{3.78}$$

is used, which has the advantage of making the measure additive—that is, for n copies of the state ρ, we have that $\mathcal{N}_L(\rho^{\otimes n}) = n\mathcal{N}_L(\rho)$. However, this measure no longer is convex (Plenio 2005).

Due to the fact that the negativity is constructed from the PPT-criterion, it fails to detect entangled states whose partial transpose is positive. However, as we only consider decomposable witnesses, this is not a restriction in our case. In fact, there is a close connection between the negativity and optimal decomposable witness, in that their expectation value exactly yields the value of the negativity (Jungnitsch, Moroder, and Gühne 2011). Thus, the witnesses constructed by our process automatically yield a lower bound to the negativity of the state that is being examined.

We now proceed as follows. First, a random state ρ is drawn according to the discussion in Sec. 3.3.2. Then, the expectation value of this state with (again randomly drawn) measurements A_i and B_j is computed. Since one needs at least two distinct local measurements for the detection of entanglement (Tóth and Gühne 2005), in the first round, we calculate two expectation values $\langle A_i \otimes B_j \rangle$. Then, these expectation values and the measurements that were performed are fed into our SDP. If the SDP produces a negative optimal value, we have detected the entanglement of the state ρ, and the procedure stops; otherwise, one or more new random measurement(s) are added, and the process is repeated, until either a detection is achieved, or we reach the tomographic limit.

There are several possible strategies for the addition of new measurements:

1. At each step, a new measurement is added on either $\mathcal{H}_A$ or $\mathcal{H}_B$, followed by measuring all combinations of measurements in the pool so far.

2. A new measurement is added on both sides. Thus, at the k-th iteration step, we have the expectation values of $\{A_i \otimes B_i\}_{i=1}^k$.

3. A new measurement is added alternatively on $\mathcal{H}_A$ or $\mathcal{H}_B$, while the other side simply continues their measurement. This yields a succession of measurements of the form $A_1 \otimes B_1 \to A_1 \otimes B_2 \to A_2 \otimes B_2 \to \ldots$

Since the second strategy already enables detection in the second round, this is the one we will use in the following. First, we test the method on 10^5 random 2×2-dimensional states. The results are shown in Fig. 3.5.

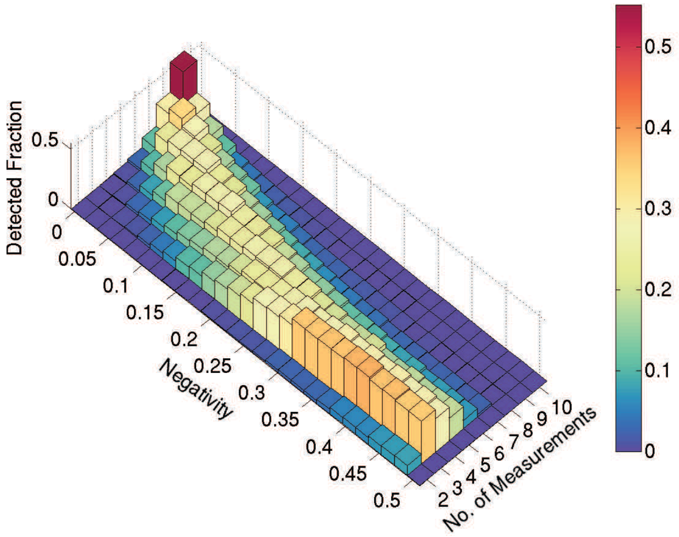


FIGURE 3.5: 10^5 runs of our procedure using 2×2-dimensional states drawn uniformly at random. The data is normalized with respect to the value of the negativity, such that it sums to one in each bin. As can be seen, for low entanglement content, the number of measurements converges to the tomographic maximum of 9 measurements.

One can clearly see that the method gets more effective as states with higher entanglement content are examined. This is only to be expected, as the overlap of such states with the set of separable states gets smaller, and hence, intuitively, they are at a greater 'distance' to the set of separable states, making it easier to find suitable witnesses separating them.

The gain in efficiency is even more pronounced for 3×3-dimensional states. Testing our method on $3 \cdot 10^4$ random instances, we find a distribution of necessary measurements in order to detect the states as shown in Fig. 3.6.

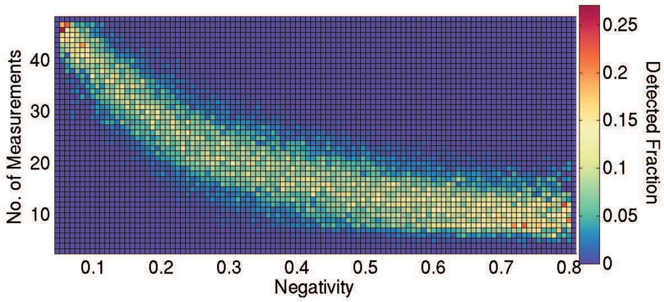


FIGURE 3.6: $3 \cdot 10^4$ runs of our procedure using 3×3-dimensional states drawn uniformly at random. The data is again normalized with respect to the value of the negativity, such that it sums to one in each bin. As only relatively few states of low negativity are produced, the distribution is cut off at a value of $\mathcal{N}(\rho) = 0.05$, as the statistics in that regime were too noisy to yield reliable conclusions. Likewise, too few states of maximal entanglement content were produced to yield satisfactory statistics.

Since too few highly entangled states were generated in the 3×3 dimensional case via random drawing, a separate analysis was made for maximally entangled states, see Fig. 3.7. There, $2 \cdot 10^4$ maximally entangled states were produced, and detection took on average 10 ± 3 measurements, were the uncertainty is due to the finite size of the statistics. As compared to the tomographic maximum of 64 measurements, we thus see that even moderately entangled states can be detected much more efficiently using our method.

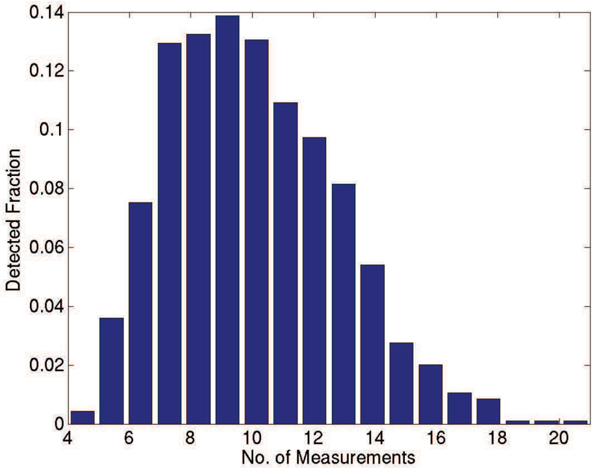


FIGURE 3.7: $2 \cdot 10^4$ runs of our procedure using 3×3-dimensional maximally entangled states.

3.3.5 Statistical Analysis

We have so far only concentrated on the case of perfect measurements, that is, used the exact quantum mechanical expectation values $\langle A_i \otimes B_j \rangle$ in our analysis. However, each real experiment is subject to error, of both a statistical and possibly systematic nature. Regarding the former, it is thus interesting to see how our method performs if we consider the effects of finite-size statistics.

Experimentally, using dichotomic measurements yielding n_+ times the value $+1$ and n_- times the value -1, the mean value of an operator M is calculated as

$$\overline{M} = \frac{1}{N}(n_+ - n_-) = \frac{1}{N}(2n_+ - N), \tag{3.79}$$

if N experiments are performed in total.

Since the outcomes are binomially distributed, the statistical uncertainty of the value n_+ is

$$\Delta n_+ = \sqrt{N p_+(1 - p_+)}, \tag{3.80}$$

with p_+ being the probability of obtaining the outcome $+1$. By error propagation, we can calculate the statistical uncertainty of $\bar{M}$ as

$$\Delta\overline{M} = \frac{\mathrm{d}M}{\mathrm{d}n_+}\Delta n_+ = \frac{2}{\sqrt{N}}\sqrt{p_+(1 - p_+)}. \tag{3.81}$$

However, the probability p_+ is of course a priori unknown. But, since the quantity $p_+(1-p_+)$ assumes its maximum of $\frac{1}{4}$ at $p_+ = \frac{1}{2}$, we can use a worst-case estimate for the uncertainty of $\overline{M}$ given by

$$\Delta\overline{M} \leq \frac{1}{\sqrt{N}}. \tag{3.82}$$

Now, our witnesses are of the form

$$W = \sum_i M_i, \tag{3.83}$$

with $M_i = A_i \otimes B_i$ (recall that we are using the second strategy presented above). A naive guess at the total statistical uncertainty of the witness expectation value would now be to again simply use standard error propagation to obtain

$$\Delta\overline{W} = \sqrt{\sum_i \left(\frac{\mathrm{d}W}{\mathrm{d}M_i}\right)^2 (\Delta\overline{M}_i)^2} = \sqrt{\sum_i c_i^2 (\Delta\overline{M}_i)^2}. \tag{3.84}$$

This would, however, be incorrect: the coefficients c_i are not independent of the mean values $\overline{M}_i$, and thus, likewise are subject to error.

This challenge can be overcome by dividing the data into two bins, one of which is used to calculate the coefficients c_i via the SDP, which are then used to evaluate the witness expectation value using the data from the second bin (Moroder et al. 2013). Thus, the coefficients are indeed independent of the statistical uncertainties of the data in that bin, and hence, can be treated as constants; then, we can use the formula in Eq. 3.84 to calculate the uncertainty of the witness expectation value, which yields

$$\Delta\overline{W} = \sqrt{\sum_i c_i^2 \frac{4}{N_i} p_i(1-p_i)} \leq \sqrt{\sum_i \frac{c_i^2}{N_i}}. \tag{3.85}$$

If we now measure every observable the same number of times, that is, $N_i = N$ for all i, this simply becomes

$$\Delta\overline{W} \leq \frac{1}{\sqrt{N}} \sqrt{\sum_i c_i^2}. \tag{3.86}$$

This estimate can then help to facilitate the decision of whether it is experimentally more prudent to add another measurement, or rather, increase the number of measurement repetitions. As we have elaborated, our method yields a lower bound to the negativity; thus, adding measurements improves this bound, and hence, a smaller number of repetitions may be necessary to unambiguously (up to some statistical certainty) conclude that the expectation value is lower than zero.

As can be seen in Fig. 3.8, in the case of a single two-qubit state ρ with a (low) negativity of $\mathcal{N}(\rho) = 0.0163$, the maximum of the 3σ confidence interval decreases sharply after adding another measurement direction, thus allowing to conclude the presence of entanglement after a far smaller number of measurement repetitions.

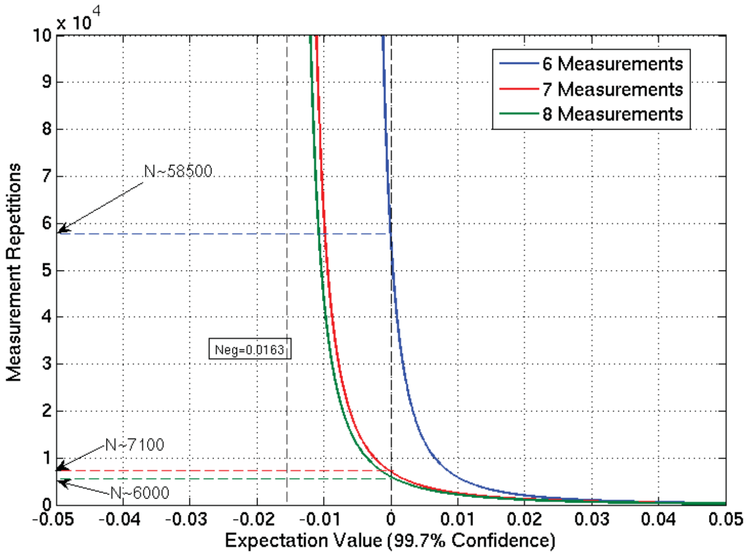


FIGURE 3.8: The maximum of the 3σ-confidence interval for the detection of a two-qubit state ρ with negativity $\mathcal{N}(\rho) = 0.0163$, yielding the number of measurement repetitions necessary to conclude entanglement for 6, 7 and 8 measurements.

Chapter 4

Their Applications

A major driving force behind the development of quantum information theory was the realization that non-classical correlations, instead of being a mere curiosity, can be viewed as a resource. Thus, they may be applied to solve problems that are classically either infeasible, or downright impossible. Entanglement has, so far, received the most attention in this regard: two important early applications were *quantum teleportation*, where entangled resources can be used to transmit the quantum information in, e.g, a single qubit state using only two classical bits of communication (Bennett, Brassard, et al. 1993), and *superdense coding*, where in some sense the reverse occurs—a single qubit is used to send two bits of classical information (Bennett and Wiesner 1992).

Since then, a plethora of applications of quantum correlations has been proposed: it can be used to reduce the amount of communication necessary between parties trying to jointly evaluate a function of some input data (Brukner, Żukowski, et al. 2004), to reduce statistical uncertainties in parameter-estimation tasks beyond the classical limit (Giovannetti, Lloyd, and Maccone 2006), to create precisely synchronized clock networks (Komar et al. 2014), and it is instrumental in bringing about the quantum speedup at least for certain kinds of quantum computation (Jozsa and Linden 2003). Recently, quantum entanglement has even made its way into biology, with speculations that it might be instrumental to photosynthesis (Sarovar et al. 2010) and the magnetic sense of certain birds (Gauger et al. 2011).

However, the area that arguably stands to profit the most from technologies harnessing quantum entanglement is cryptography. While there are cryptographic protocols that do not rely on entangled resources, yet guarantee absolute security against any adversary (Bennett 1984), protocols using entanglement, going back to the protocol by Ekert (1991), have the additional feature of *device independence* (Mayers and Yao 1998): in a device-independent setting, no assumptions need to be made about any of the apparata—e.g., sources and detectors—used; in fact, they may be fully under the control of an adversary trying to spy on the parties attempting to establish a secure communications channel.

This becomes possible only using the violation of Bell inequalities (see Chapter 2). The basic logic is that classical resources are unable to yield such violations, and thus, the presence of a violation certifies the presence of a quantum resource; furthermore, any actions of an eavesdropper tend to destroy the correlations necessary to yield the violation. Hence, Bell inequality violation suffices to conclude that no significant information has been leaked to the eavesdropper.

Making this qualitative reasoning fully quantitative had been a longstanding problem that was only solved in full by Vazirani and Vidick (2014). In the following, we will not be concerned with the details of this security proof. Rather, our aim is to first introduce the device-independent scenario, and then, as the third contribution of this thesis, introduce a novel problem—bounding the detection efficiency of uncharacterized detectors—whose solution depends on entangled quantum resources (Szangolies, Kampermann, and Bruß 2016).

4.1 The Device-Independent Framework

Device independence is an attractive feature for security-critical applications. While it was realized early on that quantum mechanics may provide security against malicious parties in cryptographic settings (Bennett 1984), such implementations may fail to be secure in the presence of direct tampering with experimental equipment, or even just simple experimental noise (Scarani and Kurtsiefer 2009). However, by moving towards implementations that are secure independently of the physical implementation of the devices, unconditional security can be restored in realistic cases.

Since thus device independence finds its natural home in cryptographic settings, we will introduce it from this vantage point, starting out by introducing some necessary basic notions of cryptography, and then discussing their device-independent implementation in the protocol of Ekert (1991).

4.1.1 Cryptography Basics

The main object of cryptography is the establishment of secure communication in the presence of untrusted third parties, called *adversaries* or *eavesdroppers*. To this end, if one party (Alice) intends to share information with another party (Bob) that must be kept secure from an eavesdropper (Eve), the outline of a typical cryptographic protocol is as follows:

1. Alice and Bob establish an *encryption scheme* that is used to convert a message, e.g. ordinary text (the *plaintext*), into a format (the *ciphertext*) that is illegible to anybody that does not possess the tools necessary for decryption.

2. Alice takes her plaintext message, encrypts it, and sends it to Bob via a public channel.

3. Bob receives Alice's ciphertext, and uses the decryption method in order to access the plaintext message.

If the protocol is secure, then no third party, even if they do intercept Alice's message, can access the plaintext. In order to establish this security, several techniques may be used. First, and by far the most popular, one may apply to the plaintext a function that is hard to invert; the security of such a protocol then rests on the assumption that any eavesdropper does not possess the computational tools necessary to perform this inversion, and hence, access the plaintext, while a trusted party, e.g. Bob, possesses additional information that renders this task manageable.

In this vein, the popular RSA scheme (Rivest, Shamir, and Adleman 1978) relies on the computational hardness of prime factorization: a pair of prime numbers is generated, and then multiplied. From this, a *public key*, which is available to anyone to encrypt their data, is generated. In order to decode a message, one further needs the *private key*; this key can be generated knowing both the public key and the pair of primes. Thus, while everybody can encrypt their data using the public key, only those in possession of the private key are able to decrypt it; hence, Alice is able to send a secure message to Bob using his public key, without any untrusted parties (which do not possess Bob's private key) being able to decode the message.

This protocol relies on the practical infeasibility of finding the prime factors of sufficiently large numbers. In 2009, a 232-digit (768-bit) number was factorized using the number field sieve method (Lenstra et al. 1993), an effort that took two years on several hundred CPUs (Kleinjung et al. 2010). Factorizing a 1024-bit number (a size currently typical for RSA encryption) would take an effort about a thousand times greater. However, since the first 512-bit key was factored only a decade prior to the factoring of the 768-bit key (Cavallar et al. 2000), and the increase in complexity was of comparable magnitude, factoring of 1024-bit RSA keys may become possible by similar efforts by 2020 (Kleinjung et al. 2010). Furthermore, while it is often believed to be the case, it has not been proven that no efficient algorithm to solve factorization problems exists.

Another challenge to the security of such protocols, and one more relevant to the present concerns, comes from the field of quantum computation: Shor (1994) was able to construct a quantum algorithm capable of factoring large numbers whose complexity grows only polynomially with the length of the number to be factored, instead of exponentially (or subexponentially) as in the case of the best-known classical algorithms.

In light of these challenges it seems prudent to look for an alternative way of encryption that does not rely on (conjectured) hardness of inversing certain mathematical operations. A class of such cryptographic systems are the so-called *information-theoretically secure* systems: in protocols based on an information-theoretically secure encoding, an adversary simply does not possess enough information in order to break the encryption (whereas, in systems such as the RSA encryption briefly discussed above, the information is present, although hard to obtain). Thus, such systems are unbreakable by cryptanalytic techniques.

A special case of information-theoretic security is *perfect security*: in a perfectly secure protocol, the ciphertext provides no information at all about the plaintext—that is, the probability distribution over possible plaintexts is independent of the ciphertext. The most well-known perfectly secure encryption method is the *one-time pad*, also known as *Vernam cipher* after Gilbert Vernam, who developed it in 1918 (Singh 1999). The idea of the method is simple: a key consisting of random characters is added (modulo the alphabet size) to the plaintext to produce the ciphertext. If this key is now at least as long as the plaintext, and is truly random, then the resulting encryption is provably perfectly secure, provided the key is kept secret and never reused.

This, however, also highlights a drawback of the method: in order to establish their secure communication channel, Alice and Bob have to share a pre-agreed key; that is, they must have already exchanged a string of random characters that is the same length as the message they want to share in secret. Hence, the overall protocol is only secure if Alice and Bob can be confident that no third party ever had access to the key, and thus, that their method of key distribution is itself perfectly secure.

It is here that quantum correlations enter into the picture. In a classical world, information leakage is nigh impossible to prevent, given sufficient resources of the eavesdropper. However, the unique properties of quantum mechanics enable a method of key distribution whose security is guaranteed by the laws of quantum mechanics. In the following, we turn towards the description of a particular protocol achieving this secure *quantum key distribution* (QKD), and use it as a way to introduce the important device-independent setting.

4.1.2 The Ekert Protocol and Device-Independence

The protocol presented by Ekert (1991) aims to accomplish the goal of secure key distribution using the properties of quantum correlations for security. The basic setup is a modified version of the CHSH-setting (see Fig. 2.1), using three, instead of two, observables per party. Alice's observables are $A_i = \boldsymbol{a_i} \cdot \boldsymbol{\sigma}$, with

$$\boldsymbol{a_1} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \boldsymbol{a_2} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad \boldsymbol{a_3} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}. \tag{4.1}$$

Likewise, Bob's observables are $B_j = \boldsymbol{b_j} \cdot \boldsymbol{\sigma}$ with

$$\boldsymbol{b_1} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \boldsymbol{b_2} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad \boldsymbol{b_3} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}. \tag{4.2}$$

Now, the protocol runs as follows:

1. Alice and Bob share two qubits in the singlet state $|\Phi^+\rangle$ (see Eq. 1.67).

2. Alice chooses $i \in \{1, 2, 3\}$ at random, and performs measurement A_i; likewise, Bob chooses $j \in \{1, 2, 3\}$ at random, and measures B_j. These first two steps are repeated until sufficiently many measurements to yield conclusive statistics have been performed.

3. Alice and Bob announce the bases they have measured in publicly.

4. The raw key is formed by using those cases in which both parties have performed either their first or third measurement: due to the correlations in the state $|\Phi^+\rangle$, whenever Alice obtains a $+1$-outcome, and Bob measures in the same basis, he will likewise obtain a $+1$-outcome (and equivalently for the -1-case), thus leaving both with perfectly correlated data.

5. The remaining measurements are used to compute the value of the CHSH-quantity

$$\langle \mathcal{C}_{\text{CHSH}} \rangle = \langle A_1 \otimes B_3 \rangle + \langle A_1 \otimes B_2 \rangle + \langle A_2 \otimes B_3 \rangle - \langle A_2 \otimes B_2 \rangle. \tag{4.3}$$

> If there has now been any interference by an eavesdropper, this value will not exceed the classical bound of $\langle \mathcal{C}_{\text{CHSH}} \rangle = 2$: any measurement of Eve destroys the entanglement between the two qubits of Alice and Bob, and hence, as discussed in Sec. 2.2.1, subsequent measurements performed by Alice and Bob will yield correlations compatible with a classical model. Conversely, a value of
>
> $$\langle \mathcal{C}_{\text{CHSH}} \rangle = 2\sqrt{2} \tag{4.4}$$
>
> guarantees the absence of an eavesdropper, and consequently, enables the distribution of a secure cryptographic key.

The above protocol now achieves the goal of distributing a random bit string of arbitrary length in such a way that only Alice and Bob have access to it. Hence, it provides a secure foundation for cryptographic schemes such as the one-time pad. However, most interesting for our purpose is that it can be implemented in a device-independent way: Alice and Bob need not make any assumptions on the correct functioning of their apparata; in fact, those can even be completely untrusted, e.g. manufactured by a possibly adversarial third party.

The reason for this is the use of Bell inequality violation as a security certificate: all that is needed to conclude the absence of an eavesdropper are the observed measurement results; the way in which they are produced is of no consequence. Knowing that there is a Bell inequality violation, from the discussion in Sec. 2.1.2, we know that there cannot be independent, predefined definite values for all observables; consequently, no eavesdropper could have obtained these values surreptitiously. It can be shown that, in fact, an efficient quantum key distribution scheme is possible in this way (Vazirani and Vidick 2014).

This realization has led to considerable attention being devoted to the device-independent scenario. For an overview, see e.g. the *New Journal of Physics* special issue curated by Pironio, Scarani, and Vidick (2016), which among others features contributions on topics including device-independent randomness certification (Mironowicz et al. 2016), entanglement quantification (Goh, Bancal, and Scarani 2016), testing of causal order (Baumeler and S. Wolf 2016), and self-testing of quantum states (McKague 2016).

Among these, the latter, *self-testing* has particular relevance to the application we will describe in the following. The object of self-testing is, essentially, to use unknown (or untrusted) devices, and nevertheless extract information about the implemented measurements and the quantum state. A simple self-testing scenario includes a source, which is claimed to produce a certain quantum state (say, $|\Phi^+\rangle$), together with two spacelike separated apparata, which are claimed to carry out certain measurements. It can then be shown that the observed probability distributions suffice to decide whether the claims are correct, up to a local change of basis (Mayers and Yao 2004).

In the following, we propose a protocol aimed at self-testing the *quality* of the detectors used. That is, using this protocol, absent any further assumptions on the detectors or source, one can use Bell inequality violations to certify a lower bound on the detection efficiency η, i.e. the probability that a detector registers an accurate outcome.

4.2 Device-Independent Detection Efficiency Bounding

Consider the following scenario. Your lab needs a new detector; funding being tight, you turn to your local used detector vendor. Naturally, they promise you quality products. However, you are not sure whether you can trust their promises (and all sales are final). Given that all equipment—detectors and sources—is under the vendor's control, is there a way to ensure that you purchase a detector whose detection efficiency meets your needs?

Classically, the answer is no: a shrewd enough vendor can manipulate the detector to yield spurious detections according to some pre-set program, they can vary the source rate from the rate it is claimed to have, or use other means of tampering with the equipment.

Fortunately, as we will show, the answer is different in quantum mechanics. To demonstrate this, we will first discuss a method to construct Bell inequalities a posteriori, that is, using only the observed measurement outcomes. If these fail to be consistent with a classical model, the resulting Bell inequality violation is then used to certify a bound on the minimal efficiency of the detectors involved.

4.2.1 Bell Inequalities from Measurement Statistics

In order to certify bounds on detector efficiencies, we first need to find a method to construct Bell inequalities using only the observed measurement statistics. The simplest idea would be, of course, to simply agree on a Bell inequality beforehand, and see whether it is violated. Indeed, this is the common strategy employed in many self-testing protocols (see, e.g., Mayers and Yao 2004; McKague, Yang, and Scarani 2012; Miller and Shi 2012).

However, this method has the drawback that while its conclusions are robust, cases in which the chosen Bell inequality is not violated, but some other Bell inequality violation might be achievable by the state with some given set of measurements, are ignored. Thus, we aim to find a method that finds a Bell inequality violation whenever non-classical measurement statistics are present.

It has previously been studied whether random local measurements can yield Bell inequality violations (Liang et al. 2010; Shadbolt et al. 2012; Wallman and Bartlett 2012; Wallman, Liang, and Bartlett 2011). However, the previously investigated schemes used restricted classes of Bell inequalities, such as the CHSH inequality and the class of Mermin-Ardehali-Belinsky-Klyshko (MABK) inequalities (Ardehali 1992; Belinsky and Klyshko 1993; Mermin 1990a). Our method, in contrast, constructs a Bell inequality from nothing but the observed statistics, and is thus not limited to violations of any fixed Bell inequality.

The basis of the method is as follows. According to the discussion in Sec. 2.1.2, the classical probability distributions form a polytope. Hence, any probability distribution not contained in the polytope, that is, any distribution that cannot be written as a convex combination of the vertices of this polytope, does not possess a classical model, and consequently violates some Bell inequality. Our task is then, given the observed measurement statistics, to decide whether they can be written as such a convex combination.

The setting is again a modified CHSH-setting (see Fig. 2.1), where now Alice has access to n dichotomic local observables A_i, while Bob likewise measures m observables B_j. For any n and m, the polytope of classical correlations has 2^{n+m} vertices $\boldsymbol{v_k}$. Our experimental data consists of the measurement statistics, that is, the probabilities $\Pr\left(A_i^+\right)$ that observable A_i yields the $+1$-outcome, the probabilities $\Pr\left(B_j^+\right)$, and the joint probabilities $\Pr\left(A_i^+ B_j^+\right)$, which we collect into the $n+m+nm$-dimensional vector

$$\boldsymbol{P}_{\text{obs}} = \begin{pmatrix} \Pr\left(A_1^+\right) \\ \vdots \\ \Pr\left(A_n^+\right) \\ \Pr\left(B_1^+\right) \\ \vdots \\ \Pr\left(B_m^+\right) \\ \Pr\left(A_1^+ B_1^+\right) \\ \vdots \\ \Pr\left(A_n^+ B_m^+\right) \end{pmatrix} \tag{4.5}$$

If this vector cannot be written as

$$\boldsymbol{P}_{\text{obs}} = \sum_k \lambda_k \boldsymbol{v_k}, \tag{4.6}$$

with $0 \leq \lambda_k \leq 1$, $\sum_k \lambda_k = 1$, no classical model for the observed statistics exists.

This can be translated into a linear separation problem: if we can find a hyperplane separating the vertices $\boldsymbol{v_k}$ from $\boldsymbol{P}_{\text{obs}}$, we know that $\boldsymbol{P}_{\text{obs}}$ cannot lie within the convex hull of the $\boldsymbol{v_k}$, that is, it cannot be contained in the classical polytope. A hyperplane in $n+m+nm$ dimensions can be characterised by its normal vector $\boldsymbol{h}$, together with a constant x_0. It consists of all points (probability distributions) $\boldsymbol{P}$ such that

$$\sum_\alpha h_\alpha P_\alpha = x_0. \tag{4.7}$$

Here, α runs over the elements of $\boldsymbol{h}$, which are given by

$$\boldsymbol{h} = \begin{pmatrix} h_{A_1} \\ \vdots \\ h_{A_n} \\ h_{B_1} \\ \vdots \\ h_{B_m} \\ h_{A_1 B_1} \\ \vdots \\ h_{A_n B_m} \end{pmatrix}. \tag{4.8}$$

Thus, we have to solve the following satisfiability problem:

$$\begin{aligned} \text{find:} \quad & \boldsymbol{h} \in \mathbb{R}^{n+m+nm},\ x_0 \in \mathbb{R} \\ \text{subject to:} \quad & \boldsymbol{h}^T \boldsymbol{v_k} < x_0 \, \forall k \in \{1, \dots, 2^{n+m}\} \\ & \boldsymbol{h}^T \boldsymbol{P}_{\text{obs}} > x_0. \end{aligned}$$

If there exists a solution to this problem, then the observed measurement statistics $\boldsymbol{P}_{\text{obs}}$ do not have a classical model. The hyperplane found in this manner then defines the Bell inequality

$$\sum_{\alpha} h_\alpha P_\alpha = \sum_{i=1}^{n} h_{A_i} \Pr\left(A_i^+\right) + \sum_{j=1}^{m} h_{B_j} \Pr\left(B_j^+\right) + \sum_{i,j=1}^{nm} h_{A_i B_j} \Pr\left(A_i^+ B_j^+\right) \leq x_0. \tag{4.9}$$

In order to maximize the quantum violation $Q > x_0$ of the Bell inequality, we can turn the satisfiability problem above into an optimization:

$$\begin{aligned} \text{maximize:} \quad & \boldsymbol{h}^T \boldsymbol{P}_{\text{obs}} \\ \text{subject to:} \quad & \boldsymbol{h}^T \boldsymbol{v_k} < x_0 \, \forall k \in \{1, \dots, 2^{n+m}\} \\ & \boldsymbol{h}^T \boldsymbol{P}_{\text{obs}} > x_0 \\ & -1 \leq h_i \leq 1 \, \forall i \in \{1, \dots, n+m+nm\}, \end{aligned}$$

where the constraint on the magnitude of the elements of $\boldsymbol{h}$ merely ensures the boundedness of the problem, and sets an arbitrary overall scale. The Bell inequality found in this way will directly bound the polytope of classical correlations, and is called *tight*.

An example of a Bell inequality (which happens to be tight) that may be found with this method is the CH-inequality (see Eq. 2.10) with $\boldsymbol{h} = (-1, 0, -1, 0, 1, 1, 1, -1)^T$ and $x_0 = 0$.

The method as outlined so far thus allows us to find Bell inequalities using nothing but the observed measurement statistics. But there exists a confounding issue: due to the finite efficiency of the detectors involved, some events will fail to be detected; but in this case, the observed measurement statistics will only approximate the real probabilities if the detected events constitute a fair sample of all events. If, instead, certain events are systematically rejected, it becomes possible to produce spurious violations of Bell inequalities, despite the existence of an underlying classical model (Pearle 1970). This leads to the so-called *detection* or *fair-sampling loophole*. We will now discuss this issue in more detail, and then propose a solution within our framework.

4.2.2 The Pearle Model and the Detection Loophole

The detection loophole was first pointed out by Pearle (1970), who proposed an explicit model in which data rejection by the detectors leads to apparent violations of a Bell inequality, even though all events are sampled from a joint probability distribution (cf. the discussion in Sec. 2.1.1). We will now briefly discuss this model, largely following the simplified exposition due to Gill (2015).

We consider once again the CHSH-scenario (Fig. 2.1). A source distributes two particles to parties A and B. In the Pearle model, now, each particle carries a hidden variable, say $\boldsymbol{X}_A$ for the particle sent to A, and $\boldsymbol{X}_B$ for the one sent to B, such that $\boldsymbol{X}_A = -\boldsymbol{X}_B$. The hidden variables are each composed of a scalar r and a point on the two-sphere $\mathbb{S}^2$, $\boldsymbol{q}$, such that $\boldsymbol{X}_A = r\boldsymbol{q} = -\boldsymbol{X}_B$. The scalar r can be considered an amplitude, while the unit vector $\boldsymbol{q}$ represents the direction of the spin of the particle sent to A (while $-\boldsymbol{q}$ is the analogue for B). The direction $\boldsymbol{q}$ is uniformly distributed on $\mathbb{S}^2$, independently of r.

Parties A and B carry out measurements in directions $\boldsymbol{a}$ and $\boldsymbol{b}$, respectively. The experimental outcomes are then generated by the response functions for the detectors,

$$A(\boldsymbol{X}_A) = \begin{cases} \mathrm{sgn}(\boldsymbol{q}\cdot\boldsymbol{a}) & \text{if } \arccos(|\boldsymbol{q}\cdot\boldsymbol{a}|) \geq \frac{r\pi}{2} \\ 0 & \text{else} \end{cases} \tag{4.10}$$

and

$$B(\boldsymbol{X}_B) = \begin{cases} -\mathrm{sgn}(\boldsymbol{q}\cdot\boldsymbol{b}) & \text{if } \arccos(|\boldsymbol{q}\cdot\boldsymbol{b}|) \geq \frac{r\pi}{2} \\ 0 & \text{else,} \end{cases} \tag{4.11}$$

where $\mathrm{sgn}(x)$ yields the sign of x, and 0 signals a non-detection.

Now, in the quantum setting, the prediction for the correlation between two measurement directions $\boldsymbol{a}$ and $\boldsymbol{b}$ is

$$\langle \boldsymbol{a}\cdot\boldsymbol{\sigma} \otimes \boldsymbol{b}\cdot\boldsymbol{\sigma} \rangle = -\boldsymbol{a}\cdot\boldsymbol{b} \equiv -\cos(\phi), \tag{4.12}$$

where ϕ is the angle between $\boldsymbol{a}$ and $\boldsymbol{b}$, if we assume A and B share the singlet state

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{4.13}$$

This yields a maximal violation of the CHSH-inequality for, e.g., the directions

$$\begin{aligned} \boldsymbol{a_1} &= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \boldsymbol{b_1} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ -1 \\ 0 \end{pmatrix}, \\ \boldsymbol{a_2} &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \boldsymbol{b_2} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \end{aligned} \tag{4.14}$$

since

$$\langle \mathcal{C}_{\text{CHSH}} \rangle = -\boldsymbol{a_1}\cdot\boldsymbol{b_1} - \boldsymbol{a_1}\cdot\boldsymbol{b_2} - \boldsymbol{a_2}\cdot\boldsymbol{b_1} + \boldsymbol{a_2}\cdot\boldsymbol{b_2} = 2\sqrt{2}. \tag{4.15}$$

This correlation can be reproduced by the Pearle model for a specific choice of distribution of the amplitude r. This distribution is somewhat complicated (Gill 2015); however, matters can be simplified by equivalently choosing $S = \frac{r\pi}{2}$ such that

$$S = \frac{2}{\sqrt{1 + \frac{3v}{\pi}}} - 1, \tag{4.16}$$

and drawing v uniformly at random from the interval $[0, \pi]$. The correlations obtained using this model are shown in Fig. 4.1, which shows a very good agreement with the quantum mechanical prediction.

In the Pearle model, data rejection rates vary with the angle between $\boldsymbol{a}$ and $\boldsymbol{b}$, ranging from maximally $\frac{2}{3}$ to $\frac{4}{3}(1 - \frac{2}{\pi}) \approx 0.485$ (Pearle 1970). Even if the overall source rate is thus unknown, an experimenter could notice this systematic variation and hence, conclude that there is something suspicious

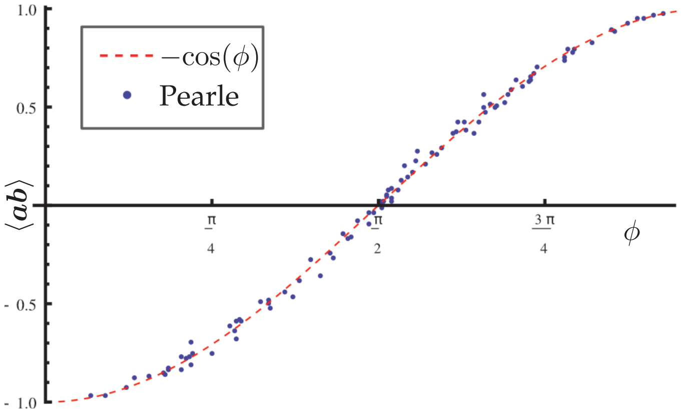


FIGURE 4.1: Numerical simulation of the Pearle-model. 100 datapoints were generated by performing 10^5 simulated measurements each, according to Eqs. 4.10 and 4.11.

about the behavior of the apparata. However, as shown by N. Gisin and B. Gisin (1999), data-rejection based models exist that do not suffer from this issue.

There are several possible responses to the detection loophole. One is the so-called *fair-sampling assumption* (Clauser and Horne 1974): we simply assume that the detected events form a fair sample of the complete set of events, and thus, asymptotically obey the same statistics. While this is a physically well-motivated assumption, in our scenario, it cannot be allowed; after all, a malicious vendor is under no obligation to let their detectors detect a fair sample.

Another response alters the Bell inequalities based on the finite efficiency of the detectors involved. Garg and Mermin (1987) thus replace the correlation functions $\langle AB \rangle$ with functions taking the conditional probability for a detection into account,

$$E(A,B) = \sum_{a,b} ab\Pr\left(A^a, B^b \middle| A \text{ and } B \text{ click}\right). \tag{4.17}$$

If the probability for each detector to correctly produce a click is η, then these modified correlation functions are related to the correlators as defined in Eq. 2.4 by (Garg and Mermin 1987, s.a. Larsson 2014)

$$E(A,B) = \frac{\eta}{2-\eta}\langle AB \rangle, \tag{4.18}$$

which yields a modified bound for the CHSH-inequality,

$$\langle A_1B_1 \rangle + \langle A_1B_2 \rangle + \langle A_2B_1 \rangle - \langle A_2B_2 \rangle \leq \frac{4}{\eta} - 2. \tag{4.19}$$

However, as the detection efficiency is unknown in our case, this solution likewise is not open to us. Fortunately, there exists a third solution: certain Bell inequalities can be re-expressed using solely the known total counts generated by the detectors (Eberhard 1993). It is to this method that we turn in the following.

4.2.3 The Classical Cone

Imagine that, during the course of an experiment, the source sent out exactly N particle pairs, such that ideal detectors would have produced N clicks in total. Now, of course, N is an unknown number in the case of imperfect detectors, since at least the number of cases in which both detectors failed to produce a click is necessarily unknown. However, we can use the same logic as before to derive Bell inequalities, by deriving the vertices of a polytope that all distributions of counts must obey if there is an underlying classical model producing these counts.

TABLE 4.1: Extreme values of count rates in the ideal scenario.

A^+	B^+	$A^+ \wedge B^+$
0	0	0
0	N	0
N	0	0
N	N	N

In the extremal case yielding the vertices of the polytope, as shown in Table 4.1, all N particle pairs can either produce the $+1$-outcomes for A, B, or for both, in the case of ideal detectors. Thus, the polytope is identical to the one derived in Sec. 2.1.1, merely uniformly stretched in all directions by a factor N. Recall now that the Bell inequalities that can be derived using the polytope method had the form

$$\sum_i h_{A_i} \Pr\left(A_i^+\right) + \sum_j h_{B_j} \Pr\left(B_j^+\right) + \sum_{ij} h_{A_i B_j} \Pr\left(A_i^+ B_j^+\right) \leq x_0. \tag{4.20}$$

Now, in the limit of large N, the probabilities in this equation will be given by ratios of detected $+1$-outcomes and the overall number of events, yielding

$$\sum_i h_{A_i} \frac{N_{A_i}^+}{N} + \sum_j h_{B_j} \frac{N_{B_j}^+}{N} + \sum_{ij} h_{A_i B_j} \frac{N_{A_i B_j}^{++}}{N} \leq x_0, \tag{4.21}$$

where $N_{A_i}^+$ simply is the number of $+1$-outcomes for the observable A_i (likewise for B_j), and $N_{A_i B_j}^{++}$ counts how often both observables yielded $+1$ together. Now, we can eliminate the unknown number of particle pairs N by multiplying through with it, provided that $x_0 = 0$; otherwise, the right hand side, i.e. the classical bound, acquires a dependence on N. This leads to Bell inequalities of the form

$$\sum_i h_{A_i} N_{A_i}^+ + \sum_j h_{B_j} N_{B_j}^+ + \sum_{ij} h_{A_i B_j} N_{A_i B_j}^{++} \leq 0, \tag{4.22}$$

which now only contain the experimentally accessible total counts for all observables, and are hence free from the detection loophole. A special case of these Bell inequalities with $\boldsymbol{h} = (-1, 0, -1, 0, 1, 1, 1, -1)^T$ is then the *Eberhard inequality* (Eberhard 1993)

$$-N_{A_1}^+ - N_{B_1}^+ + N_{A_1 B_1}^{++} + N_{A_1 B_2}^{++} + N_{A_2 B_1}^{++} - N_{A_2 B_2}^{++} \leq 0. \tag{4.23}$$

In order to (for convenience) move back to Bell inequalities dealing with probabilities, we can then divide by the number of total counts N^*, which yields, strictly speaking, the conditional probability that e.g. A_i produced a $+1$-outcome, given that at least one detector produced a click. We will, however, not notationally distinguish between these conditional probabilities and the ideal probabilities, and continue writing $\Pr\left(A_i^+\right)$ for this case. Performing this operation on Eq. 4.23 then once again yields the CH-inequality, which, in terms of the probabilities generated in this way, is thus free from the detection loophole.

These inequalities can now be generated using the observed measurement statistics as before. Given the vector $\boldsymbol{P}_{\text{obs}}$ containing the measured statistics (as generated according to the above discussion), we solve the following optimization problem:

$$\begin{aligned} \text{maximize:} \quad & \boldsymbol{h}^T \boldsymbol{P}_{\text{obs}} \\ \text{subject to:} \quad & \boldsymbol{h}^T \boldsymbol{v_k} < 0 \, \forall k \in \{1, \ldots, 2^{n+m}\} \\ & \boldsymbol{h}^T \boldsymbol{P}_{\text{obs}} > 0 \\ & 0 \leq h_i \leq 1 \, \forall i \in \{1, \ldots, n+m+nm\}, \end{aligned}$$

which, if a solution exists, then yields a maximally violated Bell inequality defined by the hyperplane $\boldsymbol{h}$ which is free from the detection loophole, and whose violation is thus unambiguous even in the case of unknown detector efficiencies.

Since we have mandated that $x_0 = 0$, each such hyperplane now contains the origin, which is also necessarily one of the vertices of the set of allowed probability distributions. Geometrically, this means that these hyperplanes now only bound a convex cone, instead of a convex polytope, as before; for all probability distributions inside this cone, a classical model cannot be excluded. Hence, we term this the *classical cone*. Essentially, this is due to the fact that the unknown total number of particle pairs N sets the 'scale' of the polytope; hence, we must allow for arbitrary scaling transformations. This situation is schematically depicted in Fig. 4.2, which also shows the more general set of no-signalling correlations (see Sec. 2.1.2).

The method as presented so far already allows several intriguing applications. First of all, it enables a device-independent version of the protocols for observing Bell inequality violations between two laboratories which do not possess a shared reference frame (Liang et al. 2010; Shadbolt et al. 2012; Wallman and Bartlett 2012; Wallman, Liang, and Bartlett 2011). In (Wallman and Bartlett 2012), it is shown that two parties can always violate a Bell inequality if they share a Bell state (see Eq. 1.67) and perform three measurements along orthogonal axes of their local coordinate system, removing the necessity of establishing a shared global frame of reference.

Using our method, this result can be extended to the device-independent case. In this case, there is naturally no need for a global reference frame, and in fact, even the need for a characterization of the detectors, and hence, the local measurement directions, is eliminated. The effectiveness of the method can then be gauged by numerical simulation. In Fig. 4.3, $5 \cdot 10^5$ random maximally entangled two-qubit states were generated, and measurements were performed up to a limit of $n + m = 12$ in total (that is, 6 measurements for party A and B each), or until a Bell inequality violation was detected. As can be seen, more than half of all states were detected

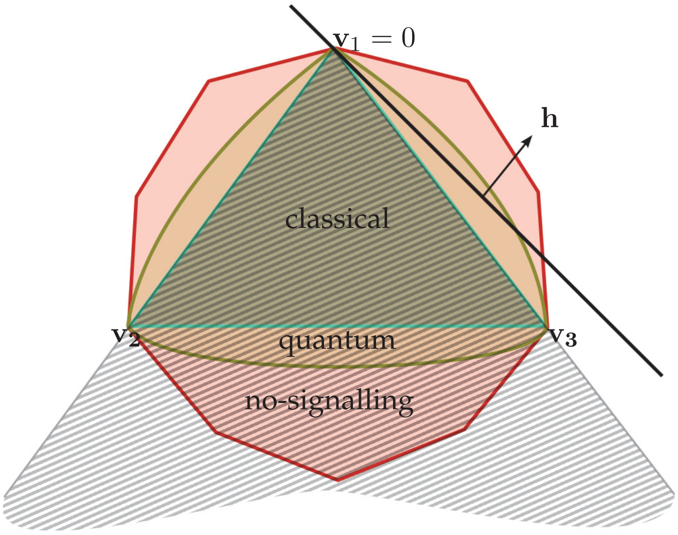


FIGURE 4.2: The sets of classical, quantum, and no-signalling correlations, together with a Bell inequality defined by its normal vector $\mathbf{h}$, and the cone of probability distributions where we cannot exclude the existence of a classical model (hatched area).

using 6 measurements or fewer, and thus, the expected number of measurements per party until detection remains of the same order as in the protocol of Wallman and Bartlett (2012), even though no characterization of the detectors was assumed in our case.

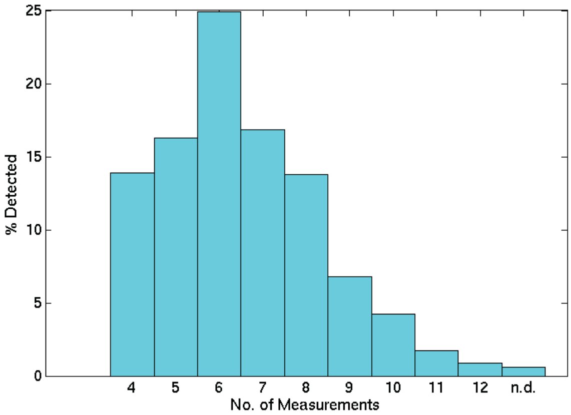


FIGURE 4.3: Numerical simulation of $5 \cdot 10^5$ detection attempts for a maximally entangled two-qubit state. The percentage of states detected is plotted against the total number $n + m$ of local measurements.

Furthermore, our method can be viewed as constructing a device-independent entanglement witness that does not have to be tailored to a state beforehand (cf. Sec. 3.3). Given a Bell inequality

$$\sum_i h_{A_i} \mathrm{Pr}\left(A_i^+\right) + \sum_j h_{B_j} \mathrm{Pr}\left(B_j^+\right) + \sum_{ij} h_{A_i B_j} \mathrm{Pr}\left(A_i^+ B_j^+\right) \leq 0, \tag{4.24}$$

with (unknown) operators $E^+_{A_i}$ and $E^+_{B_j}$ such that

$$\begin{aligned}\Pr\left(A_i^+\right) &= \mathrm{tr}\left(E^+_{A_i}\otimes\mathbb{1}\rho\right)\\ \Pr\left(B_j^+\right) &= \mathrm{tr}\left(\mathbb{1}\otimes E^+_{B_j}\rho\right)\\ \Pr\left(A_i^+B_j^+\right) &= \mathrm{tr}\left(E^+_{A_i}\otimes E^+_{B_j}\rho\right),\end{aligned} \tag{4.25}$$

we can construct the witness operator

$$W = -\sum_i h_{A_i}E^+_{A_i}\otimes\mathbb{1} - \sum_j h_{B_j}\mathbb{1}\otimes E^+_{B_j} - \sum_{ij} h_{A_iB_j}E^+_{A_i}\otimes E^+_{B_j}. \tag{4.26}$$

From the construction of our Bell inequalities, it is immediate that a negative value for $\mathrm{tr}\,(W\rho)$ implies that ρ is entangled. Thus, the construction can be used to detect the entanglement of an unknown state in a device-independent way, and hence represents a natural further development of the method presented in (Szangolies, Kampermann, and Bruß 2015).

Finally, our method suggests a device-independent QKD (DIQKD) protocol in which the participants do not agree on a Bell inequality beforehand, but simply perform some set of measurements available to them, and then see whether the resulting measurement statistics violated a Bell inquality. In most DIQKD protocols, closing the detection loophole is a difficult problem, necessitating measures such as using a heralded amplifier to boost signal strengths (N. Gisin, Pironio, and Sangouard 2010) or an entanglement swapping relay to ensure a sufficient violation of a given Bell inequality (Curty and Moroder 2011).

In contrast, since the Bell inequalities generated by our construction do not suffer from the detection loophole, any violation detected using our method suffices to guarantee security. Furthermore, since we find that Bell inequality which is maximally violated, we can directly optimize the rate R of secret bits distributed between Alice and Bob, as this rate is connected to the quantum violation Q by (Masanes, Pironio, and Acín 2011)

$$R \geq -\log_2 f(Q) - H(a|b). \tag{4.27}$$

Here, $f(Q)$ is a function depending on the Bell inequality used that can be determined by semidefinite methods, and $H(a|b)$ is the conditional Shannon entropy of Alice's outcomes a and Bob's outcomes b.

Thus, this ensures that a Bell inequality is chosen that leads to the best key rate given the actually performed measurements (which may differ from the measurements Alice and Bob set out to perform, either due to noise or the actions of an eavesdropper), while simultaneously evading the detection loophole.

Besides these applications, we now move on to a novel task: the bounding of detector efficiencies. That is, our aim in the following is to find, for at least one of the involved detectors, a lower bound on η such that the detector can be certified to possess at least this detection efficiency. To do so, we first introduce a tool that will aid us in computing these lower bounds, the Navascués-Pironio-Acín hierarchy.

4.2.4 The Navascués-Pironio-Acín Hierarchy

In a scenario with limited detection efficiencies, our observed probabilities will differ from the quantum mechanical predictions for the ideal case. That is, if η_A is the detection efficiency of the detector A, η_B correspondingly for B, we have to consider the probabilities that the detector produces a click and yields the outcome $+1$, that is

$$\begin{aligned}\Pr\left(A_i^+ \wedge A\,\text{clicks}\right) &= \eta_A \operatorname{tr}\left(\Pi_{A_i}^+ \otimes \mathbb{1}\rho\right)\\ \Pr\left(B_j^+ \wedge B\,\text{clicks}\right) &= \eta_B \operatorname{tr}\left(\mathbb{1} \otimes \Pi_{B_j}^+\rho\right)\\ \Pr\left(A_i^+ B_j^+ \wedge A\,\text{and}\,B\,\text{click}\right) &= \eta_A\eta_B \operatorname{tr}\left(\Pi_{A_i}^+ \otimes \Pi_{B_j}^+\rho\right),\end{aligned} \tag{4.28}$$

where e.g. $\Pi_{A_i}^+$ is the projector on the $+1$-eigenspace of A_i. Note that it suffices here to consider projective measurements and a pure state $\rho = |\psi\rangle\langle\psi|$, since we leave the dimension of the underlying quantum system unspecified, and every POVM can be realized using a projective measurement on a higher-dimensional system in a pure state via Naimark's extension (Naimark 1940, 1943). Thus, our Bell inequalities now take the form

$$\eta_A \sum_i h_{A_i} \Pr\left(A_i^+\right) + \eta_B \sum_j h_{B_j} \Pr\left(B_j^+\right) + \eta_A\eta_B \sum_{ij} h_{A_iB_j} \Pr\left(A_i^+B_j^+\right) \leq 0. \tag{4.29}$$

Let us, for the moment, make the simplifying assumption that all detector efficiencies are equal, $\eta_A = \eta_B \equiv \eta$. We can then calculate the critical detection efficiency as

$$\eta_{\text{crit}} = -\frac{\sum_i h_{A_i} \Pr\left(A_i^+\right) + \sum_j h_{B_j} \Pr\left(B_j^+\right)}{\sum_{ij} h_{A_iB_j} \Pr\left(A_i^+B_j^+\right)}. \tag{4.30}$$

Any detection efficiency exceeding this threshold allows for a violation of the inequality 4.29. Inverting this logic, thus, means that observing a violation implies that the detectors used possess minimally the detection efficiency η_{crit}.

Calculation of this detection efficiency necessitates an optimization over all $\boldsymbol{P}_{\text{obs}}$ that have a quantum model, that is, which can be observed in a quantum mechanical experiment. Thus, we have the following optimization problem:

$$\begin{aligned}\text{minimize:}\quad & \eta\\ \text{subject to:}\quad & \eta = -\tfrac{\sum_i h_{A_i}\Pr\left(A_i^+\right)+\sum_j h_{B_j}\Pr\left(B_j^+\right)}{\sum_{ij} h_{A_iB_j}\Pr\left(A_i^+B_j^+\right)}\\ & \Pr\left(A_i^+\right) = \langle\psi|\, E_{A_i}^+\, |\psi\rangle\\ & \Pr\left(B_j^+\right) = \langle\psi|\, E_{B_j}^+\, |\psi\rangle\\ & \Pr\left(A_i^+B_j^+\right) = \langle\psi|\, E_{A_i}^+ E_{B_j}^+\, |\psi\rangle\\ & E_{A_i}^{+\dagger} = E_{A_i}^+, E_{B_j}^{+\dagger} = E_{B_j}^+\\ & E_{A_i}^2 = E_{A_i}, E_{B_j}^2 = E_{B_j},\end{aligned}$$

where we have introduced the operators $E^+_{A_i} = \Pi^+_{A_i} \otimes \mathbb{1}$ and $E^+_{B_j} = \mathbb{1} \otimes \Pi^+_{B_j}$. This is a challenging optimization to perform even in simple cases. Fortunately, there exists a tool, the so-called *Navascués-Pironio-Acín (NPA) hierarchy* (Navascués, Pironio, and Acín 2007, 2008), which allows us to compute lower bounds to η_{crit} in an efficient way.

The NPA hierarchy introduces an infinite sequence of criteria, each more stringent than the last, such that every quantum mechanical probability distribution obeys all criteria. Thus, on every level of the hierarchy, additional probability distributions are excluded. For the case we are interested in, which includes projective measurements with two outcomes, we first form the set of observables

$$\mathcal{E} = \mathbb{1} \cup \{E^+_{A_i}\} \cup \{E^+_{B_j}\}, \tag{4.31}$$

where $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, m\}$. Then consider the set of operators $\mathcal{O} = \{O_1, \ldots, O_k\}$, which are linear combinations of products of operators in $\mathcal{E}$. $\mathcal{O}$ can be viewed as a finite subset of the algebra generated by $\mathcal{E}$.

Consider linear equations of the form

$$\sum_{ij} (F_k)_{ij} \langle \psi | O_i^\dagger O_j | \psi \rangle = g_k(\boldsymbol{P}), \tag{4.32}$$

where $k \in \{1, \ldots, l\}$, and $g_k(\boldsymbol{P})$ are linear functions of the probabilities,

$$g_k(\boldsymbol{P}) = (g_k)_0 + \sum_{i,j} (g_k)_{ij} \Pr\left(A_i^+ B_j^+\right). \tag{4.33}$$

Now define the sets $\mathcal{S}_n$ of operators as

$$\mathcal{S}_0 = \{\mathbb{1}\}, \tag{4.34}$$

$$\mathcal{S}_1 = \mathcal{S}_0 \cup \{E^+_{A_i}\} \cup \{E^+_{B_j}\}, \tag{4.35}$$

$$\mathcal{S}_2 = \mathcal{S}_1 \cup \{E^+_{A_i} E^+_{A_j}\} \cup \{E^+_{B_i} E^+_{B_j}\} \cup \{E^+_{A_i} E^+_{B_j}\}, \tag{4.36}$$

$$\mathcal{S}_3 = \ldots \tag{4.37}$$

That is, the set $\mathcal{S}_n$ is simply the set of all products of observables up to length n. Every operator $O_i \in \mathcal{O}$ can be written as a linear combination of operators from $\mathcal{S}_n$ for sufficiently large n.

Navascués, Pironio, and Acín (2007) now show that it is a necessary and sufficient condition for $\boldsymbol{P}$ to have a quantum model if there exists a *certificate* Γ such that

$$\sum_{ij} (F_k)_{ij} \Gamma_{ij} = g_k(\boldsymbol{P}) \tag{4.38}$$

for all equations of the form 4.32 such that Γ is a Hermitian complex positive semidefinite matrix.

Furthermore, whenever there exists a certificate for a set of operators $\mathcal{O}$, there also exists a certificate for any set $\mathcal{O}'$ that can be generated from $\mathcal{O}$ by linear combinations; hence, it suffices to check the existence of a certificate for the sets in Eq. 4.34, and the associated equations 4.32.

Consequently, there exists a hierarchy of tests, each yielding a certificate Γ^n associated with one of the sets $\mathcal{S}^n$, such that a probability distribution

$\boldsymbol{P}$ is quantum if and only if it passes all of these tests, and conversely, any non-quantum probability distribution will fail a test at some level $n < \infty$.

Now, these tests can be implemented via semidefinite programming (see Sec. 3.2); moreover, a ready-made implementation exists in the freely-available MATLAB-toolbox QETLAB (Johnston 2016) that also allows setting the fulfillment of the hierarchy to some given level (in practice ≤ 4) as a constraint for optimization tasks.

4.2.5 Bounding Detector Efficiencies

Having now assembled the necessary tools, we move on to the next main contribution of this thesis, namely, establishing lower bounds on the efficiencies of detectors in an adversarial setting. As discussed in the previous section, the critical detection efficiency can be obtained by using the expression in Eq. 4.30 (for the case of identical detectors), and finding the minimum over all probability vectors $\boldsymbol{P}$ such that $\boldsymbol{P}$ has a quantum model, that is, could have originated from a quantum state ρ and measurements performed on it.

Since this optimization is, in general, infeasible—for one, we would have to allow for Hilbert spaces of arbitrary dimension—, we can establish a series of increasingly better lower bounds using successive levels of the NPA-hierarchy. In practice, low levels of the hierarchy often suffice, even yielding exact bounds in certain cases—for instance, for the CH-inequality, the minimum detection efficiency is $\eta_{\text{crit}} \approx 66.7\%$ (Eberhard 1993), which can already be found using the '0'th level of the hierarchy, which simply optimizes over all no-signalling correlations.

In Fig. 4.4, we demonstrate the effect of including additional levels of the NPA-hierarchy on the lower bound for η_{crit}. There, detectors with a simulated efficiency of 90% were used to perform random measurements on maximally entangled two-qubit states, until a Bell inequality violation was detected. Then, using the coefficients of the Bell inequalities generated, lower bounds on the critical detection efficiencies were calculated using the NPA-hierarchy up to the third level, which however did not yield an appreciable increase over the second.

The above scenario assumes that both detectors have the same efficiency. Clearly, this is not an assumption we would want to make in the fully device-independent scenario. If both detectors are unknown, the lowest bound for the detection efficiency of one detector is achieved by assuming that the other detector is perfect. Thus, taking into account the quantum violation Q, the bound for the unknown detector in this case is

$$\eta_{A,\text{crit}} = \frac{Q - \sum_j h_{B_j} p(B_j^+)}{\sum_{ij} h_{A_i B_j} p(A_i^+ B_j^+) + \sum_i h_{A_i} p(A_i^+)}. \tag{4.39}$$

For the CH-inequality, its mere violation suffices to certify a bound of $\eta_{A,\text{crit}} = 0.5$. However, other inequalities allow the certification of better lower bounds. Take, for example, the Bell inequality defined by the coefficients in Table 4.2, which has $n = 6$ and $m = 5$ measurements, and was found using our method by performing random unit-efficiency measurements on a maximally entangled two-qubit state.

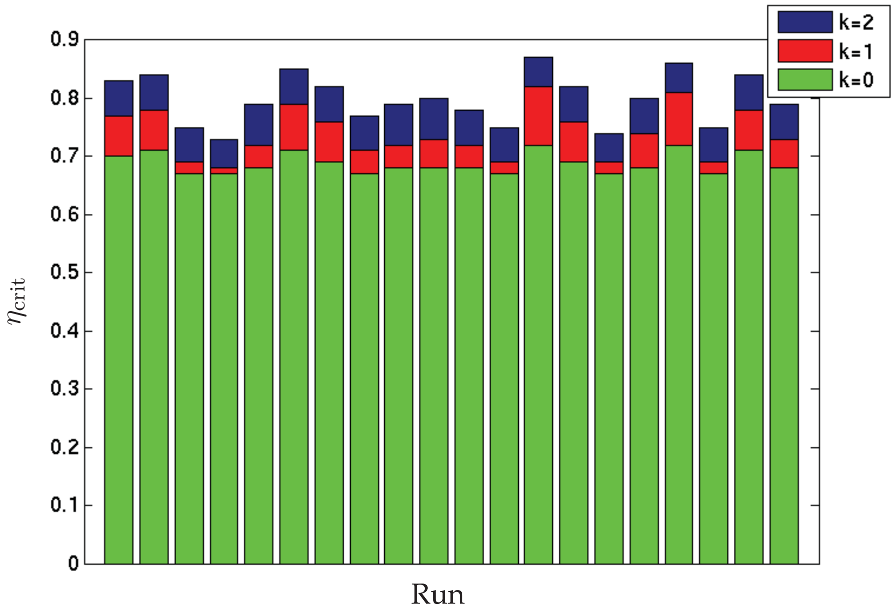


FIGURE 4.4: Effect of using further levels of the NPA-hierarchy. To generate the plot, random measurements were performed by detectors with a simulated efficiency of $\eta = 0.9$ on a maximally entangled 2-qubit state until a Bell inequality violation was detected. Then, the critical detection efficiency was computed on different levels of the NPA-hierarchy, starting with the 0th level, which merely tests the no-signalling constraint. The third level was also tested, but yielded no further improvement.

TABLE 4.2: Coefficients for a Bell inequality with $n = 6$ and $m = 5$ measurements. The first column and the top row yield the coefficients h_{A_i} and h_{B_j} respectively, while the entry (i, j) of the remaining array yields the coefficient $h_{A_iB_j}$.

	-2	-6	-4	-6	-6
-4	6	0	2	2	-2
-6	-6	6	6	2	4
-6	0	3	-2	5	5
-4	0	-3	-2	6	6
-6	6	6	0	-6	6
0	-2	0	4	4	-6

This Bell inequality, in the symmetric case, is violated if both detectors exceed an efficiency of $\eta_{\text{crit}} > 0.86$ (this and all following values were calculated using the second level of the NPA-hierarchy). If we set $\eta_B = 1$, the mere violation still serves to certify $\eta_A > 0.751$, which is already substantial. Furthermore, in the simulation, a violation of $Q = 1.971$ was produced (an upper bound for the maximal violation computed using the second level of the NPA-hierarchy is $Q_2 = 3.6791$), which suffices to certify a minimum detection efficiency of $\eta_A > 0.886$.

Hence, even in the fully device-independent case, strong lower bounds on the detection efficiency of a single detector are achievable. Nevertheless, it may be beneficial to rely on a detector with a known upper bound η_{known} on its detection efficiency in order to characterize a completely unknown one. Thus, we now modify our scenario slightly, and assume that you brought an old detector that you wish to replace with a certifiably better one with you. To illustrate this approach, in Fig. 4.5, the lower bound on the detection efficiency of the unknown detector is plotted against the efficiency of the known detector for testing the CH-inequality with a quantum violation in the range of $Q = \{0.04, 0.08, 0.12, 0.16, 0.2\}$.

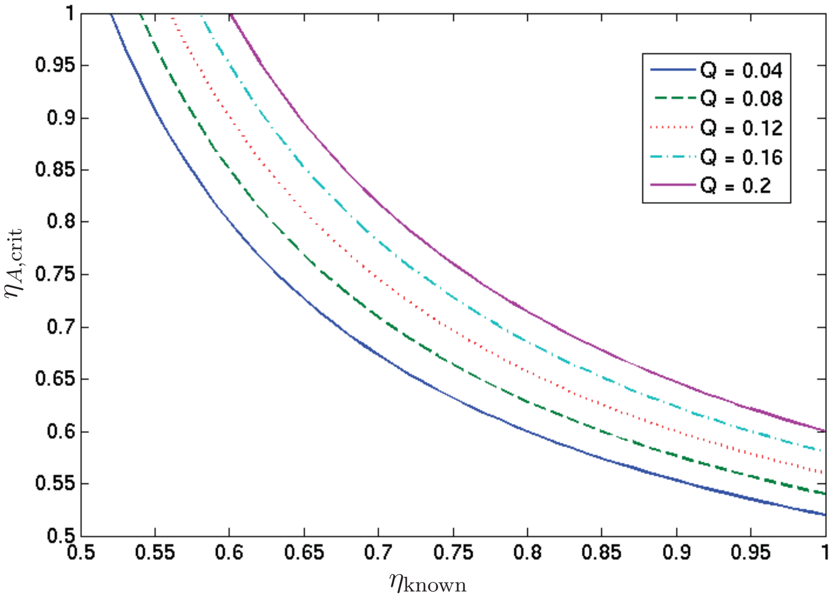


FIGURE 4.5: Certified lower bound on the detection efficiency of an unknown detector versus the efficiency of the known detector using the CH-inequality for the indicated quantum violations Q.

Thus, we see that the method of using Bell inequality violations constructed from nothing but the observed measurement statistics, besides the already-mentioned applications to finding Bell inequality violations independent of a global reference frame, device-independent entanglement detection of unknown states, and quantum cryptography, serves to establish bounds on detection efficiency both in the fully device-independent case, and in the case where one detector is (at least partially) characterized. This represents a novel advantage of using quantum mechanical, as opposed to classical, resources.

Chapter 5

Their Foundations

In the previous chapter, we have described a novel task where using quantum mechanical resources confers an advantage as compared to classical resources. Besides the potential practical uses of such a method, finding such advantages also helps to more precisely delineate the boundary between quantum and classical theories. That is, viewed from the operational framework as introduced in Sec. 1.1, we may view classical and quantum theories as theories allowing (or prohibiting) certain tasks, such that they can be used to characterize these theories. We have already seen several examples of such tasks: classical information can be copied, while information in quantum states, in general, cannot (see Sec. 2.2.1); quantum mechanics allows for secure key distribution, whereas this security cannot be guaranteed in the classical world; and so on.

It is remarkable that few such operational constraints suffice to isolate quantum theory within a broad class of theories. Clifton, Bub, and Halvorson (2003) postulate the following three constraints:

1. *No signalling*: information cannot be transmitted between two parties faster than light.

2. *No broadcasting*: for a given state ρ and a reference state σ, there exists in general no transformation T such that

$$\mathrm{tr}_A\left(T(\rho\otimes\sigma)\right)=\mathrm{tr}_B\left(T(\rho\otimes\sigma)\right)=\rho, \tag{5.1}$$

   that is, which leaves all reduced states equal to the original ρ (this is essentially a generalization of the no-cloning theorem to include the case of mixed states).

3. *No (unconditionally secure) bit commitment*: there exists no protocol such that Alice sends Bob an encrypted bit of data, which Bob can only decode upon receiving additional information from Alice, such that Alice cannot cheat, i.e. change the information contained in the bit after having sent it to Bob (i.e. she is 'committed' to that information).

They show that these suffice to isolate important properties (e.g. the existence of non-simultaneously measurable effects and entanglement) of quantum mechanics within a class of theories including classical theories and theories more general than quantum mechanics.

The basic goal behind such a characterization of quantum mechanics is to recast it in the form of a *principle theory*. Here, a principle theory is a theory whose empirical content is deducible from a few postulates (or even a single one), ideally of transparent physical or operational content. An archetypical example of such a theory is special relativity. Ultimately, all of its novelty (as compared to Newtonian mechanics) stems from the adoption of two empirically motivated principles (Einstein 1905):

1. *Relativity*: the same physical laws hold across all inertial frames of reference.

2. *Constancy of the speed of light*: the speed of light is the same in all frames of reference, regardless of the motion of the source.

The combination of these principles yields the full empirical content of special relativity—the impossibility of defining a universal standard of simultaneity, relativistic length contraction, time dilation, the equivalence of mass and energy, the existence of a universal speed limit, and so on. Thus, the entire catalogue of phenomena special relativity gives rise to is, in some way, implicit within these two simple postulates of transparent physical meaning. Ultimately, these postulates root the abstract mathematical apparatus of special relativity in simple physical facts.

The question that projects such as the one of Clifton, Bub, and Halvorson (2003) now attempt to address is: does there exist a similar set of postulates, likewise rooting the diverse phenomena of quantum mechanics within transparent physical (or operational, or information-theoretic) postulates?

Besides their formulation, there exist several other approaches aimed at identifying the principles of quantum mechanics. We will not attempt here a survey of these proposals, much less an evaluation of their relative strengths and failings. Rather, we will pinpoint a common notion that is present in several recent reconstructions of quantum mechanics—namely, the idea of an *epistemic restriction*: the existence of an in-principle bound on the knowledge that is obtainable about a given physical system. Later on, we will give arguments for how such a restriction naturally arises in certain kinds of systems.

Before proceeding with this task, though, we will give a (somewhat heuristic) motivation outlining how quantum mechanics may be derived, in a way analogous to special relativity, by adding a further constraint—a new principle—to the original classical formulation.

5.1 Reconstructing Quantum Mechanics

In order to explore the relationship between classical and quantum mechanics, it is advantageous to cast both into the same mathematical framework. Usually, quantum mechanics, with its noncommutative algebra of observables acting on complex Hilbert spaces, seems to be a very different beast from classical mechanics, where observables form a commutative algebra of smooth real-valued functions on, e.g., phase space. However, it was realized early on that this is not a fundamental distinction: Koopman (1931) and von Neumann (1932) showed that classical mechanics can be recast in the language of operators on Hilbert spaces; likewise, Groenewold (1946) and Moyal (1949), building on earlier work by Weyl (1927) and Wigner (1932), provided a formulation of quantum mechanics on phase space.

Indeed, we have already introduced a framework capable of encompassing both quantum and classical theories, as well as more general ones, in the GPT-framework introduced in Sec. 1.1. However, this framework starts out assuming the probabilistic nature of these theories; since the fact that quantum mechanics yields only probabilistic predictions was an early reason for skepticism regarding its completeness, we instead need a framework that includes the deterministic Newtonian theory, and take our leave from there.

It is thus the formulation of quantum mechanics in phase space that will be of particular interest for us. Formulating quantum mechanics in phase space allows us to pinpoint the areas of agreement with and divergence from classical mechanics more accurately, and thus, serves to elucidate what kind of new principle is needed in order to arrive at the novelties of quantum mechanics. For an overview of phase space quantum mechanics, see e.g. (Curtright and Zachos 2012).

5.1.1 Phase-Space Quantum Mechanics

We begin this short introduction to quantum mechanics in phase space with a brief reminder of some of the fundamental quantities of classical mechanics in its phase-space formulation. The classical phase space Π_S of an n-particle system S is a $6n$-dimensional manifold spanned by the system's generalized momenta $\boldsymbol{q}$ and positions $\boldsymbol{p}$. The system's state $\boldsymbol{x} = (\boldsymbol{q}, \boldsymbol{p}) = (q_1, \ldots, q_n, p_1, \ldots, p_n)$ is a given point of Π_S. Observable quantities are given by smooth real-valued functions on phase space, which are composed using the pointwise product—given two functions f and g, their product fg is the function

$$(fg)(\boldsymbol{x}) = f(\boldsymbol{x})g(\boldsymbol{x}). \tag{5.2}$$

The time evolution of the system is governed by Hamilton's equations (see Eq. 1.1). By means of the *Poisson bracket*

$$\{f, g\} = \sum_i f \left(\overleftarrow{\partial}_{q_i} \overrightarrow{\partial}_{p_i} - \overleftarrow{\partial}_{p_i} \overrightarrow{\partial}_{q_i} \right) g, \tag{5.3}$$

where the arrows on the partial derivatives indicate whether they act on functions on the left or right, Hamilton's equations become

$$\begin{aligned} \frac{\mathrm{d}q_i}{\mathrm{d}t} &= \frac{\partial H}{\partial p_i} = \{q_i, H\}, \\ \frac{\mathrm{d}p_i}{\mathrm{d}t} &= \frac{\partial H}{\partial q_i} = \{p_i, H\}; \end{aligned} \tag{5.4}$$

and for a general observable f, we have

$$\frac{\mathrm{d}f}{\mathrm{d}t} = \{f, H\}. \tag{5.5}$$

In general, the Poisson bracket can be interpreted as giving the rate of change of an observable given the translations induced by the other; hence, since the Hamiltonian generates time translations, the Poisson bracket of an observable with the Hamiltonian yields the former's time evolution.

Often, we do not have perfect information about the state $\boldsymbol{x}$ of a given system. As an example, the precise values of positions and momenta of the molecules in a single mole of gas constitute an unmanageable amount of data, and hence, we must instead consider a description of the system that takes the ignorance of the complete state of the system into account. Such a description is given by the *Liouville distribution* $L(\boldsymbol{p}, \boldsymbol{q}, t)$, which is defined such that $L(\boldsymbol{p}, \boldsymbol{q}, t)\, \mathrm{d}^n\boldsymbol{p}\, \mathrm{d}^n\boldsymbol{q}$ yields the probability of finding the system in the infinitesimal phase space volume $\mathrm{d}^n\boldsymbol{p}\, \mathrm{d}^n\boldsymbol{q}$ at time t. Its total time derivative vanishes,

$$\frac{\mathrm{d}L}{\mathrm{d}t} = \frac{\partial L}{\partial t} + \sum_i \left(\frac{\partial L}{\partial q_i}\dot{q}_i + \frac{\partial L}{\partial p_i}\dot{p}_i \right) = 0, \tag{5.6}$$

which expresses the conservation of the volume bounded by neighboring phase space trajectories. Using Hamilton's equations to replace the time derivatives of positons and momenta, this then yields

$$\frac{\partial L}{\partial t} = -\{L, H\}. \tag{5.7}$$

Quantum mechanics can now be formulated in much the same terms: we remain in the arena of phase space, and observables remain the same smooth, real-valued functions as before. However, we must modify the algebra of observables: they are no longer composed as in Eq. 5.2, but rather, using the noncommutative *star product*

$$f \star g = \sum_i f \exp\left[\frac{i\hbar}{2}\left(\overleftarrow{\partial}_{q_i}\overrightarrow{\partial}_{p_i} - \overleftarrow{\partial}_{p_i}\overrightarrow{\partial}_{q_i}\right)\right] g. \tag{5.8}$$

Additionally, the Poisson bracket is replaced by the *Moyal bracket*

$$\{f, g\}_\star = \frac{1}{i\hbar}(f \star g - g \star f), \tag{5.9}$$

and Liouville's equation (Eq.5.7) becomes *Moyal's equation*

$$\frac{\partial W}{\partial t} = -\{W, H\}_\star, \tag{5.10}$$

where $W = W(q, p, t)$ is the *Wigner function* (Wigner 1932), a quasiprobability distribution (which may assume negative values) on phase space that reduces to the Liouville distribution in the limit $\hbar \to 0$.

Note that the above formulation of the star product makes the connection between the noncommutativity of the algebra of observables and the impossibility of a local realistic description manifest: the star product depends on all of the derivatives of the functions f and g. But for smooth functions, knowledge of all derivatives at a given point is equivalent to knowledge of the function across the whole space; hence, if we want to describe observables in quantum mechanics using real-valued functions instead of operators, we need to take the values of these functions at all points into account.

This yields a formulation of quantum mechanics that is completely equivalent to the standard Hilbert space formalism. This equivalence is made explicit by the *Wigner-Weyl transform*, which maps phase space functions to Hilbert space operators (*Weyl map*), or vice versa (*Wigner map*).

Thus, e.g., the Weyl transform of the Wigner function W is the density matrix ρ, and Moyal's equation becomes

$$\frac{\partial \rho}{\partial t} = -\frac{i}{\hbar}[\rho, H], \tag{5.11}$$

the familiar von Neumann equation governing the time evolution of the density matrix.

We now have a formulation of quantum mechanics within the same arena as classical mechanics. This allows us to elucidate their connection, and introduce a prospective new principle underlying quantum mechanics.

5.1.2 Deformations of Physical Theories

The formalism of phase space quantum mechanics allows us to view it as a *deformation* of classical mechanics. Here, a deformation of a mathematical object is, essentially, the introduction of a parameter (or a set thereof), such that the original object is recovered in a certain limit. This yields a family of new objects associated with each value of the parameter. In this sense, an ellipse is a deformation of a circle, since in the limit of vanishing eccentricity $\epsilon \to 0$, every ellipse becomes a circle.

For physical theories, deformations are a way to complete a theory to a new domain in such a way that the original theory is recovered in the appropriate limit (that is, in the theory's original domain of validity). In this sense, special relativity can be viewed as a deformation of Newtonian mechanics whose deformation parameter is the speed of light, c: letting formally $c \to \infty$, or equivalently, considering the domain $v \ll c$, again reproduces the Newtonian phenomenology. This gives an immediate interpretation of the postulate of the constancy of the speed of light as necessitating the deformation of the Newtonian theory, and thus, illustrates the connection between the physical principle and the mathematical formalism.

Now, can we speak of quantum mechanics as a deformation in the same sense? And if this is the case, does this help with our search for a principle of 'quantumness'?

We first observe that the star product of Eq. 5.8 can be written in terms of a power series (see, e.g., (Hirshfeld and Henselder 2002), which will guide much of our presentation in the following)

$$f \star g = \sum_{n=0}^{\infty} (i\hbar)^n C_n(f,g) = fg + i\hbar C_1(f,g) + O(\hbar^2), \tag{5.12}$$

which indeed reduces to the pointwise product in the (formal) limit $\hbar \to 0$. Here, the expressions $C_n(f,g)$ denote functions of the derivatives of f and g. In general, these may be arbitrary, thus yielding many potential deformations; however, it was shown by Gerstenhaber (1964) that requiring associativity of the new product places strong constraints on the C_n, essentially determining them uniquely in many cases. The requirement of associativity can be expressed as

$$\sum_{j+k=n} C_j(C_k(f,g),h) = \sum_{j+k=n} C_j(f, C_k(g,h)). \tag{5.13}$$

Furthermore, to yield the correct classical limit, we require that

$$C_0(f,g) = fg, \tag{5.14}$$

and

$$C_1(f,g) - C_1(g,f) = \{f,g\}. \tag{5.15}$$

The final requirement essentially expresses the *correspondence principle*: if we define the $\star$-commutator as

$$[f,g]_\star = f \star g - g \star f, \tag{5.16}$$

it can be written as

$$\lim_{\hbar \to 0} \frac{1}{i\hbar}[f,g]_\star = \{f,g\}, \tag{5.17}$$

that is, in the classical limit, the Poisson structure of phase space is recovered. It can then be shown (Gerstenhaber 1964) that the the Moyal star product of Eq. 5.8 fulfills these requirements (in the case of a flat Euclidean phase space).

There is, however, a question regarding the uniqueness of this scheme. We call two star products $\star$ and $\star'$ *c-equivalent* (where the c stands for *cohomology*) if there exists a transformation T with $T = \sum_{n=0}^{\infty} \hbar^n T_n$ such that

$$f \star' g = T^{-1}(T(f) \star T(g)). \tag{5.18}$$

Now, all star products consistent with the above requirements are c-equivalent; however, they constitute different quantization schemes, and in general, may yield different spectra for physical observables. Hence, additional physical requirements are needed to single out the appropriate scheme in any given case (Bayen et al. 1978a,b).

We will not discuss these difficulties any further in the following, and content ourselves with the above demonstration—which albeit remains heuristic—to motivate looking for the new principle of quantumness in the direction indicated by the idea that quantum mechanics should be regarded as a deformation of the classical theory due to the non-vanishing of Planck's constant $\hbar$. The idea then is that just as the finiteness of the speed of light entails the deformation of classical mechanics into the theory of special relativity, so does the existence of a nonzero $\hbar$ motivate the formalism of quantum mechanics.

However, what, exactly, is meant by 'nonzero $\hbar$'? There is a clear operational interpretation of the invariant speed of light: every measurement will yield the same value for c, regardless of the motion of the observer. What is the analogous interpretation of $\hbar$?

Several independent lines of reasoning suggest the interpretation that it essentially corresponds to an *epistemic restriction*: a nonzero $\hbar$, roughly, means that there exists a smallest volume beyond which the state of a system cannot be further 'localized' in phase space. We will clarify this notion in the following.

5.2 Self-Reference and Epistemic Restrictions

The discussion in the preceding Section suggests that quantum mechanics can be viewed as a deformation of classical mechanics, yielding a completion of the latter in the realm where the nonvanishing value of $\hbar$ becomes relevant—that is, the realm of small action S (see Chap. 1). In this section, we want to examine the suggestion that the positive value of $\hbar$ essentially constitutes an epistemic restriction. Here, an epistemic restriction means a restriction on the knowledge about a given physical system (from Greek *epistēmē*, meaning 'knowledge').

Several reconstruction attempts centrally feature such a restriction. In (Grinbaum 2003) three such attempts are discussed, due to Rovelli (1996), Brukner and Zeilinger (2003), and Fuchs (2002), and assumptions common to each are identified; in a similar vein, the approaches of Masanes, Müller, et al. (2013), and von Weizsäcker (1985) (for an English translation, see (von Weizsäcker, Görnitz, and Lyre 2006)) likewise include a bound on the knowledge obtainable for a single system. We will have a more detailed look at these examples, and their common assumptions, in the following.

5.2.1 Epistemic Restrictions and the Reconstruction of Quantum Mechanics

Grinbaum (2003) gives an overview over several distinct attempts at reconstructing the formalism of quantum mechanics from first principles, viewed from an information-theoretic vantage point. He notes that there exists a common thread across these reconstructions, in that they are broadly concerned with limits on the acquisition of information about physical systems. Thus, for instance, in his reconstruction of quantum mechanics, Rovelli (1996) proposes the following two principles:

(R1): "There is a maximum amount of relevant information that can be extracted from a system."

(R2): "It is always possible to acquire new information about a system."

Similarly, Brukner and Zeilinger (2003) propose that:

(BZ): "The information content of a quantum system is finite,"

which is an obvious cognate of 'Zeilinger's Principle' that an elementary system contains one bit of information (Zeilinger 1999). Furthermore, they introduce the notion of complementary observables, and postulate that maximal information about an observable entails zero information about all others—thus also introducing the possibility of acquiring novel information that cannot be reduced to the information already possessed about the system.

Fuchs (2002) considers that:

(F1): "There is maximal information about a system."

(F2): "There will always be questions that we can ask of a system for which we cannot predict the outcomes."

The approach of Masanes, Müller, et al. (2013) is located within the GPT-framework (see Sec. 1.1), where they propose as an 'information unit' the gbit, which is characterized as follows:

(M1): "[T]he state of a gbit can be characterized with a finite number of measurements. [...] [I]f a gbit is used to perfectly encode one classical bit, it cannot simultaneously encode any further information."

(M2): "[A]ll linear functions $E : \mathcal{S}_{\text{gbit}} \to [0, 1]$ correspond to outcomes of measurements that can in principle be performed."

Finally, an early example is provided by the reconstruction of quantum theory due to von Weizsäcker (1985), in terms of what he calls 'ur-alternatives' (where 'ur' means, roughly, primitive or primordial). He proposes that

(vW1): "[O]ne can lay down as a definition that to every 2^k-fold alternative will belong exactly the information k[.]"

(vW2): "[O]ne must add, however, that the decidability of this alternative itself implies a formally infinite quantity of other alternatives and thus of information belonging to the same object."

The common gist behind these formulations is a *finiteness assumption*, that is, an assumption stating that there is a finite maximum of information that can be extracted (via measurement) from a qiven system, and an *assumption of additional information*, according to which one can always acquire more information about a system.

At first blush, these assumptions appear contradictory: if maximal information about a system is known, then it seems no further information can in principle be attained. That this is not so is best demonstrated by appealing to the *toy theory* of Spekkens (2007). Spekkens postulates the *knowledge balance principle*:

(Sp): "If one has maximal knowledge, then for every system, at every time, the amount of knowledge one possesses about the ontic state of the system at that time must equal the amount of knowledge one lacks."

Here, the qualifier *ontic* (from Greek *ontos*, meaning 'of that which is') refers to the actual physical state of a system, to be constrasted with an *epistemic state*, which refers to a state of knowledge about a system. As an example, picture a system's actual phase space state $\boldsymbol{x} = (\boldsymbol{q}, \boldsymbol{p})$, in contrast with a Liouville distribution associated to it if this ontic state is not exactly known.

Spekkens' toy theory implements a version of the above assumptions: the knowledge one has is always finite; but, since there is more information contained in the state of a system in the theory, this information is, in principle, accessible to measurement—at the cost of invalidating previous information. This is, in fact, the emergence of a first characteristically quantum notion: after making a measurement, knowledge gathered during previous measurements may be obsolete; in this case, the two measurements are complementary.

The toy theory provides an accessible laboratory to demonstrate how certain quantum effects follow from epistemic restrictions of the above kind. Thus, we introduce it here in a little more detail.

The elementary system in the toy theory, the *toy bit* (tbit), is characterized by four different states t_1, t_2, t_3 and t_4; thus, two bits of information are needed to uniquely specify the state of a tbit. However, by the knowledge balance principle, only one bit is available at any time, and consequently, we can at most 'localize' any given tbit within a two-element subset of its state space. That is, there are six toy bit states of maximum knowledge, $\{t_1, t_2\}$, $\{t_2, t_3\}$, $\{t_1, t_3\}$, $\{t_2, t_4\}$, $\{t_1, t_4\}$, $\{t_3, t_4\}$, and one single state of less-than-maximal knowledge, here equivalent to the state of complete ignorance $\{t_1, t_2, t_3, t_4\}$.

Measurements in the toy theory distinguish between disjunct subsets of the state space. There are three different measurements; measurement outcomes for the different ontic states are shown in Table 5.1.

TABLE 5.1: Measurements in Spekkens' toy theory.

	t_1	t_2	t_3	t_4
m_z	1	1	0	0
m_x	1	0	1	0
m_y	1	0	0	1

Accordingly, the outcome 1 upon measuring m_x means that the tbit is in either the state t_1 or t_2; the outcome 1 for m_z means it is either in t_1 or t_4; and so on. Consequently, after obtaining the outcome 1 for m_x, the outcome of a m_z measurement is completely unknown.

However, suppose we now measure m_z, after having obtained the outcome 1 in an m_x-measurement. No matter what outcome we obtain, both bits of information, taken together, would suffice to exactly pinpoint the ontic state of the tbit, in violation of the knowledge balance principle. Consequently, the ontic state of the system must be changed upon obtaining the second bit of information, in such a way as to be consistent with the measurement outcome obtained upon measuring m_z, but not necessarily with the previously obtained result for the m_x-measurement. Thus, after the m_z-measurement, the outcome of any further m_x measurement must be completely uncertain. In this way, the knowledge balance principle introduces the phenomenon of complementarity.

Starting from this example, we can now examine the role played by epistemic restrictions in general in giving rise to quantum phenomena. As Rovelli (1996) observes, the finiteness assumption already introduces the constant $\hbar$ into the formalism: if there exists a maximum for the information that can be obtained about a given physical system, then there exists a smallest phase space volume such that a system cannot be localized further in phase space. Since this volume has the dimension $(\mathrm{kgm}^2\mathrm{s}^{-1})^{3n}$ for an n-particle system, this then implies the existence of a constant of dimension $\mathrm{kgm}^2\mathrm{s}^{-1}$ characterizing this minimum phase space volume, which is just the dimension of Planck's constant.

Thus, recalling the discussion of quantum mechanics as a deformation of classical mechanics in Sec. 5.1.2, the logic is the following: the finiteness assumption introduces the constant $\hbar$ into the phase space picture; furthermore, the assumption of additional information ensures that we do not simply end up with a discretized phase space, since we can, in principle, always acquire additional information—thus, we cannot simply divide the phase space into fixed cells of volume $\hbar^{3n}$, but must allow for the possibility of, e.g., increasing our knowledge of the position of a system at a corresponding cost regarding our knowledge of its momentum. Together, thus, the two principles introduce the necessity of deforming the formalism of classical mechanics to accurately account for phenomena where the bound on our maximal information becomes relevant. This is schematically represented in Fig. 5.1.

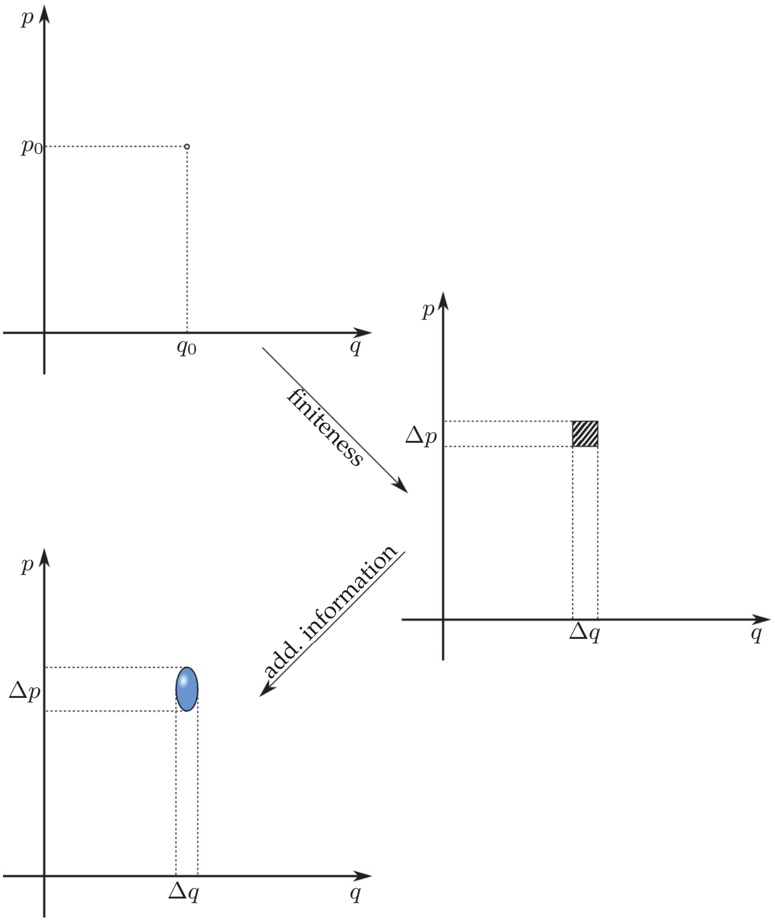


FIGURE 5.1: Effect of introducing the finiteness assumption and the assumption of additional information on the state of a system in phase space.

Consequently, if this program can be carried out to completion, we will obtain a foundation for quantum mechanics that rests on foundations similar to those of special relativity: quantum mechanics, on this view, is simply the completion of classical mechanics in the regime where we can no longer neglect the effects of the finite maximum of information that can be obtained about a system. In the same sense, special relativity is the completion of classical mechanics in the regime where we can no longer neglect the finite maximum speed of propagation of physical systems. Note that this, too, is sometimes formulated as a restriction on information: namely, the speed of light poses a limit on how fast information propagates through spacetime—thus e.g. leading to the no-signalling principle.

However, this still leaves a question open: what is it that prohibits us from acquiring more information about a given system? The analogous question in special relativity receives an answer from the geometry of Minkowski spacetime: for spacetime events A and B, if they are separated such that no speed-of-light signal could reach one from the other, there always exist frames of reference R and R' such that A occurs before B in R, but after B in R'. Consequently, for any signal passing between them, an observer in R would perceive it as moving from A to B, while an observer in R' would see it moving from B to A, making a causal ordering of both events impossible.

Is there a similar foundation for the epistemic restrictions giving rise to quantum phenomena? In the following, we give a candidate for such a foundation, by deriving intrinsic limits on the ability to predict measurment outcomes, and on the accuracy with which a given system can be 'localized' within its state space. To set the stage, we provide a brief excursus discussing the connection between randomness, mathematical undecidability, and epistemic restrictions.

5.2.2 Randomness and Undecidability

The fact that for every quantum state, certain measurements yield random outcomes, is one of the most salient features of quantum theory. Furthermore, it was at the center of early worries regarding the completeness of quantum theory: in classical theories, randomness only occurs due to ignorance of the complete physical state; hence, it seems natural to wonder whether quantum mechanics really constitutes a fundamental theory, or if there could be some completion eliminating this randomness.

As we have seen, there are strict constraints on any putative completion, given (among others) by the no-go results discussed in Sec. 2.2. We will thus take quantum randomness as given, and instead continue the present thread of investigation by asking for its origin.

First of all, it is clear that in any theory based on the epistemic restrictions discussed above, certain measurement outcomes must be random. The assumption of additional information entails that there are measurement outcomes that are not predictable from maximal knowledge about a physical system; these outcomes must hence be random. We can see this, again, explicitly in the toy theory: after a measurement, the ontic state is randomized among the possibilities consistent with this outcome, in order to uphold the knowledge balance principle, thus yielding an analogue of the projection postulate for this theory.

Now, mathematically, there exists a close connection between randomness and the notion of *undecidability* (for an in-depth study on the connection between these concepts and their application to physics, see (Svozil 1993)). Famously, Gödel (1931) proved that any (consistent) theory capable of finitely axiomatizing (a certain fragment of) elementary number theory contains propositions that are not decidable from the axioms of this theory. Similarly, Turing (1936) demonstrated the existence of functions that cannot be computed by any Turing-machine equivalent device—which, if we assume the Church-Turing thesis (Kleene 1943), entails that there exist questions such that there is no algorithmic means of answering them (with the prototype of such a question being the famous *halting problem*, i.e. the question of whether a given machine will eventually halt on a given input).

These arguments make use of the notion of *self-reference*: an axiomatic system strong enough to encode number theory can encode propositions about itself (demonstrating this was a major part of Gödel's ingenuous proof), which may yield paradoxical consequences, such as in the famous Epimenides- or liar-paradox of uttering the sentence 'this sentence is false'.

A particularly elegant demonstration of the connection between randomness and undecidability is given by *Chaitin's constant*. Chaitin's constant for a (possibly universal) Turing machine U is given by (Chaitin 1975)

$$\Omega_U = \sum_{x:U(x)\,\text{halts}} 2^{-|x|}. \tag{5.19}$$

Here, x denotes the (binary representation of) a program on a so-called *prefix-free set*, that is, a set of programs such that if x is a valid program, no x' such that x' is an extension of x (i.e. the first $|x|$ bits of x', where $|x|$ denotes the length of x, are equal to x) is also a valid program. Together with Kraft's inequality (Kraft 1949), this requirement ensures that the sum converges to a real number between 0 and 1. Ω_U can then be interpreted as the probability that U halts, given a random program, and is thus often referred to as *halting probability*.

Ω_U must be uncomputable, since knowledge of the precise value of its first n bits allows solving the halting problem for all programs of less than n bits length (Chaitin 1975): one runs all programs of less than n bits in parallel (by a dovetailing process), and adds the corresponding factor for each program that has halted to an estimate for Ω_U; as soon as that estimate reaches the true value, one knows that none of the programs that are still running will halt.

Furthermore, for each axiomatic system (again at least strong enough to axiomatize number theory), there exists a constant k such that the system cannot decide the value of any bit beyond the kth; that is, the values of these bits are undecidable statements (this is a consequence of *Chaitin's incompleteness theorem* (Chaitin 1974); see also Sec. 5.2.5).

Finally, Chaitin's constant is *algorithmically random*—and indeed, any algorithmically random number such that there exists a computable series of rational approximations from below for this number (i.e. such that is is *recursively enumerable*) is a Chaitin constant for some Turing machine U (Calude, Hertling, et al. 1998). Here, algorithmic randomness is defined using the notion of *Kolmogorov complexity* (Kolmogorov 1963).

The Kolmogorov complexity $K(\sigma)$ of a string σ is the length of the shortest program x for a given Turing machine U (which takes as programs strings from a prefix-free set) such that it produces σ, i.e.

$$K(\sigma) = \min_{x:U(x)=\sigma} |x|. \tag{5.20}$$

Note that the Kolmogorov complexity of a string σ is uncomputable; indeed, if one could compute Kolmogorov complexity, one could also solve the halting problem (Chaitin, Arslanov, and Calude 1995).

An important property of Kolmogorov complexity is the *invariance theorem*: for two different universal Turing machines U and U', the Kolmogorov complexity of a string σ differs by at most an additive constant c, since for any program x for U, it holds that there exists a program y for U' with $|y| < |x| + c$ such that

$$U(x) = U'(y), \tag{5.21}$$

such that consequently, the length of the shortest program producing σ on U' is at most the length of the shortest program on U, plus the constant c.

A string σ is then algorithmically random roughly if its Kolmogorov complexity is equal to its length (up to an additive constant): in this case, the number is incompressible, and hence, there is no 'law' according to which it is generated. More precisely, an infinite string σ is algorithmically random if there exists a constant c such that for any n-bit prefix σ_n of σ (that is, a string containing the first n bits of σ) (Levin 1973; Schnorr 1973),

$$K(\sigma_n) > n - c. \tag{5.22}$$

It can be shown that this notion of randomness is equivalent to other notions, e.g. Martin-Löf randomness (Martin-Löf 1966). Hence, Chaitin's constant shows a direct connection between the undecidable propositions corresponding to the digits of the halting probability (beyond some given index k), and its random nature.

At first, it is not clear that these formal results should have any application to physics. However, it is possible to realize instances of undecidable questions within physical systems: certain physical systems are equivalent to Turing machines, and consequently, questions about their properties may be mapped to undecidable questions about their equivalent Turing machines. Such an equivalence was recently used by Cubitt, Perez-Garcia, and M. M. Wolf (2015) to show that the question of whether a system possesses a spectral gap—i.e. a finite energy difference between the ground state and the first excited state—is undecidable. They used a mapping between the ground state of spin systems and the problem of tiling the plane with tiles having colored edges, such that only the same colors meet, which is known to be undecidable (Berger 1966). Earlier results along similar lines had been obtained by Lloyd (1993, 1994). Since this is an in principle measurable quantity, the outcome of this measurement hence must be undecidable.

Other applications of undecidability to physics exist. Perhaps the first application is due to Popper (1950a,b), who argued that no physical system can, in general, perfectly predict its own behavior. More intriguingly, the notion of self-reference and the paradoxes it yields has been applied to the notion of measurement in quantum mechanics in several ways. Dalla Chiara (1977) considers the question from the point of view of quantum logic, while Zwick (1978) speculates that the result of the state reduction after a measurement might be analogous to a proposition undecidable from the information encoded in the state beforehand.

A related point of view is offered by Peres and Zurek (1982), who claim that the inability of quantum theory to completely describe the measurement process is a logical necessity analogous to Gödel's theorem. In a similar vein, Breuer (1995) shows by a self-referential argument that it is impossible for a given observer to accurately distinguish all states of a system that includes itself as a proper part, while Aerts (2005) shows that there are properties pertaining to the observer that cannot be perfectly observed. Also of interest is the result of Calude and Stay (2007) showing that an uncertainty principle between two observables implies an incompleteness result relating the value of a real number and the knowledge of the length of the shortest program computing it.

More recently, Brukner (2009) and Paterek et al. (2010) have demonstrated that the outcome of a quantum measurement is random exactly if a proposition encoded within the measurement is undecidable from information encoded within the quantum state—however, the axiom systems they use are very simple, and, in principle, completable. Finally, Eisert, Müller, and Gogolin (2012) could show that whether a given port of a measurement apparatus ever yields a detection is an undecidable question.

We have seen that there is a broad array of literature on the connection between quantum mechanics, its randomness, and mathematical undecidability. The idea to explore this connection as yielding the sought-for foundational principle for quantum mechanics seems to have first been entertained by Wheeler: in notes that have only recently been published online, he proposed that the 'point of origin' of the quantum principle are the '"undecidable propositions" of mathematical logic' (Wheeler 1974). Indeed, Wheeler had once confronted Gödel with the question of what connection the latter saw between his incompleteness theorem and Heisenberg's uncertainty relation; however, Gödel was apparently not too taken with the idea, as he reportedly 'threw [Wheeler] out of his office' (cf. the account provided in (Barrow 1999, p. 221)).

Gödel's reservations notwithstanding, we will in the following explore the possibility of giving Wheeler's notion—what he sometimes called 'an idea for an idea' (see e.g. (Buckley and Peat 1996, p. 87))—a more stringent formulation. In order to do so, we will first introduce some necessary notions and notations.

5.2.3 Properties and Measurements

We consider a physical system S to be represented by its state space Σ_S. For generality, we do not wish to make too many assumptions about this state space; it can be thought of as the collection of states s, where a state is a mathematical object containing all information about the system. To guide intuition, one may imagine this state space as analogous to phase space, and the state then as a given phase space point.

Not every state space is suitable for a physical theory, however. A first requirement is that Σ_S be a *metric space*, that is, a space such that there exists, for any two elements s and s', a distance $d(s,s')$ such that

$$\begin{aligned} d(s,s') &\geq 0, \\ d(s,s') &= 0 \Leftrightarrow s = s', \\ d(s,s') &= d(s',s), \\ d(s,s'') &\leq d(s,s') + d(s',s''). \end{aligned} \tag{5.23}$$

This is due to the fact that we want to be able to compare two states, e.g. to assess how close a prepared state is to some given target state, or to quantify experimental errors via the spread of states reconstructed from a series of independent experiments.

Additionally, measurement data is always finite, simply due to the fact that it must be stored in some way—in memory, on a notepad, or in a computer. Thus, data belongs to a set that is at most countable, i.e. of the cardinality of the natural numbers $\mathbb{N}$, since there exists a one-to-one correspondence between finite strings in some (finite) alphabet and the natural numbers. To then tell two states s and s' apart, we must be able to approximate either arbitrarily well using these finite pieces of data.

What it means to be able to differentiate between s and s' using our finite pieces of data now is the following: there exists some mapping from the (countable) set of data to states of Σ_S; call states in the image of this mapping *reconstructible*. Then, we say that a reconstructible state s^* *ϵ-approximates* s if s^* lies in an ϵ-neighborhood of s. Here, an ϵ-neighborhood of a state s is an open ball with radius ϵ, that is, the set

$$B_\epsilon(s) = \{s' \in \Sigma_S | d(s, s') < \epsilon\}. \tag{5.24}$$

Then, to differentiate between two arbitrary states s and s', we need to be able to find an ϵ and a state s^* reconstructible using our finite data such that s^* ϵ-approximates s, but not s' (or vice versa). This is the case if and only if the set of states reconstructible from finite data lies dense in the state space Σ_S: for a subset Y of X to lie dense in X merely means that any neighborhood of elements from X contains at least one element of Y. A set containing a countable dense subset is called *separable*.

As we have seen, our state space Σ_S needs to be a separable metric space. A consequence of this is that its cardinality can at most be that of the set $\mathbb{R}$ of real numbers (Aliprantis and Border 2006), standardly denoted $\mathfrak{c}$. In the following, we will thus assume that the cardinality of all state spaces considered is equal to $\mathfrak{c}$, unless explicitly noted otherwise; this is justified by the fact that in general, even the simplest systems—e.g. a point of mass moving in one dimension—already have a continuous space of states available to them.

With the notion of state space in hand, we can now define a *property* π as simply a subset of state space, $\pi \subset \Sigma_S$. Any state $s \in \pi$ possesses the property, while states in the complement $\pi^\perp$ do not possess it. This is again in analogy to a phase space-based description: consider, for example, the property 'having energy less than E_0', which is simply the set $\pi_{E_0} = \{s \in \Sigma_S | H(s) < E_0\}$, where H is the Hamiltonian of the system.

The set of all properties of S then is the powerset 2^{Σ_S}, i.e. the set of all subsets of Σ_S. An equivalent interpretation of 2^{Σ_S} is as the set of all *indicator functions* $m_\pi : \Sigma_S \to \{0, 1\}$, which yield 1 for all $s \in \pi$, and 0 for all $s \in \pi^\perp$. We can consider the indicator function m_π to yield the truth value of the proposition 'S has property π in state s'.

This truth evaluation by means of indicator functions forms the basis of a propositional calculus that can be used to reason about properties of a system. There exists a (partial) ordering relation given by set inclusion, such that for all properties π_a, π_b, and π_c

$$\begin{aligned}
&\pi_a \subseteq \pi_a, \\
&\pi_a \subseteq \pi_b,\ \pi_b \subseteq \pi_a \Leftrightarrow \pi_a = \pi_b, \\
&\pi_a \subseteq \pi_b,\ \pi_b \subseteq \pi_c \Rightarrow \pi_a \subseteq \pi_c.
\end{aligned} \tag{5.25}$$

We can view this ordering as yielding a logical implication relation, such that for propositions a and b (where we may read, e.g., a as the proposition 'S has property π_a') $a \rightarrow b$ (read: 'a implies b') whenever $\pi_a \subseteq \pi_b$. To emphasize its role as an ordering relation, we will also write $a \leq b$ if $\pi_a \subseteq \pi_b$. Additionally, set intersection $\pi_a \cap \pi_b$ and union $\pi_a \cup \pi_b$ defines logical connectives $a \wedge b$ and $a \vee b$, respectively, while negation is given by the complement, i.e. if a is true of all elements of π_a, then $\neg a$ holds of all elements of $\pi_a^\perp$. The set Σ_S, equipped with set inclusion as ordering relation and set intersection and union then forms a *lattice*.

The effect of epistemic restrictions can also be illustrated at this level: as shown by Grinbaum (2005), the finiteness assumption entails that the lattice of propositions as defined above is *orthomodular*, i.e. that the inference

$$a \leq b \rightarrow a \vee (a^\perp \wedge b) = b \tag{5.26}$$

holds. Such orthomodular lattices are important in the field of *quantum logic*: a quantum logic is the logical calculus formed by the lattice of subspaces of Hilbert space with subspace inclusion as partial order relation (Birkhoff and von Neumann 1936). Such lattices are orthomodular, and hence, the epistemic restriction induces a logic isomorphic to quantum logic.

Orthomodularity can be considered as a weakening of the notion of *distributivity*. A lattice is distributive if

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \tag{5.27}$$

(and likewise with the connectives reversed). Famously, distributivity holds in classical logic, but not in quantum logic, where we can view classical logic as the lattice of subsets of phase space, together with set inclusion as ordering relation.

Take for instance the following propositions:

- a: The particle's momentum is in the interval $[0, \frac{1}{2}]$.
- b: The particle's position is in the interval $[0, \frac{1}{2}]$.
- c: The particle's position is in the interval $[\frac{1}{2}, 1]$.

Then, the proposition

$$a \wedge (b \vee c), \tag{5.28}$$

for a certain particle, may evaluate to *true*, since the uncertainty principle yields $\Delta p \Delta q \geq \frac{1}{2}$, in units where $\hbar = 1$. However, the proposition

$$(a \wedge b) \vee (a \wedge c) \tag{5.29}$$

is necessarily *false*, since both $a \wedge b$ and $a \wedge c$ imply an uncertainty of $\frac{1}{4}$, in violation of the uncertainty principle, and hence, both evaluate to *false*. Consequently, distributivity fails to hold in the quantum world; and moreover, this failure can be attributed to the nonvanishing of $\hbar$, which comes about due to the epistemic restriction.

Using the calculus as developed so far, we can combine properties logically. A system that possesses properties π_a and π_b, likewise possesses the property $\pi_{ab} = \pi_a \cap \pi_b$; if every system that possesses property π_a also possesses property π_c, then π_a implies π_c (see the illustration in Fig. 5.2).

Thus, certain properties of a system in state s suffice to determine others; more generally, since every singleton subset of a set can be considered as the intersection of all subsets containing the singleton, we can equivalently specify the state of a system by giving a list of properties such that all properties of the system can be inferred from this list.

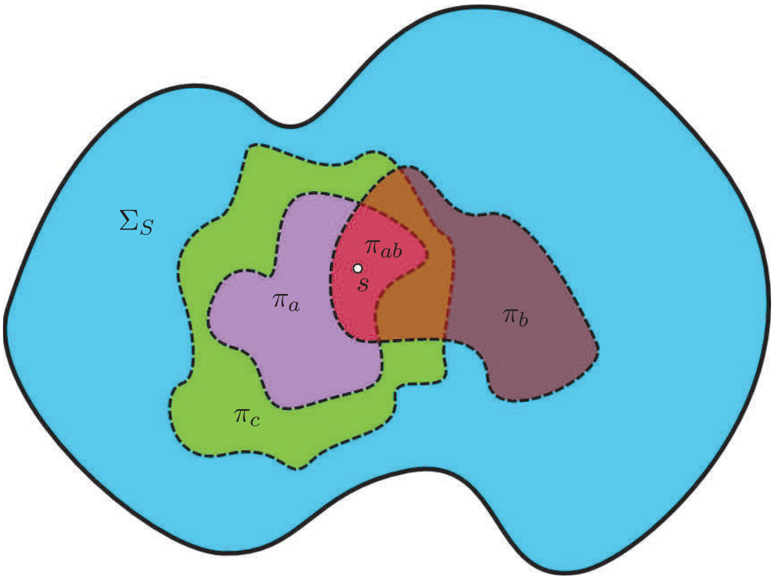


FIGURE 5.2: A state space Σ_S together with a state s, three properties π_a, π_b, and π_c, as well as their logical relations.

Let us now introduce the *measurement apparatus* A upon which we place no restriction other than that it is a physical system, and hence, possesses a state space Σ_A of cardinality $\mathfrak{c}$. A measurement apparatus is any system A that can perform *tests* on an (object) system S, such that for a certain property π, A produces the outcome 1 if S possesses that property in state s, and 0 otherwise. Hence, A effectively evaluates the characteristic function of the property π.

Furthermore, we imagine that A is equipped with a memory, such that it can store the results of previous measurements, and, moreover, that it is capable, using this stored information, to make predictions regarding the outcome of future measurements. In order to do so, A must in general be equipped with a device capable of universal computation; call an A that fulfills this requirement a *universal observer*. This models the scenario in real experiments: in general, the experimenter is able to perform arbitrary measurements, and manipulate the data thus obtained in arbitrary ways. Indeed, any experimenter equipped with enough scratch paper and ink can perform universal computation.

Now, if there are no epistemic restrictions, then A can, in principle, obtain sufficient information about the state of S to decide the outcome of any measurement in advance. We will call any theory in which this is possible (if only in principle, i.e. in the limit of infinite resources needed for full universal computation) a *classical* theory, and formulate the following

> **Criterion of classicality.** If it is possible in principle to obtain sufficient information about the state s of a given system S, such that all further measurement outcomes can be uniquely predicted from this information, then the theory is *classical*.

This criterion is exactly what the assumptions of finiteness and additional information deny: in theories in which these hold, no specification of a state s exists such that knowing this specification, all measurement outcomes become predictable (this is sometimes also expressed as these theories not having any *dispersion-free states*, i.e. states for which every observable assumes a sharp value, see e.g. (Bell 1966)).

These notions may become more clear by using again the toy theory as an example. The toy bit's (ontic) state space is simply the set $\Sigma_T = \{t_1, t_2, t_3, t_4\}$. There are three properties each toy bit can have, as given by the domains of the indicator functions (measurements) m_x, m_y, and m_z. Together with their complements, these are the subsets

$$\begin{aligned} \{t_1, t_2\} &\equiv \pi_x, \quad \{t_3, t_4\} \equiv \pi_x^{\perp}, \\ \{t_1, t_3\} &\equiv \pi_y, \quad \{t_2, t_4\} \equiv \pi_y^{\perp}, \\ \{t_1, t_4\} &\equiv \pi_z, \quad \{t_2, t_3\} \equiv \pi_z^{\perp}. \end{aligned} \tag{5.30}$$

Any two of these suffice to infer the third, and thus, yield complete knowledge about the state. Hence, we can represent the states via the properties; it turns out that there are three distinct ways to do so for each state:

$$\begin{aligned} t_1 &: (\pi_x^{(1)}, \pi_y^{(1)}) \equiv (\pi_x^{(1)}, \pi_z^{(1)}) \equiv (\pi_y^{(1)}, \pi_z^{(1)}) \\ t_2 &: (\pi_x^{(1)}, \pi_y^{(0)}) \equiv (\pi_x^{(1)}, \pi_z^{(0)}) \equiv (\pi_y^{(0)}, \pi_z^{(0)}) \\ t_3 &: (\pi_x^{(0)}, \pi_y^{(1)}) \equiv (\pi_x^{(0)}, \pi_z^{(0)}) \equiv (\pi_y^{(1)}, \pi_z^{(0)}) \\ t_4 &: (\pi_x^{(0)}, \pi_y^{(0)}) \equiv (\pi_x^{(0)}, \pi_z^{(1)}) \equiv (\pi_y^{(0)}, \pi_z^{(1)}) \end{aligned} \tag{5.31}$$

Here, the notation $\pi_i^{(v)}$ with $v \in \{0, 1\}$ denotes whether the system in the given state has ($v = 1$) or does not have ($v = 0$) the property π_i.

Consequently, if we could know the value of two properties in the toy theory, we would know the entire state, and thus, the outcome of every further measurement, fulfilling the criterion of classicality. However, this is exactly what the knowledge balance principle forbids.

Using the machinery developed above, we will now have a look at the question of whether it is possible, in principle, to predict every conceivable measurement outcome, given sufficient information about the system.

5.2.4 Not all Measurement Outcomes can be Predicted

There exists a broad similarity between many of the paradoxes of self-reference. This similarity was brought to the fore by Lawvere (1969), who showed that many of these results follow from a fixed-point theorem in the setting of Cartesian closed categories (CCCs). Here, a *category* C is a mathematical structure comprised of a class of *objects*, $\mathrm{ob}(\mathsf{C})$, a class $\mathrm{hom}(\mathsf{C})$ of *morphisms* (or *arrows*) connecting a source object X with a target object Y (i.e. $f : X \to Y$), a *composition relation* $\circ$ that allows associative composition of morphisms, and an *identity morphism* $1_X : X \to X$ for every object X.

Furthermore, a category C is *Cartesian closed* if it has a terminal object T (i.e. an object such that for every other object X in C, there exists exactly one morphism $X \to T$ taking it to the terminal object), if any two objects X and Y have a product $X \times Y$ in C, and if there exists an exponential Y^Z for any two objects Y and Z.

The archetypical example of a Cartesian closed category is the category Set, whose objects are sets, and whose morphisms are given by functions between sets, with the operation $\circ$ defined as function composition. Then, every singleton set is a terminal object, the product of sets X and Y is just their Cartesian product, and the set Y^Z is the set of all functions from Z to Y (compare the previously introduced powerset 2^{Σ_S}, which we can understand as the set of all functions from Σ_S to the set $2 = \{0, 1\}$).

An important property of the category Set is that it allows the *currying* (Curry, Feys, and Craig 1958) of functions: for every function $f : X \times Y \to Z$, there exists a curried function $g : X \to Z^Y$ such that $f(x, y) = g(x)(y)$. Thus, g maps an $x \in X$ to a function from Y to Z, such that evaluating that function at $y \in Y$ yields the same $z \in Z$ as $f(x, y)$.

Lawvere's deep result then was to make explicit the common structure behind not only Gödel's incompleteness theorems and Turing's proof of the undecidability of the halting problem, but also, Cantor's proof of the uncountability of real numbers (Cantor 1892), Russell's construction of a 'set of all sets that do not contain themselves', which contains itself if and only if it does not contain itself (Russell 1967), Tarski's proof of the impossibility of defining the notion of 'truth' in the system it pertains to (Tarski 1936), and Berry's paradox noting that 'the smallest number not definable in less than eleven words' has just been defined using ten (Russell 1908). For a pedagogical introduction to Lawvere's result with many explicit examples see (Yanofsky 2003).

Our task now is to apply Lawvere's formalism to measurement, and especially to the possibility of predicting measurement outcomes. To do so, we first need to make more precise what we mean by such prediction. As we have formalized it, measurement of a property π corresponds to evaluating the indicator function of the property, i.e. the function

$$m_\pi : \Sigma_S \to \{0, 1\} \tag{5.32}$$

that yields 1 if the system in state s possesses this property, and 0 else. In order to perfectly predict all measurement outcomes, A must be able to decide, for every property π, whether S possesses it in state s. That is, for every s and every π, A must be able to decide whether $m_\pi(s)$ yields 0 or 1.

We can formalize this as follows. First, A must choose which property to predict. In order to do so, there must be a map $\tilde{p} : \Sigma_A \to 2^{\Sigma_S}$, that is, a map that picks out a given property (i.e. an element of 2^{Σ_S}) given a state of A. We can think of A as a Turing machine, which is initialized with a certain program on its tape, where the program is the 'prediction program' for the property π; the state a of A then just determines which program has been chosen.

Then, A must be able to evaluate $\tilde{p}(a)$ on the state s of S. Recall from our discussion above that $\tilde{p}(a) \in 2^{\Sigma_S}$ is a function such that $\tilde{p}(a)(s) = m_\pi(s)$, and that, within the category of sets, there then exists a function $p(a, s) = \tilde{p}(a)(s)$. This is then our prediction map: if there exists a p such that $p(a, s) = m_\pi(s)$, then A can predict every property of S in state s.

Call an m_π such that $p(a, s) = m_\pi(s)$ *representable* by a. Thus, we can equivalently say that A is a perfect predictor for the properties of S if every m_π is representable by some $a \in \Sigma_A$.

Finally, since $|\Sigma_S| = |\Sigma_A| = \mathfrak{c}$ (see the discussion in Sec. 5.2.3), there exists a bijection $r : \Sigma_S \to \Sigma_A$, whose inverse we denote by $\bar{r}$.

We are now ready to establish the main result of this section: for a system S and a universal observer A, there does not exist a prediction map p, such that $p(a, s) = m_\pi(s)$ for all m_π.

The result follows by explicitly constructing an m_π such that $m_\pi(s) \neq p(a, s)$. In order to construct this function (and hence, the corresponding property), we will follow the method of Lawvere (1969), as presented in (Yanofsky 2003). The construction makes use of a further map $\alpha : \{0, 1\} \to \{0, 1\}$, and uses the bijection r to construct a map $\langle \mathbb{1}, r\rangle : \Sigma_S \to \Sigma_S \times \Sigma_A$ such that a state s is taken to a state $(s, a) = (s, r(s)) \in \Sigma_S \times \Sigma_A$.

Then, we define m_α by means of the commutative diagram in Fig. 5.3, i.e. $m_\alpha = \alpha \circ p \circ \langle \mathbb{1}, r\rangle$.

$$\begin{tikzcd}
\Sigma_{\mathcal{S}} \times \Sigma_{\mathcal{A}} \arrow[r, "p"] & \{0,1\} \arrow[d, "\alpha"] \\
\Sigma_{\mathcal{S}} \arrow[u, "\langle Id{,}r\rangle"] \arrow[r, "m_\alpha"] & \{0,1\}
\end{tikzcd}$$

FIGURE 5.3: Commutative diagram used in the proof of the impossibility of perfectly predicting all measurement outcomes.

Now, the claim is that there cannot exist a $p(a, s)$ such that $p(a, s) = m_\alpha(s)$. Evaluated at some given state s, $m_\alpha(s) = \alpha(p(s, r(s))) \in \{0, 1\}$. Assume now for contradiction there exists a p such that $m_\pi(s)$ is representable by some a. Evaluating p at this a yields

$$\begin{aligned}
p(\bar{r}(a), a) &= m_\alpha(\bar{r}(a)) \\
&= \alpha(p(\bar{r}(a), r(\bar{r}(a)))) \\
&= \alpha(p(\bar{r}(a), a)),
\end{aligned} \tag{5.33}$$

where the first step is just the assumption of representability, the second step follows from the definition of m_α, and the final step just uses the properties of the inverse. This establishes $p(\bar{r}(a), a)$ as a fixed point of α, since $\alpha(p(\bar{r}(a), a)) = p(\bar{r}(a), a)$. Consequently, if every m_α is to be predictable by A, then every α must have a fixed point.

This is, however, clearly not the case in general: choose for α the negation function $\neg 1 = 0$, $\neg 0 = 1$, which has no fixed point, and we arrive at the desired contradiction. Consequently, the measurement described by the map

$$m_\neg(\bar{r}(a)) = \neg p(\bar{r}(a), a) \tag{5.34}$$

cannot be equal to $p(s, a)$, and hence, A cannot coherently predict whether S possesses the associated property.

Thus, the above stated criterion of classicality cannot be fulfilled in the setting described here: no matter the knowledge A has about S, there always exist measurements such that A cannot predict their outcome; hence, we have shown that it is always possible to acquire additional information about a given object system. As in the case of the finiteness of the speed of light following from the geometry of Minkowski space, we have thus shown that an epistemic restriction of the kind discussed above follows from considerations on the predictive abilities of universal observers.

A major factor in making this proof work is the existence of the map $\langle \mathbb{1}, r \rangle$, which we can consider to be a concatenation of the bijection r and the *diagonal map* $\Delta : \Sigma_S \to \Sigma_S$ that associates to every state $s \in \Sigma_S$ the tuple $(s, s) \in \Sigma_S \times \Sigma_S$. This map essentially 'copies' the information in s, and can thus physically be considered a cloning device (see the discussion of cloning in Sec. 2.2.1). The existence of this map is closely tied to the special properties of the category Set, in particular, the Cartesian product.

An intriguing point here is that this is an operation that is impossible in quantum mechanics. Moreover, this impossibility (in its generalized form of no-broadcasting) plays a crucial role in the reconstruction of quantum mechanics due to Clifton, Bub, and Halvorson (2003). Its importance for quantum mechanics may stem from the fact that it is closely connected to measurement: cloning is equivalent to perfect state discrimination—if all states of a given set of states are perfectly discriminable, then they can be cloned, since we can just re-prepare the state the discrimination procedure indicated; and if all states in a given set are clonable, they can be discriminated, since we can just prepare sufficiently many states to perform full tomography.

We can elucidate the above proof by for the moment assuming that $|\Sigma_S| = |\Sigma_A| = \aleph_0$, i.e. that both state spaces have the cardinality of the natural numbers. This allows us to find an enumeration of the states of S and A. Now, we can propose a table of values for the function p (see Table 5.2).

TABLE 5.2: Illustration of the fixed-point argument in terms of a diagonalization technique.

	s_1	s_2	s_3	s_4	s_5	$\dots$	s_n	$\dots$
$m_1 \leftarrow a_1$	(1)	0	1	1	1	$\dots$	1	$\dots$
$m_2 \leftarrow a_2$	1	(0)	1	0	0		0	
$m_3 \leftarrow a_3$	0	1	(0)	0	0		1	
$m_4 \leftarrow a_4$	1	0	0	(1)	1		1	
$m_5 \leftarrow a_5$	0	0	0	1	(1)		0	
$\vdots$	$\vdots$					$\ddots$	$\vdots$	
$m_\neg \leftarrow a_n$	0	1	1	0	0	$\dots$	($\lightning$)	$\dots$
$\vdots$	$\vdots$						$\vdots$	$\ddots$

Each row of this table yields the values of a measurement m_π, if the state of S is s_j. In state a_1, A predicts the values of m_1 given the state of S, i.e. $p(a_1, s_j) = m_1(s_j)$, while in state a_2, A predicts the values of m_2, and so on. Consequently, the existence of this table is equivalent to the assumption that each m_π is representable by some a_i.

Now, the measurement impossible to predict is constructed by assigning to each s_j the negation of the value along the main diagonal—thus, $m_\neg(s_1) = 0$, $m_\neg(s_2) = 1$, and so on. Of course, any assignment of values to states s_j yields a valid property—we merely consider the property equivalent to the subset of Σ_S that does not contain s_1, contains s_2, and so forth.

If A now is able to predict the outcome of $m_\neg$, then there must be some state a_n such that $p(a_n, s_j) = m_\neg(s_j)$. However, this state clearly cannot be a_1, since $m_\neg$ differs from m_1 in the value assigned to s_1; it cannot be a_2, since $m_\neg$ differs from m_2 in the value assigned to s_2. Generally, for each n, $m_n(s_n) \neq m_\neg(s_n)$; hence, there can be no state in which A correctly predicts the outcomes of $m_\neg$ for all s_j.

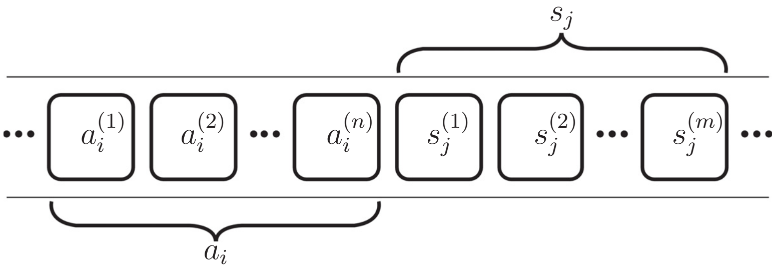


FIGURE 5.4: Schematic representation of A's prediction task: A's tape is initialized with n symbols $(a_i^{(1)}, \ldots, a_i^{(n)})$ encoding the program for predicting the ith property (that is, it is in state a_i), concatenated with m symbols $(s_j^{(1)}, \ldots, s_j^{(m)})$ encoding S's state s_j. By successively reading these symbols and carrying out the appropriate operations, it then computes the value of $p(s_j, a_i)$.

We can also look at this in the way shown in Fig. 5.4. A is considered to be a Turing machine implementing the function $p(a, s)$. On its tape, it receives an n-symbol description of a program a_i for predicting the ith property, as well as an m-symbol description of the state s_j of the system. The output then is given by the entry at position (j, i) of Table 5.2. The entries with value 1 along the main diagonal then yield the set of all states s_i such that A predicts that S in state s_i has property π_i. The set of all of those s_i is a subset of Σ_S, i.e. a property, which we will call π_Δ. Then, the complement of this set is another property $\pi_\neg = \pi_\Delta^\perp$.

If this is now the nth property, A is faced with having to make a contradictory prediction: if A predicts that s_n has the nth property, then s_n is a member of the set π_Δ; but the nth property is precisely the complement of that set, and hence A ought to predict that s_n does not have that property. Likewise, if A predicts that s_n does not have the nth property, then s_n is a member of the set $\pi_\Delta^\perp$, and consequently, possesses the nth property.

Consequently, there does not exist a Turing machine such that it can predict the values of all measurements, and if we again assume the Church-Turing thesis, there are properties such that no computable process ever accurately predicts whether a system possesses them. Note that on this formulation, we need not impose any restrictions on the cardinality of the state spaces: for whatever cardinality that may be, a Turing machine only accepts finite-length programs with finite-length inputs. Thus, if this is an accurate representation of how real-world prediction of measurement outcomes occurs, then no prediction of every possible measurement outcome is possible in general.

Nevertheless, the empirical relevance of this result might still be questioned: after all, real-world measurements always have finite accuracy;

hence, there always exists room for further improvement, and consequently, for gaining additional information about a system. Furthermore, as detailed above, A just fails to be able to consistently predict the measurement outcome of one particular measurment, if the system is in one particular state. Consequently, it might be unlikely that this possibility ever has any empirically observable consequences.

Regarding the first objection, however, we note that while this is the case with continuous state spaces, the elements of a state space whose cardinality is that of the natural numbers can be respresented exactly using a finite amount of information; nevertheless, even in this case, the result above shows that we cannot predict the outcome of all possible measurements.

The last objection can be countered by noting that we can, in fact, use the above method to construct many more (indeed, infinitely many) inconsistent properties. For instance, we need not limit ourselves to choosing the values to flip along the main diagonal; we can equally well choose the value a_i assigns to s_{i+1}, if i is even, and to s_{i-1} if it is odd (with the exception of $i = 1$, where we have to take s_1). Or, indeed, we could flip a value at some randomly chosen index j in each row, just taking care not to repeat this choice.

Consequently, there exist infinitely many measurements such that a given apparatus A cannot predict their outcome for every state s of the object system S. In fact, since the cardinality of the set of properties is that of the powerset of Σ_S, almost all (in the sense of 'all but a measure-zero subset') properties are unpredictable. But this does not imply a limit on the information to be gained about a system: for any ϵ, in a continuous state space, if we localize a system beyond the accuracy given by ϵ, we still have only gained a finite amount of information about the system, and consequently, there is still an infinite amount of information unknown to us.

Hence, we now turn to the first assumption, namely, the assumption that we can only acquire a finite amount of information for each system.

5.2.5 Making Undecidability Quantifiable: Berry's Paradox

The proof in the previous section, much like the work of Turing, Gödel, and others, establishes the *existence* of 'unsolvable questions' of a certain kind, essentially by exhibiting an example. However, it does nothing to quantify their *prevalence*. To illustrate this, consider localizing a system within its state space by a series of nested intervals. Assume for the moment that the state space is continuous, but bounded; certainly, this is effectively the case for any real physical system, with e.g. its position limited by the size of the laboratory. We can then simply map the k-dimensional state space to the k-dimensional unit hypercube $[0, 1]^{\times k}$. Such a mapping also exists if we assume an unbounded state space, and restrict ourselves to the *open* unit hypercube $(0, 1)^{\times k}$; for instance, in the one dimensional case, every $x \in \mathbb{R}$ is mapped to $y \in (0, 1)$ by

$$f(x) = \frac{1}{1 + e^{-x}}. \tag{5.35}$$

However, for every such mapping, the density of states will be highly non-uniform—in fact, for any interval $(0, a)$ with $a < 1$, almost all states will lie outside the interval. Hence, we restrict ourselves to bounded state spaces, with however arbitrary bounds.

Then, we can just ask whether s is in $(0, \frac{1}{2})$, yielding one bit of information regarding the state of S (in the case of a k-dimensional state space, we need to repeat the question for every dimension, thus yielding k bits of information). Afterwards, we again split the remaining space in half, and so on, narrowing down the state of S with ever increasing accuracy: n bits of information suffice to localize the system within a state space volume of size 2^{-n} (or, for k-dimensional state spaces, kn bits localize the system within a volume of 2^{-kn}).

However, at any given point in this procedure, there are still infinitely many questions left open, so to speak. The assumption of finite information then boils down to postulating that there is an end-point to the iteration: after having accumulated a maximum of information, say n_0 bits, the state of the system cannot be further constrained. This could occur in two ways: first, there might be no more information available—i.e. the state space is partitioned into cells of a given minimum volume, and once a state is located within that volume, we simply know all there is to know.

This possibility, however, is in conflict with the principle of additional information: as demonstrated above, it is always possible to acquire new information about a system. Hence, whenever we acquire new information, some information we already have must become obsolete, in order to not exceed the maximum. Within the toy theory, this occurs via a randomization of the ontic state consistent with the information acquired upon the most recent measurement; in quantum mechanics, we require the state to indeterministically transition to an eigenstate of a given measurement operator.

As we did with the postulate of additional information in the previous section, we now venture to likewise give a reason behind the postulate of finite information. This will be achieved as follows. The proof in the previous section relied on finding a single inconsistent assignment of values, by constructing a 'self-negating' property $\pi_\neg$. In analogy, Gödel's result can be said to rely on a suitable formalization of the liar-paradox, which likewise yields a single statement that cannot be consistently assigned a truth value. In order to extend these results, then, we will instead find a formulation such that we can find a class of 'paradoxical' statements whose extent, moreover, can be precisely quantified, and show that there exists a limit such that every question further constraining the state space localization of S falls within this class.

This construction takes its leave from the Berry paradox. As noted above, the paradox in this case is that

"the smallest number not definable in less than eleven words"

uniquely names a number if and only if that number is, in fact, not definable in less than eleven words; but in this case, the above statement is a definition of this number, consisting of merely ten words.

Berry's paradox, in a suitably formalized manner, can be used to formulate an incompleteness theorem due to Chaitin (1974) asserting that all statements beyond a given limit are undecidable within a given formal system. Since the theorem is less familiar than the Gödelian version, we will present a short outline of its proof.

First of all, we will formalize what it means to 'define' a number. Fix a universal Turing machine U, again taking programs from a prefix-free set (in the following, we will always assume programs to come from a prefix-free set). Then, a number (or string) σ is defined by a program x such that $U(x) = \sigma$. As defined in Sec. 5.2.2, the length of the shortest x such that x defines σ then is the Kolmogorov complexity of σ, denoted $K(\sigma)$.

Additionally, assume F is an axiom system of sufficient strength to formalize assertions about the Kolmogorov complexity of strings, such that F is *sound*—that is, such that every statement about complexity it proves is, in fact, true (this is a stronger requirement than necessary for establishing Gödel's incompleteness theorem, where one merely needs to require that the system is consistent, i.e. proves no contradictions).

For this system F, it can then be shown that there exists a constant n_0 such that all assertions of the form

$$K(\sigma) \geq n_0 \tag{5.36}$$

are unprovable in F. However, since there are infinitely many strings with complexity above any given threshold, this translates to infinitely many undecidable statements.

To prove this, imagine a program, p, such that p enumerates all proofs within F, and halts whenever it finds a proof that the Kolmogorov complexity of some integer z is exactly n, outputting z. This program itself has a certain Kolmogorov complexity, given by a constant c_p, specifying the program itself, plus a contribution of size $\log_2(n)$ encoding the number n. However, since p is a program that outputs z, it is itself a definition of z, of complexity $K(z) = c_p + \log_2(n)$. Yet, p outputs z if and only if the complexity of z is equal to n; but there exists some n_0 for which $n_0 > c_p + \log_2(n_0)$, and thus, while proving that z has no description shorter than n_0 bits, p is itself a description of z shorter than n_0 bits. Consequently, no such proof can be present among the proofs of F.

We now need to translate this result to our setting. First of all, consider the state s of S as given by the values assigned to a (countably infinite) set of properties π_i (cf. Eq. 5.31),

$$s = (\pi_1^{(v)}, \pi_2^{(v)}, \pi_3^{(v)}, \ldots). \tag{5.37}$$

As briefly discussed above, such a sequence suffices to 'localize' the state of S arbitrarily well within its state space. This is due to the fact that the set of all extensions of a n-bit sequence—i.e. the set of all sequences that have this sequence as their n-bit prefix—forms a set of (uniform) measure 2^{-n}, and thus, with n increasing, any desired localization can be achieved.

If we now assume that each physical system can, in principle, have each of these properties, then the above sequence is almost surely random, in the sense that the non-random infinite sequences (bit strings) form a set of measure zero (see, e.g., (Li and Vitányi 1993, p. 122)); consequently, a generic state s of a system S leads to a sequence as in Eq. 5.37 that is random with probability one.

Now, the question arises: how many bits of the sequence in Eq. 5.37 can A obtain? If the answer turns out to be infinite, then A can localize the state of S to arbitrary accuracy within its state space.

However, supposing that A can obtain knowledge of infinitely many bits of s is in fact inconsistent with the randomness of the sequence. Here, by randomness, we mean algorithmic randomness (see Eq. 5.22).

Now assume, for contradiction, that A can obtain infinitely many bits of s (the following proof closely parallels the one given by Chaitin (1992)). Furthermore, assume that there exists a program p_A modeling the process by which A obtains bits of s. Then, there exists a special-purpose computer C and a program p given by the string

$$p = \underbrace{00\ldots01}_{l\text{ bits}} p_A x, \tag{5.38}$$

such that in executing this program, C does the following: first, it reads the l initial bits, which essentially just tells it the number l. Then, it executes the program p_A, generating bits of the sequence s (in no particular order); in doing so, it keeps count of the number of bits r it has read of p_A. It stops executing p_A as soon as it has found the values and positions of $r + 2l$ bits of the sequence in Eq. 5.37 (note that knowledge of the position of a given bit of this sequence is equal to knowledge of which property it is that takes the proven value). Consequently, C executes only the program p' given by

$$p' = \underbrace{00\ldots01}_{l\text{ bits}} p'_A x, \tag{5.39}$$

where p'_A is given by the first r bits of p_A.

Thus, after having executed this program, C knows the values and positions of $r + 2l$ bits of the representation of s as given in Eq. 5.37. Then, C determines the value of that bit of the sequence that is the furthest to the right, i.e. the last bit whose value it has proven. Say this bit is at position n. Consequently, C knows the values (and positions) of $r + 2l$ bits (including the final one) of the initial segment

$$s_n = (\pi_1^{(v)}, \pi_2^{(v)}, \pi_3^{(v)}, \ldots, \pi_n^{(v)}). \tag{5.40}$$

Now, there are $n-r-2l$ bits in this sequence C does not know. These bits are given to it in the string x of the program p'. As a result, C then knows the first n bits of s, outputs them, and halts. Its action on the program p' is thus

$$C(\underbrace{00\ldots01}_{l\text{ bits}} p_A x) = s_n. \tag{5.41}$$

The length of p' is given by

$$|p'| = l + r + n - r - 2l = n - l. \tag{5.42}$$

Consequently, we can give an upper bound on the Kolmogorov complexity of s_n given by

$$K(s_n) \leq n - l + c', \tag{5.43}$$

where c' is a constant equal to the length of the shortest program simulating C on some universal Turing machine. Due to the randomness of s, we thus have

$$n - c < K(s_n) \leq n - l + c', \tag{5.44}$$

which implies that $l < c + c'$. Consequently, if we now take $l = c + c'$, we obtain again a contradiction of the Berry type: $K(s_n)$, if A could obtain the values of $r + 2l$ bits of s, must be smaller than $n - c$; but we know that this bound must hold by the randomness of s. Hence, A cannot obtain all of these values, and thus, can only approximate it to a finite degree of precision. In other words, we have proven that the maximal information obtainable about the state of S by a universal observer A is finite.

As it stands, this proof has an obvious lacuna: we have assumed that the process by which A obtains the values of elements of s—that is, by which it decides whether S has a given property π_i in state s—is equivalent to some program p_A. This is equivalent to assuming the *physical* Church-Turing thesis (or sometimes *Church-Turing-Deutsch thesis* (Deutsch 1985), which states that all physically computable functions are Turing-computable (Piccinini 2007). If this thesis does not hold, then the proof above fails: there might not exist a (Turing-computable) program p_A; consequently, the process by which A decides whether a given system has some property would be non-computable, and the conjunction of the systems A and S would constitute a device capable of computing a non-Turing computable function—a so-called *hypercomputer* (Copeland 2002; Copeland and Proudfoot 1999).

This is a substantive, and controversial, thesis about physical reality. Attitudes towards it range from the assumption that the universe, in some sense, is itself nothing but a giant computer (a notion which takes its origin with Zuse's *Rechnender Raum* (*calculating space*) (Zuse 1969)), to the idea that the process behind quantum state reduction allows the harnessing of hypercomputational resources (Hameroff and Penrose 2014). We will not propose to enter this discussion here, but merely note that the thesis is, in principle, experimentally refutable—although what exact form such a refutation would take is itself subject to discussion (Leitsch, Schachner, and Svozil 2008). Consequently, we adopt it as an empirical principle on par with the finiteness of the speed of light, or the geometry of Minkowski space.

It is interesting to note here that Masanes, Müller, et al. (2013) point out that their assumption that a suitable set of gbits suffices to reversibly encode any unknown state of an arbitrary system essentially amounts to assuming the Church-Turing-Deutsch thesis.

Combining the results of this and the previous section, we have thus shown a possible point of origin for both the postulate of finite information and the possibility of always being able to obtain additional information, in the same sense that the geometry of Minkowski space is the point of origin for the finiteness of the speed of light. According to these results, the possibility of obtaining additional information originates from the impossibility of predicting all possible measurement outcomes, as established via Lawvere's fixed-point theorem; while the impossibility of obtaining infinite information about a system then follows from a contradiction of the Berry type that arises in assuming that an observer could predict infinitely many of the properties of an object system, combined with the assumption that there exist no physical resources capable of hypercomputation.

Chapter 6

Conclusions and Outlook

In this thesis, we have engaged with the topic of quantum correlations from three different vantage points: regarding the methods of their detection, their possible applications to tasks not classically feasible, and finally, their foundations.

We first considered a generalization of the Kochen-Specker theorem aimed at making its predictions testable in real-world experiments. A necessary assumption in the Kochen-Specker theorem is the compatibility of measurements that are performed jointly; however, due to unavoidable experimental noise, this compatibility is in general not given in experiments: this is the problem of compatibility.

We demonstrated, using a simple class of Markov models, that in the case of imperfect compatibility, spurious violations of inequalities derived to enable the experimental testability of the Kochen-Specker theorem may occur. To remedy this, we proposed a new nondisturbance assumption, noncontextual evolution, that essentially posits that a system traverses a sequence of hidden-variable states independently of the measurements that are performed on it. This allowed us to derive modifications of existing Kochen-Specker inequalities, such that the performed measurements obey a time-ordering. We showed that, in contrast to the usual Kochen-Specker inequalities, these inequalities cannot be violated by a Markov model, and consequently, allow for experimental testing even if the observables fail to be compatible.

Since the nondisturbance assumption we posit reduces to Kochen-Specker noncontextuality in the limit of perfect compatibility, these modified inequalities may thus be regarded as enabling the real-world experimental implementation of tests against a more general set of hidden-variable theories.

Furthermore, we considered the possibility of detecting the entanglement content of completely unknown quantum states. Many tests for entanglement, such as e.g. entanglement witnesses, have to be tailored towards a specific state whose entanglement one wants to detect, such that they may fail to detect the entanglement in case a different, yet entangled, state is prepared by the source. On the other hand, tests of unknown quantum states, such as for instance quantum state tomography, become prohibitively resource-intensive for even comparatively small systems.

We proposed a construction of witness operators from random local measurements, such that a semidefinite program is used to determine if entanglement has been detected. This enables a protocol that is guaranteed to eventually detect the entanglement of any given state: we may simply continue to add local measurements, until the semidefinite program concludes a detection.

We demonstrated that this procedure scales much more favorably with system size than quantum tomography. Additionally, we discussed the effect of performing additional measurements on the statistics—and thus, the number of repetitions of individual measurements—needed to conclude a detection within a given level of confidence.

Turning then to the possible applications of quantum correlations, we proposed a new task having no classical solution that can nevertheless be performed using quantum resources: the certification of lower bounds on detector efficiency. While classically, it is always possible to introduce, e.g., source rate variations or false clicks in order to 'fake' a given detection efficiency if one does not have access to the devices' inner workings, in quantum mechanics, it turns out that the violation of Bell inequalities can be leveraged to produce a bound on the minimum efficiency a detector must exceed.

In order to achieve this, we proposed a method of generating Bell inequalities using only the observed measurement data. This is possible due to the fact that the classically achievable correlations from a convex polytope defined by finitely many vertices. Since these vertices are uniquely determined by the given experimental setting (i.e. the number n of observables on Alice's, and the number m of observables on Bob's side), it becomes possible to check, via a linear program, whether the observed measurement statistics lie within the polytope. If they do not, then there exists a Bell inequality violated by these statistics, and moreover, this Bell inequality can be explicitly constructed such that it is maximally violated. Additionally, the construction is such that the Bell inequalities found in this way are inherently free from the fair sampling loophole, that is, their violation is not due to possible sampling effects induced by data rejection.

This method already has several interesting potential applications: for one, it can be considered a natural further development of the witness construction presented previously, where now we not only leave the quantum state, but also the performed measurements unknown. This is due to the fact that every Bell inequality can be considered an entanglement witness, since entanglement is a necessary condition to achieve Bell inequality violation. Furthermore, our construction represents a method to generate Bell inequality violations even in the absence of a shared reference frame between distant laboratories; indeed, we may leave our detectors fully uncharacterized. Finally, since the secret key rate in certain device-independent quantum key distribution schemes depends on the degree of violation of a Bell inequality, our method allows to find a protocol where no Bell inequality needs to be agreed upon a priori by the parties, but where the Bell inequality leading to the highest key rate can simply be determined from the observed measurement statistics.

However, our main focus was the certification of lower bounds on detector efficiencies. For any given Bell inequality, a minimum detection efficiency can be calculated such that no violation can be observed using detectors not meeting this minimum requirement. In general, this calculation necessitates optimization over the full set of quantum correlations, which is difficult to characterize; however, using the Navascués-Pironio-Acín hierarchy, we are able to derive a sequence of increasing lower bounds to this efficiency. Taking into account the magnitude of the quantum value then allows to compute even better lower bounds.

The last topic of this thesis then was to discuss a program to propose foundational principles on which quantum theory rests, in analogy to special relativity, whose empirical content derives from the principle of relativity combined with the constancy of the speed of light across all frames of reference. Several reconstructions of quantum mechanics share an appeal to certain epistemic restrictions as their common basis. Such restrictions essentially put a bound on the information accessible about a given system, while nevertheless stipulating that new information can always be gained via measurement.

Just as the geometry of Minkowski space underlies the principles of special relativity, we proposed to look towards logical restrictions imposed upon (universal) observers by the phenomena of paradoxical self-reference. We could show, using a diagonalization argument, that no observer can predict the outcome of every measurement—essentially, because it is possible to construct a paradoxical property such that any prediction is self-falsifying: if the observer predicts that the object system possesses the property, then it does not, and vice versa. This bears a strong analogy to the undecidability of the halting problem, which can be proved by constructing a program that halts exactly if it predicts that it fails to halt, and vice versa. Thus, this shows that new information can always be obtained about a physical system.

Furthermore, under the assumption of the physical Church-Turing thesis, it is possible to show that only finitely many of the properties of a given physical system can be simultaneously observed: for if it were the case that there exists a computable procedure that produces the values of all properties, then one could produce a program such that it yields n bits encoding whether the system has or fails to have n given properties, with the length of this program being smaller than the bound imposed by the algorithmic randomness of this sequence. Thus, there exists a finite (albeit noncomputable) bound on the total information obtainable about a given system, in other words, an epistemic restriction.

It is interesting to observe here that the proofs mentioned above depend critically on the properties of the category Set, most notably, the possibility to arbitrarily copy information. This is a feature inherent in our conception of the world: without it, communication in the everyday sense becomes impossible. After all, communication has only taken place if afterwards both the provider and the recipient are in possession of the same information—i.e. if each possesses a copy of the same information. Thus, all the information we can share (such as this thesis) is of necessity classical information: the quantum world is removed from our everyday experience not through size, but rather, through communicability.

Bibliography

Aerts, Sven (2005). “Undecidable classical properties of observers”. In: *International Journal of Theoretical Physics* 44.12, pp. 2113–2125.

Aliprantis, Charalambos D and Kim Border (2006). *Infinite dimensional analysis: a hitchhiker’s guide*. Springer Science & Business Media.

Ardehali, Mohammad (1992). “Bell inequalities with a magnitude of violation that grows exponentially with the number of particles”. In: *Physical Review A* 46.9, p. 5375.

Aspect, Alain, Jean Dalibard, and Gérard Roger (1982). “Experimental test of Bell’s inequalities using time-varying analyzers”. In: *Physical Review Letters* 49.25, p. 1804.

Aspect, Alain, Philippe Grangier, and Gérard Roger (1981). “Experimental tests of realistic local theories via Bell’s theorem”. In: *Physical Review Letters* 47.7, p. 460.

— (1982). “Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: a new violation of Bell’s inequalities”. In: *Physical Review Letters* 49.2, p. 91.

Barrett, Jonathan (2007). “Information processing in generalized probabilistic theories”. In: *Physical Review A* 75.3, p. 032304.

Barrow, John D (1999). *Impossibility: The limits of science and the science of limits*. Oxford: Oxford University Press.

Baumeler, Ämin and Stefan Wolf (2016). “Device-independent test of causal order and relations to fixed-points”. In: *New Journal of Physics* 18.3, p. 035014.

Bayen, François et al. (1978a). “Deformation theory and quantization. I. Deformations of symplectic structures”. In: *Annals of Physics* 111.1, pp. 61–110.

— (1978b). “Deformation theory and quantization. II. Physical applications”. In: *Annals of Physics* 111.1, pp. 111–151.

Belinsky, Alexander and David Nikolaevich Klyshko (1993). “Interference of light and Bell’s theorem”. In: *Physics-Uspekhi* 36.8, pp. 653–693.

Bell, John Stewart (1964). “On the Einstein Podolsky Rosen paradox”. In: *Physics* 1.3, pp. 195–200.

— (1966). “On the problem of hidden variables in quantum mechanics”. In: *Reviews of Modern Physics* 38.3, p. 447.

Bennett, Charles H (1984). “Quantum cryptography: Public key distribution and coin tossing”. In: *International Conference on Computer System and Signal Processing, IEEE, 1984*, pp. 175–179.

Bennett, Charles H, Gilles Brassard, et al. (1993). “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels”. In: *Physical Review Letters* 70.13, p. 1895.

Bennett, Charles H and Stephen J Wiesner (1992). “Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states”. In: *Physical Review Letters* 69.20, p. 2881.

Berger, Robert (1966). *The undecidability of the domino problem*. Memoirs of the American Mathematical Society 66. Providence (RI): American Mathematical Society.

Birkhoff, Garrett and John von Neumann (1936). “The logic of quantum mechanics”. In: *Annals of mathematics*, pp. 823–843.

Bohm, David and Yakir Aharonov (1957). “Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky”. In: *Physical Review* 108.4, p. 1070.

Bohr, Niels (1935). “Can quantum-mechanical description of physical reality be considered complete?” In: *Physical Review* 48.8, p. 696.

Boole, George (1862). “On the theory of probabilities”. In: *Philosophical Transactions of the Royal Society of London* 152, pp. 225–252.

Bourennane, Mohamed et al. (2004). “Experimental detection of multipartite entanglement using witness operators”. In: *Physical Review Letters* 92.8, p. 087902.

Boyd, Stephen and Lieven Vandenberghe (2004). *Convex optimization*. Cambridge: Cambridge university press.

Breuer, Thomas (1995). “The impossibility of accurate state self-measurements”. In: *Philosophy of Science*, pp. 197–214.

Brukner, Časlav (2009). “Quantum complementarity and logical indeterminacy”. In: *Natural Computing* 8.3, pp. 449–453.

Brukner, Časlav and Anton Zeilinger (2003). “Information and fundamental elements of the structure of quantum theory”. In: *Time, quantum and information*. Berlin: Springer, pp. 323–354.

Brukner, Časlav, Marek Żukowski, et al. (2004). “Bell's inequalities and quantum communication complexity”. In: *Physical Review Letters* 92.12, p. 127901.

Buckley, Paul and F David Peat (1996). *Glimpsing reality: Ideas in physics and the link to biology*. Toronto: University of Toronto Press.

Cabello, Adán (2008). “Experimentally testable state-independent quantum contextuality”. In: *Physical Review Letters* 101.21, p. 210401.

Calude, Cristian S, Peter H Hertling, et al. (1998). “Recursively enumerable reals and Chaitin Ω numbers”. In: *Annual Symposium on Theoretical Aspects of Computer Science*. Springer, pp. 596–606.

Calude, Cristian S and Michael A Stay (2007). “From Heisenberg to Gödel via Chaitin”. In: *International Journal of Theoretical Physics* 46.8, pp. 2013–2025.

Cantor, Georg (1892). “Über eine elementare Frage der Mannigfaltigkeitslehre”. In: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 1, pp. 75–78.

Cavallar, Stefania et al. (2000). “Factorization of a 512-bit RSA modulus”. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, pp. 1–18.

Cereceda, Jose L (2000). “Local hidden-variable models and negative-probability measures”. In: *arXiv preprint quant-ph/0010091*.

Chaitin, Gregory J (1974). “Information-theoretic limitations of formal systems”. In: *Journal of the ACM (JACM)* 21.3, pp. 403–424.

— (1975). “A theory of program size formally identical to information theory”. In: *Journal of the ACM (JACM)* 22.3, pp. 329–340.

— (1992). “Information-theoretic incompleteness”. In: *Applied Mathematics and Computation* 52.1, pp. 83–101.

Chaitin, Gregory J, Asat Arslanov, and Cristian S Calude (1995). “Program-size complexity computes the halting problem”. In: *Bulletin of the EATCS* 57, p. 198.

Cirel’son, Boris S (1980). “Quantum generalizations of Bell’s inequality”. In: *Letters in Mathematical Physics* 4.2, pp. 93–100.

Clauser, John F and Michael A Horne (1974). “Experimental consequences of objective local theories”. In: *Physical Review D* 10.2, p. 526.

Clauser, John F, Michael A Horne, et al. (1969). “Proposed experiment to test local hidden-variable theories”. In: *Physical Review Letters* 23.15, p. 880.

Clifton, Rob, Jeffrey Bub, and Hans Halvorson (2003). “Characterizing quantum theory in terms of information-theoretic constraints”. In: *Foundations of Physics* 33.11, pp. 1561–1591.

Copeland, B Jack (2002). “Hypercomputation”. In: *Minds and machines* 12.4, pp. 461–502.

Copeland, B Jack and Diane Proudfoot (1999). “Alan Turing’s forgotten ideas in computer science”. In: *Scientific American* 280.4, pp. 98–103.

Cubitt, Toby S, David Perez-Garcia, and Michael M Wolf (2015). “Undecidability of the spectral gap”. In: *Nature* 528.7581, pp. 207–211.

Curry, Haskell Brooks, Robert Feys, and William Craig (1958). *Combinatory logic, vol. 1*. Amsterdam: North-Holland Publishers.

Curtright, Thomas L and Cosmas K Zachos (2012). “Quantum mechanics in phase space”. In: *Asia Pacific Physics Newsletter* 1.01, pp. 37–46.

Curty, Marcos and Tobias Moroder (2011). “Heralded-qubit amplifiers for practical device-independent quantum key distribution”. In: *Physical Review A* 84.1, p. 010304.

Dalla Chiara, Maria Luisa (1977). “Logical self reference, set theoretical paradoxes and the measurement problem in quantum mechanics”. In: *Journal of Philosophical Logic* 6.1, pp. 331–347.

Deutsch, David (1985). “Quantum theory, the Church-Turing principle and the universal quantum computer”. In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. Vol. 400. 1818. The Royal Society, pp. 97–117.

Dieks, DGBJ (1982). “Communication by EPR devices”. In: *Physics Letters A* 92.6, pp. 271–272.

Doherty, Andrew C, Pablo A Parrilo, and Federico M Spedalieri (2002). “Distinguishing separable and entangled states”. In: *Physical Review Letters* 88.18, p. 187904.

Eberhard, Philippe H (1993). “Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment”. In: *Physical Review A* 47.2, R747.

Einstein, Albert (1905). “Zur Elektrodynamik bewegter Körper”. In: *Annalen der Physik* 322.10, pp. 891–921.

Einstein, Albert, Boris Podolsky, and Nathan Rosen (1935). “Can quantum-mechanical description of physical reality be considered complete?” In: *Physical Review* 47.10, p. 777.

Eisert, Jens, Markus P Müller, and Christian Gogolin (2012). “Quantum measurement occurrence is undecidable”. In: *Physical Review Letters* 108.26, p. 260501.

Ekert, Artur K (1991). “Quantum cryptography based on Bell’s theorem”. In: *Physical Review Letters* 67.6, p. 661.

Eldar, Yonina C (2003). “A semidefinite programming approach to optimal unambiguous discrimination of quantum states”. In: *IEEE Transactions on information theory* 49.2, pp. 446–456.

Freedman, Stuart J and John F Clauser (1972). “Experimental test of local hidden-variable theories”. In: *Physical Review Letters* 28.14, p. 938.

Fritz, Tobias (2010). “Quantum correlations in the temporal Clauser–Horne–Shimony–Holt (CHSH) scenario”. In: *New Journal of Physics* 12.8, p. 083055.

Fuchs, Christopher A (2002). “Quantum mechanics as quantum information (and only a little more)”. In: *arXiv preprint quant-ph/0205039*.

Garg, Anupam and N David Mermin (1987). “Detector inefficiencies in the Einstein-Podolsky-Rosen experiment”. In: *Physical Review D* 35.12, p. 3831.

Gauger, Erik M et al. (2011). “Sustained quantum coherence and entanglement in the avian compass”. In: *Physical Review Letters* 106.4, p. 040503.

Gerstenhaber, Murray (1964). “On the deformation of rings and algebras”. In: *Annals of Mathematics*, pp. 59–103.

Gill, Richard D (2015). “Pearle’s Hidden-Variable Model Revisited”. In: *arXiv preprint arXiv:1505.04431*.

Giovannetti, Vittorio, Seth Lloyd, and Lorenzo Maccone (2006). “Quantum metrology”. In: *Physical Review Letters* 96.1, p. 010401.

Gisin, Nicolas and Bernard Gisin (1999). “A local hidden variable model of quantum correlation exploiting the detection loophole”. In: *Physics Letters A* 260.5, pp. 323–327.

Gisin, Nicolas, Stefano Pironio, and Nicolas Sangouard (2010). “Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier”. In: *Physical Review Letters* 105.7, p. 070501.

Giustina, Marissa et al. (2015). “Significant-loophole-free test of Bell’s theorem with entangled photons”. In: *Physical Review Letters* 115.25, p. 250401.

Gödel, Kurt (1931). “Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I”. In: *Monatshefte für Mathematik und Physik* 38.1, pp. 173–198.

Goh, Koon Tong, Jean-Daniel Bancal, and Valerio Scarani (2016). “Measurement-device-independent quantification of entanglement for given Hilbert space dimension”. In: *New Journal of Physics* 18.4, p. 045022.

Grinbaum, Alexei (2003). “Elements of information-theoretic derivation of the formalism of quantum theory”. In: *International Journal of Quantum Information* 1.03, pp. 289–300.

— (2005). “Information-Theoretic Princple Entails Orthomodularity of a Lattice”. In: *Foundations of Physics Letters* 18.6, pp. 563–572.

Groenewold, Hilbrand Johannes (1946). “On the principles of elementary quantum mechanics”. In: *Physica* 12.7, pp. 405–460.

Gühne, Otfried et al. (2010). “Compatibility and noncontextuality for sequential measurements”. In: *Physical Review A* 81.2, p. 022121.

Haar, Alfred (1933). “Der Massbegriff in der Theorie der kontinuierlichen Gruppen”. In: *Annals of Mathematics*, pp. 147–169.

Hameroff, Stuart and Roger Penrose (2014). “Consciousness in the universe: A review of the ‘Orch OR’ theory”. In: *Physics of Life Reviews* 11.1, pp. 39–78.

Hardy, Lucien and William K Wootters (2012). “Limited holism and real-vector-space quantum theory”. In: *Foundations of Physics* 42.3, pp. 454–473.

Hensen, Bas et al. (2015). “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres”. In: *Nature* 526.7575, pp. 682–686.

Herbert, Nick (1982). “FLASH–a superluminal communicator based upon a new kind of quantum measurement”. In: *Foundations of Physics* 12.12, pp. 1171–1179.

Hirshfeld, Allen C and Peter Henselder (2002). “Deformation quantization in the teaching of quantum mechanics”. In: *American Journal of Physics* 70.5, pp. 537–547.

Hirzebruch, Friedrich and Winfried Scharlau (1971). “Einführung in die Funktionalanalysis”. In: *Bibliographisches Institut Mannheim, Wien, Zurich*.

Horodecki, Michał, Paweł Horodecki, and Ryszard Horodecki (1996). “Separability of mixed states: necessary and sufficient conditions”. In: *Physics Letters A* 223.1, pp. 1–8.

Janotta, Peter, Christian Gogolin, et al. (2011). “Limits on nonlocal correlations from the structure of the local state space”. In: *New Journal of Physics* 13.6, p. 063024.

Janotta, Peter and Haye Hinrichsen (2014). “Generalized probability theories: What determines the structure of quantum theory?” In: *Journal of Physics A: Mathematical and Theoretical* 47.32, p. 323001.

Johnston, Nathaniel (2016). *QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9*. `http://qetlab.com`. DOI: `10.5281/zenodo.44637`.

Jozsa, Richard and Noah Linden (2003). “On the role of entanglement in quantum-computational speed-up”. In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. Vol. 459. 2036. The Royal Society, pp. 2011–2032.

Jungnitsch, Bastian, Tobias Moroder, and Otfried Gühne (2011). “Taming multiparticle entanglement”. In: *Physical Review Letters* 106.19, p. 190502.

Kampermann, Hermann et al. (2012). “Algorithm for characterizing stochastic local operations and classical communication classes of multiparticle entanglement”. In: *Physical Review A* 86.3, p. 032307.

Karush, William (1939). “Minima of functions of several variables with inequalities as side constraints”. MA thesis. Chicago: Dept. of Mathematics, University of Chicago.

Kleene, Stephen Cole (1943). “Recursive predicates and quantifiers”. In: *Transactions of the American Mathematical Society* 53.1, pp. 41–73.

Kleinjung, Thorsten et al. (2010). “Factorization of a 768-bit RSA modulus”. In: *Annual Cryptology Conference*. Springer, pp. 333–350.

Kleinmann, Matthias et al. (2012). “Optimal inequalities for state-independent contextuality”. In: *Physical Review Letters* 109.25, p. 250402.

Klyachko, Alexander A et al. (2008). “Simple test for hidden variables in spin-1 systems”. In: *Physical Review Letters* 101.2, p. 020403.

Kochen, Simon and Ernst P Specker (1969). “The problem of hidden variables in quantum mechanics”. In: *Journal of Mathematics and Mechanics* 17, pp. 59–87.

Kolmogorov, Andrei N (1963). "On tables of random numbers". In: *Sankhyā: The Indian Journal of Statistics, Series A*, pp. 369–376.

Komar, Peter et al. (2014). "A quantum network of clocks". In: *Nature Physics* 10.8, pp. 582–587.

Koopman, Bernard O (1931). "Hamiltonian systems and transformation in Hilbert space". In: *Proceedings of the National Academy of Sciences* 17.5, pp. 315–318.

Kraft, Leon Gordon (1949). "A device for quantizing, grouping, and coding amplitude-modulated pulses". PhD thesis. Massachusetts Institute of Technology.

Kraus, Karl et al. (1983). "States, effects, and operations: fundamental notions of quantum theory". In: *States, Effects, and Operations: Fundamental Notions of Quantum Theory*. Vol. 190.

Kuhn, Harold W and Albert W Tucker (1951). "Nonlinear programming". In: *Proceedings of 2nd Berkeley Symposium*. Berkeley: University of California Press, pp. 481–492.

Lahti, Pekka and Sylvia Pulmannová (1997). "Coexistent observables and effects in quantum mechanics". In: *Reports on Mathematical Physics* 39.3, pp. 339–351.

Larsson, Jan-Åke (2014). "Loopholes in Bell inequality tests of local realism". In: *Journal of Physics A: Mathematical and Theoretical* 47.42, p. 424003.

Lawvere, F William (1969). "Diagonal arguments and cartesian closed categories". In: *Category theory, homology theory and their applications II*. Springer, pp. 134–145.

Leggett, Anthony J and Anupam Garg (1985). "Quantum mechanics versus macroscopic realism: Is the flux there when nobody looks?" In: *Physical Review Letters* 54.9, p. 857.

Leitsch, Alexander, Günter Schachner, and Karl Svozil (2008). "How to Acknowledge Hypercomputation?" In: *Complex Systems* 18, pp. 131–143.

Lenstra, Arjen K et al. (1993). "The number field sieve". In: *The development of the number field sieve*. Springer, pp. 11–42.

Levin, Leonid (1973). "On the notion of a random sequence". In: *Soviet Mathematics Doklady* 14, pp. 1413–1416.

Lewenstein, Maciej et al. (2000). "Optimization of entanglement witnesses". In: *Physical Review A* 62.5, p. 052310.

Li, Ming and Paul Vitányi (1993). *An introduction to Kolmogorov complexity and its applications*. 1st ed. New York: Springer Science & Business Media.

Liang, Yeong-Cherng et al. (2010). "Nonclassical correlations from randomly chosen local measurements". In: *Physical Review Letters* 104.5, p. 050401.

Lloyd, Seth (1993). "Quantum-mechanical computers and uncomputability". In: *Physical Review Letters* 71.6, p. 943.

— (1994). "Necessary and sufficient conditions for quantum computation". In: *Journal of Modern Optics* 41.12, pp. 2503–2520.

Löfberg, Johan (2004). "YALMIP: A toolbox for modeling and optimization in MATLAB". In: *Computer Aided Control Systems Design, 2004 IEEE International Symposium on*. IEEE, pp. 284–289.

Ludwig, Günther (1983). *An Axiomatic Basis for Quantum Mechanics: Volume 1 Derivation of Hilbert Space Structure*. Berlin: Springer.

Mackey, George W (1963). *Mathematical foundations of quantum mechanics*. New York: Benjamin.

Martin-Löf, Per (1966). "The definition of random sequences". In: *Information and control* 9.6, pp. 602–619.

Masanes, Lluís, Antonio Acin, and Nicolas Gisin (2006). "General properties of nonsignaling theories". In: *Physical Review A* 73.1, p. 012112.

Masanes, Lluís, Markus P Müller, et al. (2013). "Existence of an information unit as a postulate of quantum theory". In: *Proceedings of the National Academy of Sciences* 110.41, pp. 16373–16377.

Masanes, Lluís, Stefano Pironio, and Antonio Acín (2011). "Secure device-independent quantum key distribution with causally independent measurement devices". In: *Nature communications* 2, p. 238.

Maudlin, Tim (2014a). "Reply to comment on 'What Bell did'". In: *Journal of Physics. A, Mathematical and Theoretical (Online)* 47.42.

— (2014b). "What Bell did". In: *Journal of Physics A: Mathematical and Theoretical* 47.42, p. 424010.

Mayers, Dominic and Andrew Yao (1998). "Quantum cryptography with imperfect apparatus". In: *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*. IEEE, pp. 503–509.

— (2004). "Self testing quantum apparatus". In: *QIC* 4.4, p. 273.

McKague, Matthew (2016). "Self-testing in parallel". In: *New Journal of Physics* 18.4, p. 045013.

McKague, Matthew, Tzyh Haur Yang, and Valerio Scarani (2012). "Robust self-testing of the singlet". In: *Journal of Physics A: Mathematical and Theoretical* 45.45, p. 455304.

Mermin, N David (1990a). "Extreme quantum entanglement in a superposition of macroscopically distinct states". In: *Physical Review Letters* 65.15, p. 1838.

— (1990b). "Simple unified form for the major no-hidden-variables theorems". In: *Physical Review Letters* 65.27, p. 3373.

Mezzadri, Francesco (2007). "How to generate random matrices from the classical compact groups". In: *NOTICES of the AMS* 54, pp. 592–604.

Miller, Carl A and Yaoyun Shi (2012). "Optimal robust quantum self-testing by binary nonlocal xor games". In: *arXiv preprint arXiv:1207.1819*.

Mironowicz, Piotr et al. (2016). "Increased certification of semi-device independent random numbers using many inputs and more post-processing". In: *New Journal of Physics* 18.6, p. 065004.

Moroder, Tobias et al. (2013). "Certifying systematic errors in quantum experiments". In: *Physical Review Letters* 110.18, p. 180401.

Moyal, José E (1949). "Quantum mechanics as a statistical theory". In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 45. 01. Cambridge Univ Press, pp. 99–124.

Naimark, Mark (1940). "Spectral functions of a symmetric operator". In: *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya* 4.3, pp. 277–318.

— (1943). "On a representation of additive operator set functions". In: *Dokl. Akad. Nauk SSSR*. Vol. 41, pp. 359–361.

Navascués, Miguel, Stefano Pironio, and Antonio Acín (2007). "Bounding the set of quantum correlations". In: *Physical Review Letters* 98.1, p. 010401.

Navascués, Miguel, Stefano Pironio, and Antonio Acín (2008). "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations". In: *New Journal of Physics* 10.7, p. 073013.

Norris, James R (1998). *Markov chains*. Cambridge: Cambridge university press.

Paterek, Tomasz et al. (2010). "Logical independence and quantum randomness". In: *New Journal of Physics* 12.1, p. 013019.

Pearle, Philip M (1970). "Hidden-variable example based upon data rejection". In: *Physical Review D* 2.8, p. 1418.

Peres, Asher (1990). "Incompatible results of quantum measurements". In: *Physics Letters A* 151.3-4, pp. 107–108.

— (1996). "Separability criterion for density matrices". In: *Physical Review Letters* 77.8, p. 1413.

Peres, Asher and Wojciech H Zurek (1982). "Is quantum theory universally valid?" In: *American Journal of Physics* 50.9, pp. 807–810.

Piccinini, Gualtiero (2007). "Computationalism, the Church–Turing thesis, and the Church–Turing fallacy". In: *Synthese* 154.1, pp. 97–120.

Pironio, Stefano, Valerio Scarani, and Thomas Vidick, eds. (2016). *New Journal of Physics* 18.6: *Focus on Device Independent Quantum Information [Special Issue]*.

Pitowsky, Itamar (1989). "Quantum probability, quantum logic". In: *Lecture notes in physics* 321.

— (1994). "George Boole's 'conditions of possible experience' and the quantum puzzle". In: *British Journal for the Philosophy of Science*, pp. 95–125.

Plenio, Martin B (2005). "Logarithmic negativity: a full entanglement monotone that is not convex". In: *Physical Review Letters* 95.9, p. 090503.

Popescu, Sandu and Daniel Rohrlich (1994). "Quantum nonlocality as an axiom". In: *Foundations of Physics* 24.3, pp. 379–385.

Popper, Karl R (1950a). "Indeterminism in quantum physics and in classical physics. Part I". In: *The British Journal for the Philosophy of Science* 1.2, pp. 117–133.

— (1950b). "Indeterminism in quantum physics and in classical physics. Part II". In: *The British Journal for the Philosophy of Science* 1.3, pp. 173–195.

Rains, Eric M (2001). "A semidefinite program for distillable entanglement". In: *IEEE Transactions on Information Theory* 47.7, pp. 2921–2933.

Rivest, Ronald L, Adi Shamir, and Leonard Adleman (1978). "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2, pp. 120–126.

Robertson, Howard Percy (1929). "The uncertainty principle". In: *Physical Review* 34.1, p. 163.

Rockafellar, Ralph Tyrell (2015). *Convex analysis*. Princeton: Princeton university press.

Rovelli, Carlo (1996). "Relational quantum mechanics". In: *International Journal of Theoretical Physics* 35.8, pp. 1637–1678.

Russell, Bertrand (1908). "Mathematical logic as based on the theory of types". In: *American journal of mathematics* 30.3, pp. 222–262.

— (1967). "Letter to Frege". In: *From Frege to Gödel: a source book in mathematical logic, 1879-1931*. Ed. by Jean Van Heijenoort, pp. 124–125.

Sarovar, Mohan et al. (2010). "Quantum entanglement in photosynthetic light-harvesting complexes". In: *Nature Physics* 6.6, pp. 462–467.

Scarani, Valerio and Christian Kurtsiefer (2009). "The black paper of quantum cryptography: real implementation problems". In: *arXiv preprint arXiv:0906.4547*.

Schnorr, Claus-Peter (1973). "Process complexity and effective random tests". In: *Journal of Computer and System Sciences* 7.4, pp. 376–388.

Shadbolt, Peter et al. (2012). "Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices". In: *Scientific reports* 2.

Shalm, Lynden K et al. (2015). "Strong loophole-free test of local realism". In: *Physical Review Letters* 115.25, p. 250402.

Shimony, Abner (1986). "Events and processes in the quantum world". In: *Quantum Concepts in Space and Time*. Ed. by Roger Penrose and Christopher Isham. Oxford: Clarendon Press, pp. 182–203.

Shor, Peter W (1994). "Algorithms for quantum computation: Discrete logarithms and factoring". In: *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. IEEE, pp. 124–134.

Short, Anthony J and Jonathan Barrett (2010). "Strong nonlocality: a tradeoff between states and measurements". In: *New Journal of Physics* 12.3, p. 033034.

Singh, Simon (1999). *The code book: the science of secrecy from ancient Egypt to quantum cryptography*. New York: Doubleday.

Spekkens, Robert W (2007). "Evidence for the epistemic view of quantum states: A toy theory". In: *Physical Review A* 75.3, p. 032110.

Svozil, Karl (1993). *Randomness and Undecidability in Physics*. Singapore: World Scientific.

Szangolies, Jochen (2015). *Testing Quantum Contextuality: The Problem of Compatibility*. Berlin: Springer.

Szangolies, Jochen, Hermann Kampermann, and Dagmar Bruß (2015). "Detecting entanglement of unknown quantum states with random measurements". In: *New Journal of Physics* 17.11, p. 113051.

— (2016). "Device-Independent Bounds on Detection Efficiency". In: *arXiv preprint arXiv:1609.06126*.

Szangolies, Jochen, Matthias Kleinmann, and Otfried Gühne (2013). "Tests against noncontextual models with measurement disturbances". In: *Physical Review A* 87.5, p. 050101.

Tarski, Alfred (1936). "Der Wahrheitsbegriff in den formalisierten Sprachen". In: *Studia Philosophica* 1, pp. 261–405.

Terhal, Barbara M (2000). "Bell inequalities and the separability criterion". In: *Physics Letters A* 271.5, pp. 319–326.

Toh, Kim-Chuan, Michael J Todd, and Reha H Tütüncü (1999). "SDPT3–a MATLAB software package for semidefinite programming". In: *Optimization methods and software* 11.1-4, pp. 545–581.

Tóth, Géza and Otfried Gühne (2005). "Detecting genuine multipartite entanglement with two local measurements". In: *Physical Review Letters* 94.6, p. 060501.

Turing, Alan Mathison (1936). "On computable numbers, with an application to the Entscheidungsproblem". In: *Journal of Mathematics* 58.345-363, p. 5.

Vandenberghe, Lieven and Stephen Boyd (1996). "Semidefinite programming". In: *SIAM Review* 38.1, pp. 49–95.

Vazirani, Umesh and Thomas Vidick (2014). "Fully device-independent quantum key distribution". In: *Physical Review Letters* 113.14, p. 140501.

Vedral, Vlatko et al. (1997). "Quantifying entanglement". In: *Physical Review Letters* 78.12, p. 2275.

Vidal, Guifré and Reinhard F Werner (2002). "Computable measure of entanglement". In: *Physical Review A* 65.3, p. 032314.

von Neumann, John (1932). "Zur Operatorenmethode in der klassischen Mechanik". In: *Annals of Mathematics*, pp. 587–642.

von Weizsäcker, Carl Friedrich (1985). *Aufbau der Physik*. Berlin: Hauser.

von Weizsäcker, Carl Friedrich, Thomas Görnitz, and Holger Lyre (2006). *The structure of physics*. Berlin: Springer.

Wallman, Joel J and Stephen D Bartlett (2012). "Observers can always generate nonlocal correlations without aligning measurements by covering all their bases". In: *Physical Review A* 85.2, p. 024101.

Wallman, Joel J, Yeong-Cherng Liang, and Stephen D Bartlett (2011). "Generating nonclassical correlations without fully aligning measurements". In: *Physical Review A* 83.2, p. 022110.

Weihs, Gregor et al. (1998). "Violation of Bell's inequality under strict Einstein locality conditions". In: *Physical Review Letters* 81.23, p. 5039.

Werner, Reinhard F (1989). "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model". In: *Physical Review A* 40.8, p. 4277.

— (2014a). "Comment on 'What Bell did'". In: *Journal of Physics A: Mathematical and Theoretical* 47.42, p. 424011.

— (2014b). "What Maudlin replied to". In: *arXiv preprint arXiv:1411.2120*.

Weyl, Hermann (1927). "Quantenmechanik und Gruppentheorie". In: *Zeitschrift für Physik* 46.1-2, pp. 1–46.

Wheeler, John Archibald (1974). *Add "participant" to "undecidable propositions" to arrive at physics*. Accessed on 08.09.2016. URL: `https://jawarchive.files.wordpress.com/2012/03/twa-1974.pdf`.

Wigner, Eugene (1932). "On the quantum correction for thermodynamic equilibrium". In: *Physical Review* 40.5, p. 749.

Wootters, William K and Wojciech H Zurek (1982). "A single quantum cannot be cloned". In: *Nature* 299.5886, pp. 802–803.

Woronowicz, Stanisław Lech (1976). "Positive maps of low dimensional matrix algebras". In: *Reports on Mathematical Physics* 10.2, pp. 165–183.

Yanofsky, Noson S (2003). "A universal approach to self-referential paradoxes, incompleteness and fixed points". In: *Bulletin of Symbolic Logic* 9.03, pp. 362–386.

Yu, Sixia and Choo Hiap Oh (2012). "State-independent proof of Kochen-Specker theorem with 13 rays". In: *Physical Review Letters* 108.3, p. 030402.

Zeilinger, Anton (1999). "A foundational principle for quantum mechanics". In: *Foundations of Physics* 29.4, pp. 631–643.

Zhang, Xiang et al. (2013). "State-independent experimental test of quantum contextuality with a single trapped ion". In: *Physical Review Letters* 110.7, p. 070401.

Žnidarič, Marko et al. (2007). "Detecting entanglement of random states with an entanglement witness". In: *Journal of Physics A: Mathematical and Theoretical* 40.45, p. 13787.

Zuse, Konrad (1969). *Rechnender Raum*. Braunschweig: Friedrich Vieweg & Sohn.

Zwick, Martin (1978). "Quantum measurement and Gödel's proof". In: *Speculations in Science and Technology* 1.2, p. I978.

Życzkowski, Karol, Paweł Horodecki, et al. (1998). "Volume of the set of separable states". In: *Physical Review A* 58.2, p. 883.

Życzkowski, Karol, Karol A Penson, et al. (2011). "Generating random density matrices". In: *Journal of Mathematical Physics* 52.6, p. 062201.