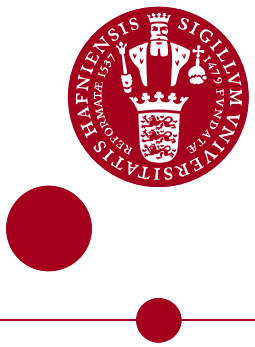
UNIVERSITY OF COPENHAGEN



Certification of quantum systems through self testing

Master's thesis
Department of Mathematical Sciences
University of Copenhagen

Sigurd A. L. Storgaard
qmt293

Primary supervisor: Simon Schmidt

Secondary supervisor: Laura Mančinska

Date: May 30, 2022

Abstract

Self testing provides a framework for studying quantum mechanical descriptions of devices based only on classical interaction. It represents the strongest type of certification possible when one only has access to the statistics obtained from a large number of measurements. In this thesis, we study self testing both at the level of correlations and maximal Bell inequality violation with a particular focus on the relation to concepts from convex geometry. We extend a result in [TFR+21] by providing a nonlocal game with optimal winning probability in a unique probability point that has inequivalent realizations. Moreover, we study a recent extension of self testing to prepare-and-measure scenarios. We introduce a novel type of weak unbiasedness in measurements which we show that certain quantum random access codes (QRAC) are capable of certifying.

Contents

1 Introduction **3**
1.1 Device independence 4
1.2 History and applications 6
1.3 Known results and our contributions 7
1.4 Thesis overview 8

2 Preliminaries **9**
2.1 Quantum states and measurements 10
2.2 States and measurements as Bloch vectors 12
2.3 Geometry of convex sets 15

3 Correlation sets **17**
3.1 Convexity and Bell inequalities 19
3.2 Tsirelson's problem 21

4 Definition of self testing **22**
4.1 Exact self testing 23
4.2 Robustness 27

5 Nonlocal games **28**
5.1 Self testing Bell inequalities 29
5.2 The CHSH game 30
5.3 Sum of squares (SOS) decomposition 33
5.4 Self testing properties of the CHSH game 33
5.5 Linear constraint system games 36
5.6 Weak self testing 40

6 Mutual unbiasedness **42**
6.1 Mutually unbiased bases 42
6.2 Weaker notions of unbiasedness 44

7 Separation of self testing correlations and exposed points **46**
7.1 Inequivalent realizations of $\omega_q^*(\mathcal{G}_{\text{MUM}})$ 50

8 Semi-device independent self testing **52**
8.1 QRACs 52

9 Discussion, conclusion and open problems **56**

1 Introduction

Some of the key features of quantum theory that separate it from classical theory are that quantum states may be entangled and measurements may be incompatible. As a consequence, quantum theory implies striking observable phenomena which are incompatible with classical theory. In 1964, John Bell showed that applying incompatible measurements to entangled states can lead to correlations that are strictly stronger than those of any classical model [Bel64]. This phenomenon has become known as Bell nonlocality.

In the early 1990s it was pointed out, for example in [Tsi93], that some Bell nonlocal correlations can only be achieved by *specific* measurements on *specific* states. This observation spawned the field of *self testing*. The aim of self testing is to identify those correlations that admit essentially unique quantum mechanical description. In even broader terms, self testing investigates to which extent it is possible to give quantum mechanical descriptions of devices with which we are only allowed to interact classically.

In order to understand in which sense quantum correlations might be stronger than classical correlations it is necessary to understand exactly what is meant by the word 'local'. In this introductory section we start with a classical model and describe the bounds on the correlations that can produced by this. Since the rest of the thesis is devoted to quantum correlations, we, for now, remain in a high-level picture with respect to these.

Classical models are described by so-called *local hidden variables*. Imagine two spatially separated parties. We call these Alice and Bob. Each of them is given a device. Their devices may have interacted in the past. For example, they may have been produced by a common source. We may think of these devices as "black boxes" i. e. Alice and Bob do not know what they consist of.

Each of the two devices is equipped with a (finite) number of measurement settings. Upon choosing a certain measurement setting Alice and Bob get some outcomes. There are a finite number of different outcomes on both Alice's and Bob's device. To fix notation, let x and y denote the choice of measurement setting of Alice and Bob respectively and $\mathcal{X}$ and $\mathcal{Y}$ denote the finite sets containing all the measurement settings. Let a and b denote the outcome of Alice and Bob respectively and $\mathcal{A}$ and $\mathcal{B}$ denote the finite sets of possible outcomes.

Since Alice and Bob are assumed not to know anything about their devices, the can only probe their devices by choosing measurement settings x and y and observing some outcomes a and b. Now, imagine moreover that Alice and Bob are spatially separated such that after receiving their devices, they are not allowed to communicate. This outlined scenario is typically called a *Bell scenario* or a *Bell experiment*. We have sketched this in Figure 1 below.

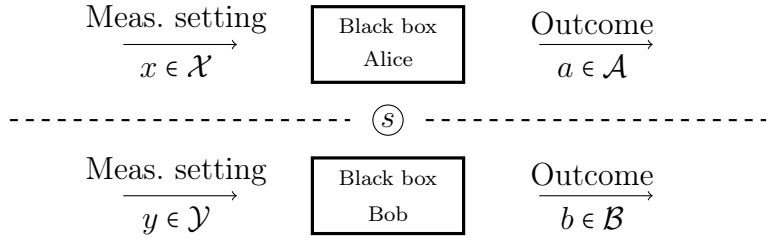


Figure 1: *Bell experiment. In the quantum version, a source is situated between the devices distributing a certain quantum state.*

The experiment proceeds as follows. After having been spatially separated and having received their devices, Alice and Bob make a large number of measurements (in an independent and identically distributed way) on their respective devices. Then, when this data collection is over, they come together to collect the statistics of their experiment. More precisely, they obtain, for each pair of measurement setting $(x, y) \in \mathcal{X} \times \mathcal{Y}$ a probability distribution given by the conditional probabilities, $p(ab|xy)$. The collection of all the probability distributions

$$\{p(ab|xy)|a \in \mathcal{A}, b \in \mathcal{B}\}_{x\in\mathcal{X},y\in\mathcal{Y}} \tag{1}$$

is called a *correlation*.

Now, the locality assumption is that we can identify a set of variables, λ that have a joint causal influence on the outcomes. With a fixed λ the measurement outcomes, in a local hidden variable model are independent, i. e.

$$p(ab|xy, \lambda) = p(a|x, \lambda)p(b|y, \lambda). \tag{2}$$

The aforementioned discovery of Bell is that in the quantum version of the above experiment (which we will introduce below), correlations can be obtained that are provably stronger than any local hidden variable can allow.

1.1 Device independence

In the quantum version of the Bell experiment we imagine that the the black boxes collectively make up a quantum state upon which Alice and Bob perform their measurements. It could be argued that once measured, the state is destroyed and therefore it is impossible to carry out enough measurements to meaningfully establish a correlation. Because of this concern we imagine instead that a source is positioned between the black boxes distributing a specific bipartite quantum state sending one part to Alice and the other part to Bob. Then, each time Alice and Bob measure, a new identical copy of the state is distributed making it possible to collect a correlation. It is still possible to use Figure 1 to illustrate this situation. Just imagine, a source situated between Alice's and Bob's devices distributing the specific state. The scenario thus described, where Alice and Bob have no knowledge about the measurements or the state emitted by the source is

called a *device-independent scenario*.

Remarkably, a direct consequence of Bells discovery is that even with such limited knowledge, Alice and Bob can in fact deduce whether or not the source emits entangled states. To understand this, we must introduce the notion of *Bell nonlocality*. At the core of Bell nonlocality lie Bell inequalities. Notice that we can view a correlation $\{p(ab|xy)\}$ as a vector $p \in \mathbb{R}^{|\mathcal{X}|\times|\mathcal{Y}|\times|\mathcal{A}|\times|\mathcal{B}|}$. A *Bell inequality* is given by a vector $B \in \mathbb{R}^{|\mathcal{X}|\times|\mathcal{Y}|\times|\mathcal{A}|\times|\mathcal{B}|}$ and a bound β such that any correlation obeying the local hidden variable model satisfies,

$$\langle B, p\rangle \leq \beta. \tag{3}$$

where $\langle\cdot,\cdot\rangle$ denotes the standard inner product on real vector spaces. It turns out, as we will see later, that if the source is emitting a non-entangled state then the correlation in fact complies with the local hidden variable model described earlier. Alice and Bob can therefore compare their measurement statistics up against any of their known Bell inequalities. If they observe that one is violated, they will have certified the presence of entanglement. Bell inequality violations thus have the remarkable ability of witnessing quantum entanglement without the need of any knowledge about the underlying physical system.

But can we make more refined statements? Can we deduce more about the state of the source than just entanglement if we only have access to a correlation? And what can we say about the measurements? It turns out, as alluded to earlier, that certain correlations can be obtained in *essentially* unique ways, leaving us with the ability to gain knowledge about the underlying physical systems based solely on classical interaction with these. What we mean by "essentially" will be made clearer in Sec. 4. For now just note that there are natural limitations stemming from the mathematical framework of quantum mechanics that prevent us from deducing the exact form of the state and measurements. For example, the application of isometries will leave the measurement statistics unchanged (see Sec. 2.1). For this introductory discussion the following tentative definition will suffice

Informal definition of self testing: The correlation $p \coloneqq p(ab|xy)$ is a self test if it is induced in an (essentially) unique way i. e. using (essentially) unique measurements applied to an (essentially) unique state.

In any experimental context there is inevitably uncertainty associated with the obtained correlations. Hence it is desirable that such self testing statements are *robust* to noise. Informally, this means that if a set of correlations is close to some correlations we have in mind, then the states and measurements producing these are close (in some norm) to certified ones.

We also give here a tentative description of a so-called *nonlocal game*. A nonlocal game provides a convenient recasting of a Bell inequality in terms of a hypothetical game played by three parties - two cooperating, noncommunicating players -

Alice and Bob - and a *referee*. The referee asks Alice and Bob questions from the sets $\mathcal{X}$ and $\mathcal{Y}$ respectively, according to some probability distribution. Alice and Bob then answer with elements from the sets $\mathcal{A}$ and $\mathcal{B}$, respectively.

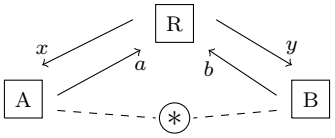


Figure 2: *Illustration of a nonlocal game. The shared quantum state upon which Alice and Bob can perform measurements in a quantum model is symbolized by* $*$.

The referee holds a *verification function*, which can be viewed as the "rules of the game". The verification function depends on the answers/questions and takes values in $\{0, 1\}$. If it is equal 0 Alice and Bob *lose*, if it is equal to 1 they *win*. Alice and Bob are allowed to make a strategy before the game starts. We think of a strategy as a correlation. If Alice and Bob have a shared quantum state upon which they can perform measurements, it is clear, since some correlations are not possible classically, that Alice and Bob might be able to perform better in such a game than they would be in a classical setting.

1.2 History and applications

Although anticipated in 1998 [MY98] the formalism behind self testing was established in the seminal 2004 paper "Self testing quantum apparatus" by Mayers and Yao who also coined the term "self testing" [MY04]. Since these inaugural papers, attacking problem of characterizing quantum systems through the framework of self testing has developed into a prosperous field within quantum information science with far reaching applications both theoretical and practical.

On the theoretical side the field of self testing has, most notably, contributed to the establishment of the MIP*=RE identity in complexity theory [JNV+21]. This led to the solution (in the negative) of the famous Connes' embedding problem. Another consequence was the solution of Tsirelson's problem [Tsi06b] by showing that the tensor and commuting models for quantum correlations are distinct. Generally, as we will see later the concept of self testing has played a major role in the recent advancement in our understanding of the structures of different sets of quantum correlations.

The notion of self testing came to life due to an ambition of designing trustworthy quantum key distribution schemes [MY98]. Hence the links to quantum cryptography are inherent from the very beginning. Also quantum randomness generation can be based on self testing. Suppose Alice and Bob collect correlations that certify the presence of a pure entangled state and some measurements. Since local measurements on pure entangled states yield random bits, this is a way of producing certified randomness (see [AM16]).

1.3 Known results and our contributions

In this section we collect some known results on self testing. This is done by posing a series of questions after which we state, what is known. The purpose of this is to put contributions contained in this thesis into a relevant context and to provide the reader with a thorough overview. First time readers on the topic may benefit from skipping this section and returning to it after Sec. 4.

Which correlations can be self tests? One of the few general statements we can make about the geometry of the quantum set of correlations is that it is convex. As shown in [GKW+18], if p is a self test it is an extreme point. So if p is not an extreme point it is not a self test. That does not mean that a nonextreme point cannot be a self test with respect to a state. In fact, in [Kan20] the author exhibits a Bell inequality which is maximally violated in a line segment in the set of quantum correlations. It is shown, that there exists a one-parameter family of inequivalent measurements on Alice and Bob achieving its maximal violation. The maximal violation does however self test a pair of maximally entangled qubits. In [Kan20], such a phenomenon is termed "weak self testing". In this thesis we will present a simplified example of weak self testing which, to the best of our knowledge is new.

It is shown in [Kan20] that in the endpoints of the considered line segment a full self testing statement is possible. The endpoints are extreme points so the follow up question naturally is:

Is every extreme point of the set of quantum correlations a self test? Recently this question has been answered in the negative [TFR+21]. There, a Bell inequality is constructed whose maximal violation certifies a maximally entangled state. On the measurement side, they show that if certain relations between Bob's measurements hold, the maximal violation can be achieved. Mutually unbiased bases, in particular fulfill these relations. And since in dimensions greater than 4 there exist inequivalent mutually unbiased bases the maximal violation is not a self test. It is then shown that their Bell inequality is maximally violated in a unique correlation p. We will review this result and contribute with a nonlocal game which proves the same statement i. e. that not all extreme points are self tests. We also note here that since the Bell function has a unique maximizer, the maximal violation in fact happens in an exposed point. Moreover the connection between measurements being inequivalent considered as mutually unbiased bases and in terms self testing is explored in more depth.

Which states can be self tested? First of all we note that is a bi-product of the work of [SVW16] that one can only hope to self test pure states. As shown there, for any correlation, $p := p(ab|xy)$, produced by a mixed state, there is a pure state of the same dimension which is compatible with p. Hence, applying a unitary to this pure state inducing the same correlation one cannot end up with a mixed state since isometries preserve purity. A remarkable result, on the other hand,

is that any pure bipartite entangled state can be self tested by some correlation. This is shown in [CGS17].

Can we self test states of unbounded local dimension with input/output sets of bounded sizes? Surprisingly, it is shown in [Fu22] that one can self test a maximally entangled state of unbounded local dimension using constant size correlations. However this scheme involves correlations with over 100 questions per party [MPS21]. In [MPS21] this result is refined: The authors show that self test the maximally entangled state of unbounded local dimension using just 4 binary output measurements per party.

Does self testing imply robust self testing? At the level of nonlocal games the answer is no. This has been shown recently [MS22a]. However, the question is different if one is concerned with a mere correlation. We will discuss a geometric picture of the difference between nonrobust self testing in terms of nonlocal games and correlations in Sec. 9.

Can the self testing notion be extended to other scenarios? Yes. Self testing ideas have recently been extended to prepare-and-measure (PaM) scenarios in [TKV+18, FK19]. It is shown in [TKV+18, FK19], that if one imposes assumptions about the dimension of the system being transmitted it is possible to make certification statements about the measurement device. Due to this apriori assumption, the scenario is called *semi-device independent*. A prime example of such is a so-called quantum random access code (Sec. 8), which is a protocol that encodes each element of $\{1, ..., d\}^n$ into distinct states. The encoded state is then sent to a measurement device that can extract one out of these n dits with a high probability.

In [FK19] it is shown that some QRACs certify that the measurements are done in mutually unbiased bases (MUB). We will introduce a strictly weaker notion of unbiased measurements called *mutually orthogonal measurements* (MOM). In prime dimensions these two classes of measurements coincide. We will show that many QRACs certify that the measurements are MOM which in nonprime dimensions is strictly weaker than being MUB.

1.4 Thesis overview

In an attempt to make the thesis as self contained as possible we start with a preliminary section containing: (1) A precise mathematical formulation of *Dirac's braket notation*, (2) a definition of quantum states and measurements, (3) a definition of Bloch vector representations of states and measurements and lastly (4) an introduction to some convex geometry. We have aimed for minimal introductions only comprising what is needed for our further investigations about self testing.

In section 3 we introduce the different correlation sets we will be studying. We

also review what is known about how these compare to each other. In particular, the so called Tsirelson's problem and its relation to the Connes' embedding problem in von Neumann algebras will be mentioned but not treated in depth.

In section 4 we give a formal definition of self testing. More precisely, we define what is meant by self testing with respect to correlations. We also define robust self testing. In section 5 we introduce nonlocal games and self testing with respect to these. We also discuss differences between self testing with respect to correlations and with respect to nonlocal games. As an example we review the proof that the well-known CHSH game self tests a maximally entangled pair of qubits. We also discuss linear constraint system games and how these can be systematically studied with group- and representation theoretic tools.

In section 6 we discuss different unbiasedness principles in measurements which turns out to be necessary in order to understand one of the main examples of this thesis which section 7 is devoted to. We show a nonself testing nonlocal game with maximal winning probability in an exposed point of the quantum correlation sets. In section 8 we study the recent extension [TKV+18, FK19] of self testing to prepare and measure scenarios and show how certain quantum random access codes can at best certify a weakened notion measurements corresponding to mutually unbiased bases.

In the last section we collect the results of the thesis and discuss the rather complex relationship between boundary points of the set of quantum relations and correlations with different self testing properties. We discuss open problems and scopes for further research.

2 Preliminaries

For some natural number n, the set $\{1, ..., n\}$ will be denoted $[n]$. All Hilbert spaces in this thesis will be over $\mathbb{C}$. The space of continuous, linear operators from one Hilbert space $\mathcal{H}_A$ to another $\mathcal{H}_B$ will be denoted $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$. We will use the notation $\mathcal{L}(\mathcal{H}) \coloneqq \mathcal{L}(\mathcal{H}, \mathcal{H})$. The Hermitian conjugate of a linear operator $X \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ will be denoted $X^\dagger \in \mathcal{L}(\mathcal{H}_B, \mathcal{H}_A)$. We will only consider separable Hilbert spaces. They will oftentimes be finite dimensional and identified with $\mathbb{C}^d$.

Let $\mathcal{H}$ be a Hilbert space with inner product denoted $\langle \cdot, \cdot \rangle$. Let $\psi \in \mathcal{H}$ and consider the map $|\psi\rangle \in \mathcal{L}(\mathbb{C}, \mathcal{H})$ given by $z \mapsto z\psi$. Its adjoint, $\langle \psi| \coloneqq |\psi\rangle^\dagger$, is the element of the dual space $\mathcal{L}(\mathcal{H}, \mathbb{C})$ given by the linear functional $\varphi \mapsto \langle \psi, \varphi \rangle$. The map $\langle \psi| \circ |\varphi\rangle \in \mathcal{L}(\mathbb{C})$ given by $z \mapsto \langle \psi, \varphi \rangle z$ will be denoted $\langle \psi | \varphi \rangle$. The map $|\psi\rangle \circ \langle \varphi| \in \mathcal{L}(\mathcal{H})$ given by $\xi \mapsto \langle \varphi, \xi \rangle \psi$ will be denoted $|\psi\rangle\langle\varphi|$. As is customary among physicists, we identify an element ψ with the map $|\psi\rangle$ and the inner product $\langle \cdot, \cdot \rangle$ with the map $\langle \cdot | \cdot \rangle$ [HL21]. We denote the computational basis by the elements $\{|i\rangle\}_{i \in \mathbb{N}}$ where $\mathbb{N}$ is simply replaced by $[d]$ if $\mathcal{H}$ has dimension d.

If $\mathcal{H}$, $\mathcal{K}$ are Hilbert spaces we define $\mathcal{T}(\mathcal{H},\mathcal{K}) \coloneqq \mathcal{L}\big(\mathcal{L}(\mathcal{H}),\mathcal{L}(\mathcal{K})\big)$. If $\mathcal{H}$ is finite dimensional, *the trace map*, denoted Tr, belongs to $\mathcal{T}(\mathcal{H},\mathbb{C})$. If $\mathcal{H}$ is infinite dimensional then the trace map is only well defined for *trace class* operators, i. e. operators with finite Hilbert-Schmidt norm. We will only encounter trace class operators. The trace map is given by $X \mapsto \sum_{i\in\mathbb{N}} \langle i|X|i\rangle$ and it is, in particular, basis independent and invariant under cyclic permutations. We will also make heavy use of the *partial trace*. This is denoted $\mathrm{Tr}_{\mathcal{K}} \in \mathcal{T}(\mathcal{H}\otimes\mathcal{K},\mathcal{H})$ and defined as $\mathrm{Tr}_{\mathcal{K}} \coloneqq \mathbb{1}_{\mathcal{H}} \otimes \mathrm{Tr}$. Oftentimes Hilbert spaces are label by some registers, $\mathcal{H}_A$, $\mathcal{H}_B$ etc. In this case, we use a subscript on operators acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ i. e. $X_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$. We will also oftentimes use the short hand notation $\mathcal{H}_{A,B} \coloneqq \mathcal{H}_A \otimes \mathcal{H}_B$. If $X_{AB} \in \mathcal{L}(\mathcal{H}_{A,B})$ we use the notation for $X_A = \mathrm{Tr}_B[X_{AB}]$.

An invertible operator $U \in \mathcal{L}(\mathcal{H})$ fulfilling $U^\dagger = U^{-1}$ is called *unitary*. An operator $V \in \mathcal{L}(\mathcal{H},\mathcal{K})$ which fulfills $V^\dagger V = \mathbb{1}_{\mathcal{H}}$ is called an *isometry*. Isometries have the property of preservation of the inner product. The symbol $\leq$ will be used to denote inequalities with respect to the partial ordering of Hermitian operators, i. e. two Hermitian operators O_1, O_2 fulfill $O_1 \leq O_2$ if and only if $O_2 - O_1$ is positive semi-definite.

2.1 Quantum states and measurements

A *pure quantum state* is an element, $|\varphi\rangle \in \mathcal{H}$ of unit norm, i. e. $\big|\langle\varphi|\varphi\rangle\big| = 1$. If $|\varphi\rangle$ is of unit norm, then $P \coloneqq |\varphi\rangle\langle\varphi|$ is a projection operator (i. e. $P^2 = P$) onto the one dimensional subspace spanned by $|\varphi\rangle$. On the other hand, since any projection operator, $P \in \mathcal{L}(\mathcal{H})$, onto a one dimensional subspace is a compact self adjoint operator, the spectral decomposition theorem ensures that there is a unit norm element, $|\psi\rangle \in \mathcal{H}$, such that $P = |\psi\rangle\langle\psi|$. We see that pure states can equivalently be represented as rank one projection operators.

A convex combination, ϱ, of pure states with n terms, i. e.

$$\varrho = \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i| . \tag{4}$$

where $p_i \geq 0$ and $\sum_{i=1}^n p_i = 1$ is called a *mixed state*. Physically, a mixed state corresponds to a system about which, we know that it is in state $|\psi_i\rangle$ with probability p_i.

Note that ϱ is positive semi-definite and has unit trace. Conversely, by the spectral decomposition theorem, any positive semi-definite, unit trace operator has an associated probability distribution over pure states and can thus be written on the form of (4). Hence the following definition

Definition 1. (*Density operator*) A positive semi-definite operator $\varrho \in \mathcal{L}(\mathcal{H})$ with unit trace is called a *density operator* or simply a *quantum state*. The set of density operators on $\mathcal{H}$ is denoted $\mathcal{D}(\mathcal{H})$.
•

An important notion about quantum states is that of entanglement. A state, ϱ_{AB}, on a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ is said to be *separable* if it admits a decomposition into a convex combination of product states i. e. if there exist $\varrho_i \in \mathcal{D}(\mathcal{H}_A)$ and $\sigma_i \in \mathcal{D}(\mathcal{H}_B)$ such that

$$\varrho_{AB} = \sum_i p_i \varrho_A^i \otimes \varrho_B^i. \tag{5}$$

If such a decomposition is not possible we call the state *entangled*. We will call the state

$$|\Phi_d\rangle := \tfrac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle \tag{6}$$

the *maximally entangled state* of local dimension d and reserve the symbol $|\Phi\rangle := |\Phi_2\rangle$. States on $\mathbb{C}^2$ are called *qubits*. So the state $|\Phi\rangle$ will sometimes be called a *maximally entangled pair of qubits*.

We will need the concept of *purification*: Consider a mixed state $\varrho_A \in \mathcal{D}(\mathcal{H}_A)$. Let $\mathcal{H}_P$ be some other Hilbert space and $|\phi\rangle_{AP} \in \mathcal{H}_{A,P}$ be some pure state. If $\varrho_A = \mathrm{Tr}_P[|\phi\rangle\langle\phi|_{AP}]$ we say that $|\phi\rangle_{AP}$ is a *purification* of ϱ and will call $\mathcal{H}_P$ a *purification space*. Purifications exist for any mixed state $\varrho_A = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|_A$. Indeed, one can just choose some $\mathcal{H}_P \cong \mathcal{H}_A$, then $|\phi\rangle_{AP} = \sum_i \sqrt{\lambda_i} |\psi_i\rangle |i\rangle$ is a purification of ϱ_A.

A *quantum measurement* is a set of measurement operators $\{M_x\}_{x\in\mathcal{X}} \subseteq \mathcal{L}(\mathcal{H})$, fulfilling the following completeness relation

$$\sum_{x\in\mathcal{X}} M_x^\dagger M_x = \mathbb{1}_{\mathcal{H}}. \tag{7}$$

where x refers to the outcome coming from the finite outcome set $\mathcal{X}$. The relation (7) ensures that the probability of obtaining some measurement outcome is 1. The most natural way of labeling the measurement outcomes is by the first $|\mathcal{X}|$ natural numbers. Hence, we let $\mathcal{X} = [N]$ for some $N \geq 1$. If initially the system is in state $\varrho \in \mathcal{D}(\mathcal{H})$, then performing measurement $\{M_x\}_{x\in[N]}$ yields a probability,

$$\mathrm{Tr}\left[M_x^\dagger M_x \varrho\right] \quad \text{(Born's rule)}, \tag{8}$$

of getting outcome x.

Since we will exclusively be concerned with measurement outcome statistics, we omit considerations about the state of the system after measurement. The common formalism to use in this case is that of *positive operator-valued measures* (POVMs)

Definition 2. (POVM) A *positive operator-valued measure* (POVM) on $\mathcal{H}$ is a partition of unity into positive semi-definite operators.
•

The motivation behind this definition is that for any quantum measurement $\{M_x\}$, the collection $\{Q_x\}$ where $Q_x \coloneqq M_x M_x^\dagger$ is a POVM. If a quantum system is in state $\varrho \in D(\mathcal{H})$ then the probability of getting outcome x upon measurement is $\mathrm{Tr}[Q_x \varrho]$. Hence the set of operators given by $\{Q_x\}$ is sufficient to determine the outcome statistics.

Conversely, if $\{Q_x\}$ is a POVM, then there is a unique quantum measurement, $\{M_x\}_{x\in[N]}$, associated with it: This follows from the fact that positive semi-definite matrices have unique positive semi-definite square roots. A POVM whose elements are idempotent is called *projective*. With these considerations in mind we will use the terms measurement and POVM synonymously throughout this thesis.

There is a similar notion of 'purification' of POVMs to that of mixed states. This is given By *Naimark's dilation theorem* which states that if $\{Q_x\} \subseteq \mathcal{L}(\mathcal{H}_A)$ is a POVM and $X \in \mathcal{L}(\mathcal{H}_A)$ then there exists a Hilbert space $\mathcal{H}_E$ and a projective measurement $\{P_x\} \in \mathcal{L}(\mathcal{H}_{A,E})$ such that $\mathrm{Tr}[Q_x X] = \mathrm{Tr}[P_x X \otimes |0\rangle\langle 0|_E]$.

We will define a quantum *observable* on $\mathcal{H}$ to be a self-adjoint operator $O \in \mathcal{L}(\mathcal{H})$ fulfilling $-\mathbb{1} \leq O \leq \mathbb{1}$. Note that a binary POVM $\{A_0, A_1\}$ can equivalently be given as a single observable $O = A_0 - A_1$ in the sense that for any O with $-\mathbb{1} \leq O \leq \mathbb{1}$ there exists a unique binary POVM $\{A_0, A_1\}$ such that $O = A_0 - A_1$. Note also that by squaring O we obtain the inequality

$$A_0^2 + A_1^2 \leq \mathbb{1} + [A_0, A_1]_+, \tag{9}$$

where $[\cdot,\cdot]_+$ is the anti commutator i. e. $[A, B]_+ \coloneqq AB + BA$. The inequality (9) is strict unless $\{A_0, A_1\}$ is projective. On the other hand, for a projective measurement, $\{A_0, A_1\}$, the corresponding observable O squares to identity. Therefore, a binary POVM is projective if and only if its corresponding observable fulfills $O^2 = \mathbb{1}$. For later reference we will use $[\cdot,\cdot]_-$ to denote the usual commutator i. e. $[A, B]_- \coloneqq AB - BA$.

2.2 States and measurements as Bloch vectors

Let $\mathcal{H} \cong \mathbb{C}^d$. In this section we briefly review the Bloch vector representation of quantum states (for a more in-depth treatment see [MS22b]). We will extend the notion to include representations of POVMs as real vectors. Let $\boldsymbol{\sigma} \coloneqq \{\sigma_i\}_{i\in[d^2-1]}$ be a subset of $\mathcal{L}(\mathcal{H})$ fulfilling

$$\sigma_i = \sigma_i^\dagger,\ \mathrm{Tr}[\sigma_i] = 0,\ (\sigma_i, \sigma_j)_{HS} = 2\delta_{ij}. \tag{10}$$

for all $i, j \in [d^2 - 1]$. In other words, $\boldsymbol{\sigma} \cup \{\mathbb{1}_d\}$, is a set of Hermitian, traceless, mutually orthogonal (with respect to $(\cdot,\cdot)_{HS}$) operators that span $\mathcal{L}(\mathcal{H})$. Such a set is called a *set of generators*. A very important example of a set of generators of $\mathcal{L}(\mathbb{C}^2)$ is the *Pauli operators* given by

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\quad \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ and } \sigma_X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{11}$$

We reserve the symbols σ_X, σ_Y and σ_Z for the three Pauli operators. For larger dimensions a common choice of generators is the set of *Gell-Mann matrices*.

It follows from the natural vector space structure of $\mathcal{L}(\mathcal{H})$, that if $X \in \mathcal{L}(\mathcal{H})$, there exist unique $\alpha_0 \in \mathbb{C}$ and $\alpha \in \mathbb{C}^{d^2-1}$ such that

$$X = \alpha_0 \mathbb{1}_d + \alpha \cdot \boldsymbol{\sigma}, \tag{12}$$

where $\alpha \cdot \boldsymbol{\sigma} := \sum_{i=1}^{d^2-1} \alpha_i \boldsymbol{\sigma}_i$. Note, that by the defining properties of generators in (10), we have $\alpha_0 d = \mathrm{Tr}[X]$ and $2\alpha_i = \mathrm{Tr}[X\sigma_i]$ and that the operator, X, is Hermitian if and only if α_0 and α are real. Thus, for any density operator, $\varrho \in \mathcal{D}(\mathcal{H})$, the component α_0 must be equal to $\frac{1}{d}$. In this way, the state can be uniquely defined by an element of $\mathbb{R}^{d^2-1}$.

Definition 3. (*Bloch vector*). Let $\varrho \in \mathcal{D}(\mathcal{H})$. The unique real vector $\beta \in \mathbb{R}^{d^2-1}$ such that

$$\varrho = \tfrac{1}{d}\mathbb{1}_d + \tfrac{1}{2}\beta \cdot \boldsymbol{\sigma} \tag{13}$$

is called the *Bloch vector (representation)* of ϱ.
•

The Bloch vector representation of some state $\sigma \in \mathcal{D}(\mathcal{H})$ is explicitly given as

$$\beta = (\mathrm{Tr}[\varrho\sigma_1], ..., \mathrm{Tr}[\varrho\sigma_{d^2-2}]). \tag{14}$$

If r is any vector in $\mathbb{R}^{d^2-1}$, we cannot guarantee that $\frac{1}{d}\mathbb{1}_d + \frac{1}{2} r \cdot \boldsymbol{\sigma}$ is positive semi-definite. Hence the following definition

Definition 4. (*Bloch space*) The set of Bloch vectors i. e.

$$\mathcal{B}_d := \{\beta \in \mathbb{R}^{d^2-1} : \tfrac{1}{d}\mathbb{1}_d + \tfrac{1}{2}\beta \cdot \boldsymbol{\sigma} \geq 0\} \tag{15}$$

is called *Bloch space*.
•

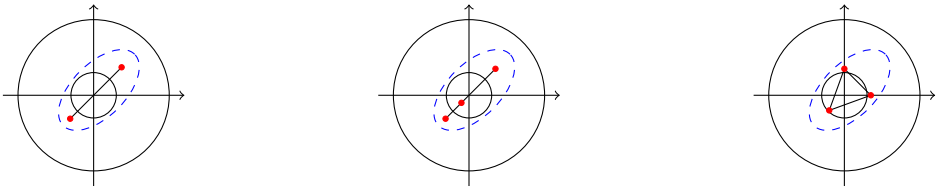
It can be shown that $\mathcal{B}_d$ is a compact and convex and that the following inclusions hold (see e.g. [MS22b]),

$$\{r \in \mathbb{R}^{d^2-1} : |r| \leq r_d\} \subseteq \mathcal{B}_d \subseteq \{r \in \mathbb{R}^{d^2-1} : |r| \leq R_d\}. \tag{16}$$

where $r_d := \sqrt{\frac{2}{d(d-1)}}$ and $R_d := \sqrt{\frac{2(d-1)}{d}}$ called the in-radius and out-radius respectively. Note that for qubits we have $r_2 = R_2 = 1$. The above inclusions coincide in this case and Bloch space becomes the well-known unit ball.

Suppose $\varrho, \varrho' \in \mathcal{D}(\mathcal{H})$ with corresponding Bloch vectors $\beta(\varrho)$ and $\beta(\varrho')$. The following relation between the overlap of ϱ and ϱ' and the inner product of their Bloch vectors will prove useful,

$$\mathrm{Tr}[\varrho\varrho'] = \tfrac{1}{d} + \tfrac{1}{2}\langle \beta(\varrho), \beta(\varrho') \rangle . \tag{17}$$



(a) Two Bloch vectors on a line segment through the origin: They define a unique two outcome POVM.

(b) Three Bloch vectors on line segment. Gives one-parameter family of three outcome POVMs.

(c) Three Bloch vectors spanning two dimensions: They define a unique three outcome POVM.

Figure 3: *Bloch vector representations of two- and three outcome POVMs.*

We can also view measurements in terms of Bloch vectors. Let $\{A_i\}_{i\in[k]}$ be a k-outcome POVM. Each A_i has a unique $\nu_i \in \mathbb{R}^{d^2-1}$ and $\mu_i > 0$[1] such that

$$A_i = \mu_i \mathbb{1} + \nu_i \cdot \boldsymbol{\sigma}. \tag{18}$$

Completeness, i. e. $\sum_i A_i = \mathbb{1}_d$, implies

$$\sum_i \mu_i = 1 \text{ and } \sum_i \nu_i = 0. \tag{19}$$

We rewrite (18) as

$$A_i = \mu_i d \left(\tfrac{1}{d}\mathbb{1}_d + \tfrac{1}{2}\tfrac{2}{\mu_i d}\nu_i \cdot \boldsymbol{\sigma} \right). \tag{20}$$

Since A_i is positive semi-definite we must have $\frac{2}{\mu_i d}\nu_i \in \mathcal{B}_d$. From (19) our k-outcome POVM can be viewed in Bloch space as the vertices of a polytope with the origin contained in its interior. If $k = 2$, the POVM corresponds to a line segment through the origin. If $k = 3$ the POVM correpsonds to a triangle containing the origin in its interior or a line segment through the origin (see Figure 3). In general a k-outcome POVM can be a k'-polytope for $k' \in [k-1]$. Based on this discussion we make the following definition,

Definition 5. *(Bloch vector representation of POVM).* Let $\{A_i\}_{i\in[k]}$ be a k-outcome POVM where $A_i = \mu_i\mathbb{1} + \nu_i \cdot \sigma$. *The Bloch vector representation of* $\{A^i\}_{i\in[k]}$ is defined as the subset, $\{m_i\}_{i\in[k]} \subseteq \mathcal{B}_d$, where $m_i = \frac{2}{\mu_i d}\nu_i$.
•

Unfortunately, we can not associate a unique k-outcome POVM to any set of Bloch vectors $\{m_i\}_{i\in[k]}$ even though this set does not contradict (19). As a simple example consider the one parameter family of three outcome POVMs given by

$$A_1 = s\mathbb{1} + s\sigma_X,\ A_2 = \tfrac{2-4s}{3}\mathbb{1} + \tfrac{1-2s}{3}\sigma_X \text{ and } A_3 = \tfrac{1+s}{3}\mathbb{1} - \tfrac{1+s}{3}\sigma_X \tag{21}$$

for any $s \in [0, \frac{1}{2}]$. All of these have the same Bloch vector representation namely $m_1 = (1,0,0)$, $m_2 = (\frac{1}{2},0,0)$ and $m_3 = (-1,0,0)$.

[1] if $\mu_i = 0$ it cannot be positive semi-definite unless $A_i = 0$, if $\mu_i < 0$ it cannot be positive semi-definite

For arbitrarily many outcomes, we need special assumptions on a set of Bloch vectors for it to correspond to a unique POVM. Consider the special case, $\sum_{i\in[k]} m_i = 0$ (center of mass in the origin), and there exists $j \in [k]$ such that $\{m_i\}_{i\neq j}$ is linearly independent (the span of $\{m_i\}$ is $k-1$ dimensional). Then since both $0 = \sum_{i\in[k]} \frac{\nu_i}{\mu_i}$ and $0 = \sum_{i\in[k]} \nu_i$ we have

$$0 = \nu_j + \sum_{i\neq j} \frac{\mu_j}{\mu_i}\nu_i = \sum_{i\neq j} \left(\frac{\mu_j}{\mu_i} - 1\right)\nu_i \tag{22}$$

Due to the linear independence of the ν_i's $(i \neq j)$ we have $\mu_1 = ... = \mu_k$. In this case there is a unique POVM associated with the Bloch vectors $\{m_i\}$.

When $k = 2, 3$ we only need the span of the Bloch vectors to be $k-1$ dimensional to have a unique POVM. Since the requirements $\mu_1 m_1 + \mu_2 m_2 + \mu_3 m_3 = 0$ and $\mu_1 + \mu_2 + \mu_3 = 1$ uniquely determines the numbers μ_1, μ_2 and μ_3.

2.3 Geometry of convex sets

In this section we will go through some definitions from convex geometry that are relevant to our further investigations. To this end we follow [HW20, GKW+18] and restrict our focus to the Euclidean framework. We will however slightly modify the usual definition of a supporting hyperplane to a more suitable one in this present work. Let n be a positive integer. A subset $A \subseteq \mathbb{R}^n$ is called *convex* if $\alpha x + (1-\alpha)y \in A$ for any pair $x, y \in A$ and $\alpha \in [0, 1]$.

Let $A \subseteq \mathbb{R}^n$ be non-empty, convex and bounded.

Definition 6. (*Supporting hyperplane*). A hyperplane

$$H := \left\{x \in \mathbb{R}^n | \langle x, g\rangle = c\right\}. \tag{23}$$

with unit normal vector $g \in \mathbb{R}^n$ and a distance of $c \geq 0$ to the origin is called a *supporting hyperplane* of A if $\mathrm{Clos}(A) \cap H \neq \varnothing$ (where $\mathrm{Clos}(A)$ denotes the closure of A) and A is contained in one of the closed half-spaces defined by H.
•

Our definition is different from the one found in most textbooks (see e. g. [HW20]). Usually one starts by assuming A to be closed. This way A can be identified with the intersection of all its supporting half-spaces. Since we do not need such a statement we choose to weaken the notion of a supporting hyperplane.

Define the functional

$$c(g) := \sup_{u\in A} \langle u, g\rangle, \ g \in \mathbb{R}^n, \tag{24}$$

and denote by $\hat{g}$ the normalized vector $g/|g|$ for some non-zero $g \in \mathbb{R}^n$. From the preceding discussion it is clear that

$$H_g := \left\{x \in \mathbb{R}^n | \langle x, \hat{g}\rangle = c(\hat{g})\right\} \tag{25}$$

is a supporting hyperplane.

Figure 4: *Different convex sets: Blue points are non-exposed extreme points, red points are exposed points. Solid lines are the boundary points.*

Definition 7. (*(Proper) exposed face*) The following subset of A,

$$\mathcal{F}_g := \{u \in A | \langle u, \hat{g} \rangle = c(\hat{g})\}. \tag{26}$$

is called the *exposed face of A in direction g*. It is called *proper* if $\mathcal{F}_g \subsetneq A$.
•

Of course, with our definitions an exposed face is empty if the supremum is not attained by an element of A.

Definition 8. (*Boundary points*) A point $x \in A$ is called a *boundary point* if it is contained in a proper exposed face.
•

Definition 9. (*Extreme points and exposed points*). A point $x \in A$ is called an *extreme point* if $x = \alpha y + (1-\alpha)z$ with $y, z \in A$ and $\alpha \in (0,1)$ implies $x = y = z$. The set of extreme points of A is denoted $\mathrm{Ext}(A)$. A point $x \in A$ is called *exposed* if there exists $g \in \mathbb{R}^n$ such that $\mathcal{F}_g = \{x\}$. The set of exposed points is denoted $\mathrm{Exp}(A)$.
•

The difference between exposed points and extreme points is subtle. On the one hand, it is easy to see that exposed points are extreme. On the other hand one might be tempted to think that the opposite is also true. This is however not the case as Figure 4 illustrates: On the left, u_1 is a non-exposed extreme point - there is no exposed face containing only u_1. u_2 is an exposed point: For example, the exposed face in the y direction contains only u_2. The boundary consists of all convex combinations of u_1 and u_2. On the right, u_1 and u_2 are exposed points. All the boundary points between u_3 and u_4 are exposed as well however u_3 and u_4 themselves are non-exposed extreme points. Lastly, we will need the following definition:

Definition 10. (*Convex hull*). Let X be any subset of $\mathbb{R}^n$. The *convex hull* of X, denoted $\mathrm{Conv}[X]$, is defined as

$$\mathrm{Conv}[X] := \left\{ \sum_{i=1}^{k} \alpha_i x_i \;\middle|\; k \in \mathbb{N},\ \sum_{i=1}^{n} \alpha_i = 1,\ \alpha_i \in [0,1],\ x_i \in X \right\}. \tag{27}$$

•

We note that the convex hull of a closed set is closed [HW20]. We will utilize the concepts from this section in our study of different correlation sets in the following sections.

3 Correlation sets

We consider a scenario as the one described in the introduction: Alice and Bob have finite numbers of different measurement settings coming from alphabets, $\mathcal{X}$ and $\mathcal{Y}$ respectively. They also have finite numbers of different outcomes for their measurements coming from alphabets, $\mathcal{A}$ and $\mathcal{B}$. If $m_a := |\mathcal{X}|$, $m_b := |\mathcal{Y}|$, $n_a = |\mathcal{A}|$, $n_b := |\mathcal{B}|$, it is convenient to let $\mathcal{X} = [m_a]$, $\mathcal{Y} = [m_b]$, $\mathcal{X} = [n_a]$ and $\mathcal{Y} = [n_b]$. Define also $M_{abxy} := m_a m_b n_a n_b$. The probability of obtaining outcome combination (a, b) given the measurement combination (x, y) is denoted $p(ab|xy)$.

Definition 11. (*Correlation*). A *correlation* is the collection of measurement statistics

$$\big\{p(ab|xy)|a \in A, b \in \mathcal{B}\big\}_{x\in\mathcal{X},y\in\mathcal{Y}} \tag{28}$$

represented as a vector $p = \big(p(ab|xy)\big) \in \mathbb{R}^{M_{abxy}}$.
•

The term *probability point* will be used synonymously with *correlation*. Sometimes it can be useful to consider the statistics in terms of a m_a-by-m_b block matrix where each block has size n_a-by-n_b,

$$p = \left(\begin{array}{c|c|c} p(ab|x=1,y=1) & \cdots & p(ab|x=1,y=m_b) \\ \hline \vdots & \ddots & \vdots \\ \hline p(ab|x=m_a,y=1) & \cdots & p(ab|x=m_a,y=m_b) \end{array}\right). \tag{29}$$

We have the normalization requirement,

$$\sum_{ab} p(ab|xy) = 1, \quad (\forall x, y). \tag{30}$$

In the matrix picture this means that the sum of the elements of each block is 1. We also have positivity

$$p(ab|xy) \geq 0, \quad (\forall a, b, x, y) \tag{31}$$

Besides these requirements, determining whether a point $p \in \mathbb{R}^{M_{abxy}}$ is realizable depends on the physical model under consideration. In the following we discuss the sets of correlation we will be concerned with in this thesis.

The local set $\mathcal{C}_c$. A probability point is called *deterministic* if the output of each party is a deterministic function of the inputs. We denote this set $\mathcal{C}_{\text{det}}(m_a, m_b, n_a, n_b)$ The *local set*, denoted $\mathcal{C}_c(m_a, m_b, n_a, n_b)$, is defined as the convex hull of $\mathcal{C}_{\text{det}}$ i. e.

$$\mathcal{C}_{\text{c}} := \text{Conv}[\mathcal{C}_{\text{det}}]. \tag{32}$$

This is a polytope since $|\mathcal{L}_{\text{det}}|$ is finite. It is easy to see that $\mathcal{C}_c$ consists of points that can be realized as

$$p(ab|xy) = \sum_{\lambda} p(\lambda) p_A(a|x,\lambda) p_B(b|y,\lambda). \tag{33}$$

Points that are attainable by these restrictions obey a *local hidden variable model* and are often just referred to as *local*.

The quantum sets $\mathcal{C}_q, \mathcal{C}_{qa}, \mathcal{C}_{qs}$ and $\mathcal{C}_{qc}$. A point $P \in \mathbb{R}^{M_{abxy}}$ belongs to the *quantum set*, denoted $\mathcal{C}_q(m_a, m_b, n_a, n_b)$ if there exist finite dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, a state $\varrho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and POVMs $\{A_a^x\}_{a\in\mathcal{A}}$ and $\{B_b^y\}_{b\in\mathcal{B}}$ for each $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ such that

$$p(ab|xy) = \mathrm{Tr}[A_a^x \otimes B_b^y \varrho_{AB}] \quad (\forall a, b, x, y). \tag{34}$$

Let the *quantum approximate set*, denoted $\mathcal{C}_{qa}(m_a, m_b, n_a, n_b)$, be the closure,

$$\mathcal{C}_{qa}(m_a, m_b, n_a, n_b) := \mathrm{Clos}\left(\mathcal{C}_q(m_a, m_b, n_a, n_b)\right). \tag{35}$$

We define $\mathcal{C}_{qs}$ to be the set one gets by weakening the requirement that $\mathcal{H}_A$ and $\mathcal{H}_B$ be finite dimensional to only requiring separability of the Hilbert spaces.

Suppose we, instead of considering tensor product measurements as in (34), let Alice and Bob act on the whole space with the weaker requirement that A_a^x and B_b^y commute for all a, b, x, y. We call the resulting set the *commuting operator set* and denote it $\mathcal{C}_{qc}(m_a, m_b, n_a, n_b)$. A point $p \in \mathbb{R}^{M_{abxy}}$ belongs this set if there exists a separable Hilbert space, $\mathcal{H}$, a state $\varrho \in \mathcal{D}(\mathcal{H})$ and POVMs $\{A_a^x\}_{a\in\mathcal{A}}, \{B_b^y\}_{b\in\mathcal{B}} \subseteq \mathcal{L}(\mathcal{H})$ fulfilling $[A_a^x, B_b^y] = 0$ for all a, b, x, y such that

$$p(ab|xy) = \mathrm{Tr}[A_a^x B_b^y \varrho] \quad \forall (a, b, x, y) \tag{36}$$

In the end of this section we will discuss the inclusive realtions between these different quantum sets. A final set of interest is:

The no-signalling set, $\mathcal{C}_{ns}$: A point $p \in \mathbb{R}^{M_{abxy}}$ belongs to the *no-signalling set* (first proposed by Popescu and Rohrlich [PR94]), denoted $\mathcal{C}_{ns}$ if it satifies

$$\sum_b p(ab|xy) = \sum_b p(ab|xy'), \quad (\forall a, x, y, y') \text{ and} \tag{37}$$

$$\sum_a p(ab|xy) = \sum_a p(ab|x'y), \quad (\forall b, x, x', y) \tag{38}$$

in addition to (30)-(31). Formally (37)-(38) can be viewed as the requirement that the marginals,

$$p(a|x) = \sum_b p(ab|xy) \text{ and} \tag{39}$$

$$p(b|y) = \sum_a p(ab|x'y), \tag{40}$$

are well-defined. It can, however, also be interpreted as the requirement that Alice's local outcome distribution may not depend on Bob's choice of measurement setting and vice versa. In other words, this means that Alice and Bob are forbidden to, in any way, use their black boxes for instantaneous communication. This way, the no-signalling constraint can be viewed as the weakest requirement ensuring no contradiction with relativity. This model is also the weakest in the sense that $\mathcal{C}_t \subsetneq \mathcal{C}_{ns}$ for all $t \in \{c, q, qs, qa, qc\}$. This follows for example from the

fact that nonlocal extreme points of $\mathcal{C}_{ns}$ are not achievable in any quantum model [RTHH16].

If one has a certain correlation in terms of a matrix as in (29), it is easy to check if it obeys the no-signalling condition. For every row of blocks the sum of each row must be constant over all the columns of blocks. Likewise, for every column of blocks each column must be constant over all rows of blocks.

3.1 Convexity and Bell inequalities

We begin this section by noting that all the correlation sets we have introduced are convex: The local and no-signalling sets are both given by a finite number of (in)equality constraints. This implies that they are polytopes and in particular convex. Since the inequalities are not strict they are also closed.

Let $p, q \in \mathcal{C}_q$ and let $(\mathcal{H}_A, \mathcal{H}_B, \varrho_{AB}, \{A_a^x\}, \{B_b^y\})$ and $(\mathcal{H}_{A'}, \mathcal{H}_{B'}, \sigma_{A'B'}, \{P_a^x\}, \{Q_b^y\})$ be realizations of p and q respectively. The goal is to identify a realization of $\tilde{p} := tp + (1-t)q$ for any $t \in (0,1)$. Let $\mathcal{H}_{A''} := \mathcal{H}_A \oplus \mathcal{H}_{A'}$ and $\mathcal{H}_{B''} := \mathcal{H}_B \oplus \mathcal{H}_{B'}$ and consider $(\mathcal{H}_{A''}, \mathcal{H}_{B''}, \tau_{A''B''}, \{E_a^x\}, \{F_b^y\})$ where

$$\tau_{A''B''} := t\varrho_{AB} \oplus (1-t)\sigma_{A'B'} \tag{41}$$

and $E_a^x := A_a^x \oplus P_a^x$ and $F_b^y := B_b^y \oplus Q_b^y$. Since the state is zero on all of $\mathcal{H}_A \otimes \mathcal{H}_{B'} \oplus \mathcal{H}_{A'} \otimes \mathcal{H}_B$ one easily verifies that

$$\tilde{p}(ab|xy) = \mathrm{Tr}[E_a^x \otimes F_b^y \tau_{A''B''}] \quad \forall a, b, x, y. \tag{42}$$

This accounts for the convexity of $\mathcal{C}_q, \mathcal{C}_{qs}, \mathcal{C}_{qa}$. The convexity of $\mathcal{C}_{qc}$ is shown similarly. Note that we used the unboundedness of the dimension to show convexity. In fact, if one works with a bound on the dimension it is possible to show that the set of quantum correlations need not be convex [DW15].

Besides convexity, little is known about the geometries of the different quantum sets. For example, one could ask if $\mathcal{C}_q(m_a, m_b, n_a, n_b)$ is closed. Tsirelson himself proved in 1980 that in the smallest possible case (i. e. $m_a = m_b = n_a = n_b = 2$) we in fact have closure. We give here an alternative proof following [Mas06].

Proposition 12. *$\mathcal{C}_q(2,2,2,2)$ is closed.*

Proof. In [Mas06] it is shown that if A_0, A_1, B_0, B_1 are projectors acting on some Hilbert space, $\mathcal{H}$ and these fulfill $A_0 + A_1 = \mathbb{1}$ and $B_0 + B_1 = \mathbb{1}$ then there exists an orthonormal basis of $\mathcal{H}$ in which all of these are block diagonal in blocks of size at most 2. This means that for any $p \in \mathcal{C}_q$ with realization $(\mathcal{H}_A, \mathcal{H}_B, \varrho_{AB}, \{A_a^x\}, \{B_b^y\})$ we can write

$$A_a^x = \bigoplus_i (A_a^x)_i \text{ and } B_b^y = \bigoplus_i (B_b^y)_i \tag{43}$$

where $(A_a^x)_i$ and $(B_b^y)_i$ are at most 2-by-2 and $(A_0^x)_i + (A_1^x)_i = (B_0^y)_i + (B_1^y)_i = \mathbb{1}_d$ for all i ($d \in \{1,2\}$ $x, y \in \{0,1\}$). We denote the projectors onto these (at most) two-dimensional subspaces $\Pi_A^{(i)}$ and $\Pi_B^{(j)}$ and let $\Pi_{AB}^{ij} := \Pi_A^{(i)} \otimes \Pi_B^{(j)}$. Define the post-measurement state

$$\varrho_{AB}^{ij} := \frac{\Pi_{AB}^{ij} \varrho_{AB} \Pi_{AB}^{ij}}{q_{ij}}, \tag{44}$$

where $q_{ij} := \mathrm{Tr}[\Pi_{AB}^{ij} \varrho_{AB}] \in (0,1]$ so $\sum_{ij} q_{ij} = 1$. Let

$$p_{ij}(ab|xy) = \mathrm{Tr}[(A_a^x)_i \otimes (B_b^y)_j \varrho_{AB}^{ij}]. \tag{45}$$

Then, using

$$(A_a^x)_i \otimes (B_b^y)_j = \Pi_{AB}^{ij} A_a^x \otimes B_b^y \Pi_{AB}^{ij} \tag{46}$$

we get

$$\begin{aligned} p(ab|xy) &= \mathrm{Tr}[A_a^x \otimes B_b^y \varrho_{AB}] && (47)\\ &= \sum_{ij} q_{ij} \mathrm{Tr}[(A_a^x)_i \otimes (B_b^y)_j \varrho_{AB}^{ij}] && (48)\\ &= \sum_{ij} q_{ij} p_{ij}(ab|xy). && (49) \end{aligned}$$

Thus any correlation can be realized as a convex combination of correlations obtained with a restriction to local dimensions of most 2. If we denote this subset by $\mathcal{C}_q^2(2,2,2,2)$ we see from the above computation that

$$\mathcal{C}_q^2(2,2,2,2) \subseteq \mathcal{C}_q(2,2,2,2) \subseteq \mathrm{Conv}\left(\mathcal{C}_q^2(2,2,2,2)\right) \tag{50}$$

Recall that $\mathrm{Conv}(\mathcal{C}_q(2,2,2,2)) = \mathcal{C}_q(2,2,2,2)$. So if we take the convex hull of all the terms in (50) we have

$$\mathcal{C}_q(2,2,2,2) = \mathrm{Conv}\left(\mathcal{C}_q^2(2,2,2,2)\right). \tag{51}$$

To finish, recall that the convex hull of a closed set is still closed. We conclude that $\mathcal{C}_q(2,2,2,2)$ is closed. □

It has recently been established that such a result cannot be generalized to any m_a, m_b, n_a, n_b. We discuss this in the next section.

Correlation set differences is usually studied by considering Bell inequalities. These are linear constraints that must be satisfied in the local model but may be violated in quantum models. More specifically, we define

Definition 13. (*Bell function/functional/inequality*). A *Bell function* is given by a real vector $B = (B_{abxy}) \in \mathbb{R}^{M_{abxy}}$. The value of the Bell functional on a correlation p is the inner product,

$$\langle B, p \rangle := \sum_{abxy} B_{abxy} p(ab|xy) \tag{52}$$

Let B be a Bell function. The functional,

$$\beta_t(B) \coloneqq \sup_{p\in\mathcal{C}_t} \langle B, p\rangle \tag{53}$$

where $t \in \{c, q, qs, qa, qc, ns\}$ is called a *Bell t-functional*. A *Bell inequality* is a pair (B, γ_c) where B is a Bell function and γ_c a real number such that $\beta_c(B) \leq \gamma_c$ •

When we talk about a Bell inequality (B, γ_c) but the bound γ_c is irrelevant in the context, we will only denote it by B. Correlation set differences can be established by finding Bell functions for which $\beta_t(B) < \beta_{t'}(B)$ for $t \neq t'$. Suppose for example that (B, γ_c) is a Bell inequality. It follows directly from hyperplane separation of convex sets that any correlation $\tilde{p}$ for which $\langle B, \tilde{p}\rangle > \gamma_c$ is indeed nonlocal. It should be remarked that in case of non-closure of a correlation $\mathcal{C}_t$ the value $\beta_t(B)$ is of course not attained. Hence establishing a strict set difference between for example, $\mathcal{C}_q$ and $\mathcal{C}_{qa}$ can instead be done by exhibiting a Bell function for which $\langle B, p\rangle < \beta_q(B)$ for all $p \in \mathcal{C}_q$.

A Bell inequality might also be viewed as an m_a-by-m_b block matrix where each block has size n_a-by-n_b,

$$B = \left(\begin{array}{c|c|c} B_{a,b,1,1} & \cdots & B_{a,b,1,m_b} \\ \hline \vdots & \ddots & \vdots \\ \hline B_{a,b,m_a,1} & \cdots & B_{a,b,m_a,m_b} \end{array}\right), \tag{54}$$

in a similar fashion as we saw for the correlations in (29). In this case we have

$$\beta_t(B) \coloneqq \sup_{p\in\mathcal{S}} \mathrm{Tr}[Bp^T]. \tag{55}$$

We will see several examples of Bell inequalities later.

3.2 Tsirelson's problem

In the preceding subsection we saw that $\mathcal{C}_q(2, 2, 2, 2)$ is closed. This is, as will become apparent in this subsection, not true for the general set, $\mathcal{C}_q(m_a, m_b, n_a, n_b)$. We will here discuss inclusive relations between the different correlation sets defined above.

John Bell's celebrated theorem states that $\mathcal{C}_c \neq \mathcal{C}_q$. One can easily see that $\mathcal{C}_t \subseteq \mathcal{C}_{qc}$ for all $t \in \{q, qs, qa\}$ by noting that $[A_a^x \otimes \mathbb{1}_B, \mathbb{1}_A \otimes B_b^y] = 0$. It was proved by Sholz and Werner [SW08] that $\mathcal{C}_{qs}$ is contained in $\mathcal{C}_{qa}$. We focus therefore on the following hierarchy of inclusions,

$$\mathcal{C}_q \subseteq \mathcal{C}_{qs} \subseteq \mathcal{C}_{qa} \subseteq \mathcal{C}_{qc}. \tag{56}$$

Whether $\mathcal{C}_{qc}$ coincides with one of either $\mathcal{C}_q$, $\mathcal{C}_{qs}$ or $\mathcal{C}_{qa}$ is known as Tsirelson's problem. This problem has an interesting history which we will briefly sketch in

the following:

Tsirelson originally stated the problem in 1993 in [Tsi93] in which he also proved that in the finite dimensional case, the inclusions coincide. Moreover he wrongly claimed, that they also coincide in the infinite dimensional case. Since this was stated without proof a rigorous proof was requested by A. Acín in 2006. Tsirelson, unable to prove his claim, posted it as a problem on the *Braunschweig website on open problems in quantum information theory* [Tsi06a]. The problem remained open until its final resolution in 2021 [JNV+21].

Leading up to this final resolution were Slofstra's breakthroughs in 2019: [Slo19b], in which he shows strict separation between $\mathcal{C}_{qs}$ and $\mathcal{C}_{qc}$. Later the same year he established strict separation between $\mathcal{C}_{qs}$ and $\mathcal{C}_{qa}$ [Slo19a]. More precisely he established $\mathcal{C}_q(184, 235, 8, 2) \neq \mathcal{C}_{qa}(184, 235, 8, 2)$. The latter, has become a landmark result since it implies the nonclosure of the quantum set $\mathcal{C}_q$. Since Slofstra's original proof, simpler proofs of nonclosure have been obtained in [DPP19, Col20]. In particular, in [DPP19] they find that $\mathcal{C}_q(5, 5, 2, 2) \neq \mathcal{C}_{qa}(5, 5, 2, 2)$. Furthermore, Coladangelo and Stark showed strict separation between $\mathcal{C}_q$ and $\mathcal{C}_{qs}$ in [CS20]. The establishment of strict separations $\mathcal{C}_q \subsetneq \mathcal{C}_{qs} \subsetneq \mathcal{C}_{qa}$ does not, however, solve Tsirelson's problem. What remained to show was whether or not $\mathcal{C}_{qa}$ and $\mathcal{C}_{qc}$ coincide.

As stated before, the last step was solved in [JNV+21] in the negative by establishing the complexity theoretical result MIP* = RE. Drawing upon the proof of this, a nonlocal game with the property that it can be won perfectly with a strategy from $\mathcal{C}_{qc}$ but with a probability strictly smaller than one with any strategy coming from $\mathcal{C}_{qa}$ was exhibited.

A surprising link to Connes' embedding theorem: In [Oza13] Ozawa shows that Tsirelson's problem is in fact equivalent with a problem from C^* algebras, known as the QWEP problem, put forth in Kirchberg's seminal work [Kir93]. There Kirchberg shows, that the QWEP problem in fact is equivalent with the long standing Connes' embedding problem in the theory of tracial von Neumann algebras [Con76]. Thus, MIP* = RE provided a negative solution to Tsirelson's problem, thereby a negative solution to the QWEP problem and finally a negative solution of Connes' embedding problem.

4 Definition of self testing

In this section we give formal definitions of self testing. We follow the majority of the literature on the subject (see e. g. [GKW+18, MPS21, ŠB20]). First we define, what we mean by a *realization*

Definition 14. (*Realization of* $p \in C_q, \mathcal{C}_{qs}, \mathcal{C}_{qc}$). Let $p \in \mathcal{C}_q, \mathcal{C}_{qs}$. A *realization* of p

is given by a tuple,

$$(\mathcal{H}_A, \mathcal{H}_B, \varrho_{AB}, \{A_a^x\}, \{B_b^y\}), \tag{57}$$

where $\mathcal{H}_A$ and $\mathcal{H}_B$ are Hilbert spaces (finite dimensional if $p \in \mathcal{C}_q$), ϱ_{AB} is a state on $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\{A_a^x\}, \{B_b^y\}$ are POVMs such that

$$p(ab|xy) = \mathrm{Tr}[A_a^x \otimes B_b^y \varrho_{AB}] \quad \forall a, b, x, y. \tag{58}$$

Let $p \in \mathcal{C}_{qc}$. A *realization* of p is given by a tuple,

$$(\mathcal{H}, \varrho_{AB}, \{A_a^x\}, \{B_b^y\}), \tag{59}$$

where $\mathcal{H}$ is a Hilbert space, ϱ is a state on $\mathcal{H}$ and $\{A_a^x\}, \{B_b^y\}$ are POVMs such that for all a, b, x, y

$$[A_a^x, B_b^y]_- = 0 \text{ and } p(ab|xy) = \mathrm{Tr}[A_a^x B_b^y \varrho_{AB}]. \tag{60}$$

•

In the following discussion we focus on a correlation $p \in \mathcal{C}_q$. Given a realization as in (57) there are at least the following two ways of which we can change the realization without changing the correlation,

(i) Let $U_A \in \mathcal{L}(\mathcal{H}_A)$ and $U_B \in \mathcal{L}(\mathcal{H}_B)$ be unitaries and let $U := U_A \otimes U_B$ and $\tilde{p}$ be the correlation one gets when using $UA_a^x \otimes B_b^y U^\dagger$ on $U\varrho_{AB}U^\dagger$. By the cyclicity of the trace function we clearly have $\tilde{p} = p$. In other words, we will not be able to deduce whether our system in fact consists of state $U\varrho_{AB}U^\dagger$ and POVMs $\{U_A A_a^x U_A^\dagger\}$ and $\{U_B B_b^y U_B^\dagger\}$.

(ii) One could consider additional degrees of freedom on which the POVMs act trivially. That is, let $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ be finite dimensional Hilbert spaces, and consider the correlation, p', produced by POVMs $\{A_a^x \otimes \mathbb{1}_{A'}\}$ and $\{B_a^x \otimes \mathbb{1}_{B'}\}$ and state $\varrho_{AB} \otimes \sigma_{A'B'}$ for some $\sigma_{A'B'} \in \mathcal{D}(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$. Again one easily finds that $p' = p$, and it is thus impossible to tell whether our system in fact consists of state $\varrho_{AB} \otimes \sigma_{A'B'}$ and POVMs $\{A_a^x \otimes \mathbb{1}_{A'}\}$ and $\{B_a^x \otimes \mathbb{1}_{B'}\}$.

4.1 Exact self testing

Based on these considerations one could ask if, given two realizations, it is possible to extract one of them from the other one using only operations similar to those listed above i. e. local changes of bases and additional degrees of freedom. This question is what self testing tries to answer.

It turns out to be useful to state the self testing conditions at the level of ket-notation. This requires the introduction of a purification space, $\mathcal{H}_P$, for the state ϱ_{AB} as in (57). Let $|\psi\rangle_{ABP}$ be a purification of ϱ_{AB}. With inspiration from [MNP21, MPS21] we make the following definition,

Definition 15. (*Local dilation*). Let $r, p \in \mathcal{C}_q$ and consider two realizations

$$\mathcal{R}_r := (\mathcal{H}_A, \mathcal{H}_B, \varrho_{AB}, \{A_a^x\}, \{B_b^y\}) \text{ and } \mathcal{R}_p := (\mathcal{H}_{A'}, \mathcal{H}_{B'}, |\varphi\rangle_{A'B'}, \{P_a^x\}, \{Q_b^y\}) \quad (61)$$

We say that $\mathcal{R}_p$ is a *local dilation of* $\mathcal{R}_r$, denoted $\mathcal{R}_r \hookrightarrow \mathcal{R}_p$, if for any purification $|\psi\rangle_{ABP}$ of ϱ_{AB} there exist

(i) Finite dimensional Hilbert spaces $\mathcal{H}_{A''}$ and $\mathcal{H}_{B''}$,

(ii) an auxiliary state, $|\xi\rangle_{A''B''P} \in \mathcal{H}_{A'',B''P}$ and

(iii) isometries $V_A : \mathcal{H}_A \to \mathcal{H}_{A',A''}$ and $V_B : \mathcal{H}_B \to \mathcal{H}_{B',B''}$

such that with $V := V_A \otimes V_B$,

$$V \otimes \mathbb{1}_P \left[A_a^x \otimes B_b^y \otimes \mathbb{1}_P |\psi\rangle_{ABP} \right] = \left[P_a^x \otimes Q_b^y |\varphi\rangle_{A'B'} \right] \otimes |\xi\rangle_{A''B''P} \quad (62)$$

for all a, b, x, y.
•

We stress the importance that the isometries do not act on the purification space. If we allowed this we could get access to entanglement for free if the physical state ϱ_{AB} is mixed and separable. We remark also that our notion of local dilation from a realization, $\mathcal{R}_r$ to another $\mathcal{R}_p$ only makes sense if $\mathcal{R}_p$ is given by a pure state. This poses no additional limitations since, as argued in the introduction, one can only hope to self test pure states.

It is convenient to define a *canonical realization* of $p \in \mathcal{C}_q$. By appropriately introducing Naimark dilations and a purification space for the state, p can be realized using projective measurement, $\{P_a^x\}$ and $\{Q_b^y\}$ and a pure state $|\Psi\rangle_{A'B'}$. Moreover, the realization can be embedded into local Hilbert spaces with dimensions equal to the rank of the reduced operators, $\varrho_{A'} = \mathrm{Tr}_{B'}[|\Psi\rangle\langle\Psi|]$ and $\varrho_B = \mathrm{Tr}_{A'}[|\Psi\rangle\langle\Psi|]$. In this way these are ensured to be full rank. A realization with such properties will be called a *canonical realization* and henceforth be denoted,

$$\tilde{\mathcal{R}}_p := (\mathcal{H}_{A'}, \mathcal{H}_{B'}, |\Psi\rangle_{A'B'}, \{P_a^x\}, \{Q_b^y\}). \quad (63)$$

Note, that canonical realizations are not unique. When we talk about *the* canonical realization we simply mean some chosen realization with the aforementioned properties. On the other hand, we imagine our physical system described by *some* realization of p consisting of a (possibly mixed) state ϱ_{AB} acting on $\mathcal{H}_{A,B}$ and measurements $\{A_a^x\}$ and $\{B_b^y\}$. This we call the *physical realization* and we will denote it

$$\mathcal{R}_p := (\mathcal{H}_A, \mathcal{H}_B, \varrho_{AB}, \{A_a^x\}, \{B_b^y\}). \quad (64)$$

It is important to remark, that we will make the assumption that the physical measurements are in fact projective. One way of justifying this is by arguing that the fundamental operations in quantum theory are projective measurements and

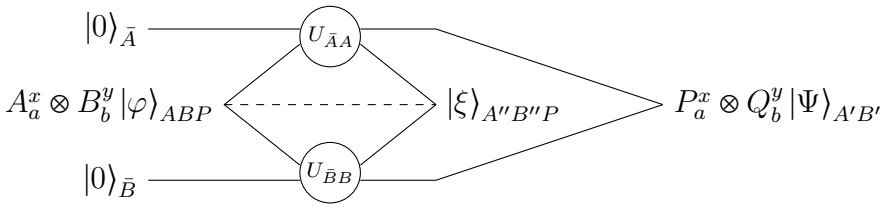


Figure 5: *Quantum circuit diagram illustrating local dilation. Consists of ancilla spaces and local unitaries capable of extracting canonical realization. The dashed line corresponds to the purification space which is unaffected by the unitaries.*

unitary evolution [ŠB20]. Thus, a POVM can only be realized through projective measurements on a dilated space.

The absence of the projectivity-assumption poses a problem in the following way. As pointed out in [ŠB20] many of the proof strategies in self testing statements explicitly require that the physical measurements be projective. Assuming for example Alice's physical measurements, $\{A_a^x\}$, to be POVMs, one might be tempted to simply introduce a map Ω that takes her measurement to its Naimark dilation, i. e.

$$\Omega[A_a^x \otimes \mathbb{1}_{BP} |\psi\rangle_{ABP}] = \tilde{A}_a^x \otimes \mathbb{1}_{BP} |\psi\rangle_{ABP} |0\rangle_{\tilde{A}} \tag{65}$$

where $\{\tilde{A}_a^x\}$ is projective. Suppose then, we have succeeded in proving a formal self testing statement based on the projectivity-assumption. That is, we have constructed local isometries V_A and V_B with all the desired properties. Could we then concatenate V and Ω to perhaps circumvent the problem? Unfortunately not. Let $a \neq a'$ and consider the inner product of the RHS of (65) with itself,

$$\langle\psi|_{ABP} \langle 0|_{\tilde{A}} \tilde{A}_a^x \tilde{A}_{a'}^x \otimes \mathbb{1}_{BP} |\psi\rangle_{ABP} |0\rangle_{\tilde{A}} . \tag{66}$$

Due to projectivity of $\{\tilde{A}_a^x\}$ this vanishes. However, the inner product of argument of Ω on the LHS of (65) does not vanish since $\{A_a^x\}$ is not projective. Hence, Ω is not an isometry. In spite of these concerns we now state the formal definition of self testing.

Definition 16. *(Exact self testing).* A correlation $p \in \mathcal{Q}_q$ *self tests* its canonical realization $\tilde{\mathcal{R}}_p$ if for any physical realization, $\mathcal{R}_p$, we have $\mathcal{R}_p \hookrightarrow \tilde{\mathcal{R}}_p$
•

An isometry can be recast as a unitary by appropriately adding ancillas. In this way, we can illustrate a local dilation as a quantum circuit diagram. Figure 5 illustrates the extraction of the canonical realization using isometries V_A and V_B as in the definition above. These are transformed into unitaries, $U_{\bar{A},A} : \mathcal{H}_{\bar{A},A} \to \mathcal{H}_{A'',A'}$ and $U_{\bar{B},B} : \mathcal{H}_{\bar{B},B} \to \mathcal{H}_{B'',B'}$ by using ancilla spaces $\mathcal{H}_{\bar{A}}$ and $\mathcal{H}_{\bar{B}}$ initiated in $|00\rangle_{\bar{A}\bar{B}}$.

Oftentimes in the literature, existence of a local dilation is simply called equivalence. This terminology is a bit misleading, as pointed out in [MPS21], since local

dilation is not an equivalence relation. When, in the rest of this thesis, we talk about equivalence in the context of self testing we really mean the existence of a local dilation.

We wish to be able to make sense of talking about self testing states and measurements individually. We show how one could do so in the following. For brevity, we let juxtaposition mean tensor product. Also, we omit tensoring with unity whenever an operator acts trivially on a subspace. Notice that if we sum over index a in (62) we get,

$$V\left[B_b^y \left|\psi\right\rangle_{ABP}\right] = \left[Q_b^y \left|\Psi\right\rangle_{A'B'}\right] \left|\xi\right\rangle_{A''B''P}, \quad \forall b, y \tag{67}$$

by using completeness of Alice's measurements. Similarly

$$V\left[A_a^x \left|\psi\right\rangle_{ABP}\right] = \left[P_a^x \left|\Psi\right\rangle_{A'B'}\right] \left|\xi\right\rangle_{A''B''P}, \quad \forall a, x \tag{68}$$

by summing over index b. Summing over both indices yields

$$V\left[\left|\psi\right\rangle_{ABP}\right] = \left|\Psi\right\rangle_{A'B'} \left|\xi\right\rangle_{A''B''P} \tag{69}$$

Since (67)-(69), do not individually imply self testing, we make the following weakened notions of self testing states and measurements alone.

Definition 17. *(Self testing of states).* If only (69) holds we say that $p \in \mathcal{Q}_q$ *self tests the state* $\left|\Psi\right\rangle_{A'B'}$.
•

As noted in [Kan17], any meaningful self testing statement about the measurement operators of either Alice or Bob can only be made on the support of their respective marginal states. Let us demonstrate how this works.

Inserting (69) in (68) gives

$$V\left[A_a^x \left|\psi\right\rangle_{ABP}\right] = P_a^x V[\left|\psi\right\rangle_{ABP}], \quad \forall a, x. \tag{70}$$

In (70) we are considering vectors with components in all the registers A', B', A'', B'' and P. If we trace out the registers B', B'' and P we obtain

$$V_A A_a^x \varrho_A = P_a^x V_A \varrho_A, \quad \forall a, x. \tag{71}$$

where $\varrho_A = \mathrm{Tr}_{BP}[\left|\psi\right\rangle\left\langle\psi\right|_{ABP}]$. Inserting unity as $V_A^\dagger V_A$, right multiplying by $V_A^\dagger$, taking everything to the LHS and factorizing gives

$$\left[V_A A_a^x V_A^\dagger - P_a^x \otimes \mathbb{1}_{A''}\right] V_A \varrho_A V_A^\dagger = 0, \quad \forall a, x. \tag{72}$$

re-adopting the tensor product. We see therefore that restricted to the support of $V_A \varrho_A V_A^\dagger$ we have the relation $V_A A_a^x V_A^\dagger = P_a^x \otimes \mathbb{1}_{A''}$. This observation motivates the following definition,

Definition 18. *(Self testing measurements).* The correlation $p \in \mathcal{C}_q$ *self tests the measurements* $\{P_a^x\}$ *and* $\{Q_b^y\}$ if for any measurements $\{A_a^x\}$ and $\{B_b^y\}$ and state ϱ_{AB} compatible with p there exist isometries V_A and V_B (as before) such that with $V \coloneqq V_A \otimes V_B$ we have

$$V_A A_a^x V_A^\dagger = P_a^x \otimes \mathbb{1}_{A''} \text{ on support of } V_A \varrho_A V_A^\dagger \tag{73}$$

$$V_B B_b^y V_B^\dagger = Q_b^y \otimes \mathbb{1}_{B''} \text{ on support of } V_B \varrho_B V_B^\dagger \tag{74}$$

for all a, b, x, y
•

If it is possible to make a full self testing statement for a correlation $p \in \mathcal{C}_q$ we sometimes call p a *self test*. It turns out, as shown in [GKW+18] that we have

Theorem 19. *If $p \in \mathcal{C}_q$ is a self test it is an extreme point of $\mathcal{C}_q$.*

Whether the inclusion is strict was resolved later in [TFR+21] where the authors exhibit a Bell inequality with maximal violation in a unique correlation which turns out to have different inequivalent realizations. In this thesis we review the proof of this, however we contribute with a nonself testing nonlocal game whose winning probability is maximized by a unique correlation.

4.2 Robustness

In experimental contexts it is impossible to achieve a correlation exactly. It is therefore clear that in order to make self testing results testable in reality they need to be robust to noise. In this subsection we will make noise-robust variants of the exact self testing conditions in the preceding section. The aim is to be able to prove that if the correlation obtained from experiment is sufficiently close to an ideal correlation, then the physical state and measurements are close (in a well-defined way) to the ideal state and measurements.

Again, with inspiration from [MPS21] we can adjust the definition of local dilation to make the following definition

Definition 20. (*Local ε-dilation*). Let $\varepsilon \geq 0$, $p, r \in \mathcal{C}_q$ and $\mathcal{R}_p$ and $\mathcal{R}_r$ be realizations

$$\mathcal{R}_p \coloneqq (\mathcal{H}_A, \mathcal{H}_B, \varrho_{AB}, \{A_a^x\}, \{B_b^y\}) \text{ and } \mathcal{R}_r \coloneqq (\mathcal{H}_{A'}, \mathcal{H}_{B'}, |\varphi\rangle_{A'B'}, \{P_a^x\}, \{Q_b^y\}). \tag{75}$$

We say that $\mathcal{R}_p$ is a *local ε-dilation of* $\mathcal{R}_r$, denoted $\mathcal{R}_r \overset{\varepsilon}{\hookrightarrow} \mathcal{R}_p$ if for any purification $|\psi\rangle_{ABP}$ of ϱ_{AB} there exist

(i) Finite dimensional Hilbert spaces $\mathcal{H}_{A''}$ and $\mathcal{H}_{B''}$,

(ii) an auxiliary state, $|\xi\rangle_{A''B''P} \in \mathcal{H}_{A'',B''P}$ and

(iii) isometries $V_A : \mathcal{H}_A \to \mathcal{H}_{A',A''}$ and $V_B : \mathcal{H}_B \to \mathcal{H}_{B',B''}$

such that with $V \coloneqq V_A \otimes V_B$,

$$\left\| V \otimes \mathbb{1}_P \left[A_a^x \otimes B_b^y \otimes \mathbb{1}_P \left| \psi \right\rangle_{ABP} \right] - \left[P_a^x \otimes Q_b^y \left| \varphi \right\rangle_{A'B'} \right] \otimes \left| \xi \right\rangle_{A''B''P} \right\|_1 \leq \varepsilon \tag{76}$$

for all a, b, x, y.
•

With this at hand, we can make the following definition of robust self testing,

Definition 21. *(Robust self testing).* A correlation $p \in \mathcal{Q}_q$ *robustly self tests* its canonical realization $\tilde{\mathcal{R}}_p$ if

(i) p self test $\tilde{\mathcal{R}}_p$ and

(ii) for each $\varepsilon \geq 0$ there exists $\delta \geq 0$ such that for any $r \in \mathcal{C}_q$ with $\|r - p\|_1 \leq \delta$ and any realization $\mathcal{R}_r$ we have $\mathcal{R}_r \overset{\varepsilon}{\hookrightarrow} \tilde{\mathcal{R}}_p$.

•

In the above definition we think of ε as the desired closeness to the canonical realization and for every such ε, we can identify δ such that whenever the physically produced correlation is δ-close to the canonical correlation the physical state and measurements are ε-close to the canonical ones. Robust self testing statements usually come with an explicit ε dependence of δ, i. e. $f(\varepsilon) = \delta$.

When discussing self testing in the context of Bell inequalities or nonlocal games the definitions have to be slightly modified. We will see this in the next section.

5 Nonlocal games

As explained in the introduction, a non local game involves three parties, two cooperating, non-communicating players - Alice and Bob - and a *referee*. The referee asks Alice and Bob questions from the sets $\mathcal{X}$ and $\mathcal{Y}$ respectively, according to some probability distribution. Alice and Bob answer with elements from the sets $\mathcal{A}$ and $\mathcal{B}$, respectively.

The rules of game are given by a *verification function* which is known to all parties. The verification function depends on the questions and answers and takes values in $\{0, 1\}$. If it is equal 0, Alice and Bob *lose*. If it is equal to 1, they *win*. This preliminary description suggests the following formal definition,

Definition 22. (Nonlocal game) A *nonlocal game* is a tuple $\mathcal{G} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \pi, V)$ where $\mathcal{X}$, $\mathcal{Y}$ are finite sets called *question sets* and $\mathcal{A}$ and $\mathcal{B}$ are finite sets called *answer sets*. V is a map $V : \mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y} \longrightarrow \{0, 1\}$ called the *verification function*. The probability of getting question pair (x, y) is determined by $\pi : \mathcal{X} \times \mathcal{Y} \longrightarrow [0, 1]$ which will be referred to as the *prior* of the game.
•

After the game has started no communication is allowed between Alice and Bob. But before starting they are allowed to make a *strategy*. We define a strategy to simply be a correlation, p. We refer to the strategy as a *t-strategy* where $t \in \{c, q, qs, qa, qc, ns\}$, depending on the smallest of these correlation sets that p belongs to. This makes sense because all the correlation sets are convex and for convex sets we have hyperplane separation.

A strategy $p = (p(ab|xy))$ results in a *winning probability* which is given by,

$$\omega(\mathcal{G}) := \sum_{x,y} \pi(x,y) \sum_{ab} V(a,b,x,y) p(ab|xy). \tag{77}$$

It follows now from the discussion in Sec. 3 that the *optimal* winning probability Alice and Bob have for $\mathcal{G}$ may depend on the physical resources available to them. We denote the optimal winning probability for t-strategies, $\omega_t^*(\mathcal{G})$. We will often refer to this as the *t-game value*. It is convenient to define the *loosing* probability of some strategy as well, $\bar{\omega}(\mathcal{G}) := 1 - \omega(\mathcal{G})$, and the difference

$$\Delta(\mathcal{G}) := \omega(\mathcal{G}) - \bar{\omega}(\mathcal{G}). \tag{78}$$

5.1 Self testing Bell inequalities

Given a nonlocal game, $\mathcal{G}$, it is easy to see that it has a corresponding Bell function given by,

$$B_{\mathcal{G}} = \left(\pi(x,y) V(a,b,x,y)\right). \tag{79}$$

However, since the verification function only takes values in $\{0,1\}$ not every Bell inequality can be transformed into a nonlocal game. As noted in [Col20], by replacing the verification function with a *score* function taking values in all of $\mathbb{R}$ in the definition of a nonlocal game, we would obtain equivalence with the definition of a Bell inequality.

Since any nonlocal game can be viewed as a Bell function, we will keep the following discussion at the level of Bell inequalities. The notion of self testing as presented in section 4 can only in part be inherited: When we talk about a *self testing a Bell inequality*, B, we mean that, observing the maximal violation, $B_q := \max_{p \in \mathcal{C}_q} \langle B, p \rangle$ (assuming the supremum is attained) allows for a full device independent description in the same way as for self testing correlations. In particular, one can define a realization of some value, c, of the functional $\langle B, \cdot \rangle$ as a realization of $p \in \mathcal{C}_q$ for which $c = \langle B, p \rangle$. Suppose therefore in the following that B is some Bell inequality for which the supremum is attained within $\mathcal{C}_q$ and let $B_q := \max_{p \in \mathcal{C}_q} \langle B, p \rangle$.

Definition 23. (*Self testing of Bell inequality*). A Bell inequality B, self tests its canonical realization of maximal violation, B_q,

$$\tilde{\mathcal{R}}\left(B_q\right) := \left(\mathcal{H}_{A'}, \mathcal{H}_{B'}, |\Psi\rangle_{A'B'}, \{P_a^x\}, \{Q_b^y\}\right) \tag{80}$$

if for any physical realization B_q,

$$\mathcal{R}\left(B_q\right) \coloneqq \left(\mathcal{H}_A, \mathcal{H}_B, \varrho_{AB}, \{A_a^x\}, \{B_b^y\}\right), \tag{81}$$

we have that $\mathcal{R}\left(B_q\right) \hookrightarrow \tilde{\mathcal{R}}\left(B_q\right)$.
•

Since all self testing correlations are extreme points, we know that if a Bell inequality, B, turns out to be a self test, its maximal violation B_q must in fact be reached by a unique correlation. One way to see this, is to assume that two distinct correlations p and $\tilde{p}$ both induce B_q. Due to the linearity of Bell functions any convex combination of p and $\tilde{p}$ also induces B_q. A non-trivial convex combination of $sp + (1-s)\tilde{p}$ for $s \in (0,1)$ is by definition not an extreme point and hence not a self testing correlation according to Theorem 19. This means there exist inequivalent realizations of $sp + (1-s)\tilde{p}$ and hence inequivalent realizations of B_q.

This observation implies a subtle difference between self testing correlations and Bell inequalities which is most easily explained by considering a generic two-section of the quantum correlation set and a Bell function, B, as in Figure 6.

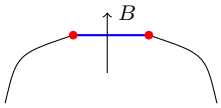


Figure 6: *Generic two-section of quantum correlation set. The winning probability is optimal along the blue line segment and in the red points which are extreme points. $\mathcal{G}$ is not a self test but the red points could possibly be.*

The Bell inequality given by B cannot be a self test due to the discussion above. However, the red points may still be self tests in the sense of Sec. 4. In fact such examples exist. We will discuss this further in Sec. 5.6. We may likewise define robust self testing Bell inequalities as

Definition 24. (*Robust self testing of Bell inequality*). A Bell inequality, B, robustly self tests its canonical realization, $\tilde{\mathcal{R}}(B_q)$, of its maximal violation, B_q, if it self tests its canonical realization of its maximal violation and for any $\varepsilon \geq 0$ there exists $\delta \geq 0$ such that for any realization $\mathcal{R}(B_q - \delta)$ of $B_q - \delta$ we have $\mathcal{R}(B_q - \delta) \overset{\varepsilon}{\hookrightarrow} \tilde{\mathcal{R}}(B_q)$.

5.2 The CHSH game

The CHSH game $\mathcal{G}_{\text{CHSH}}$ is named after Clauser, Horne, Shimony and Holt [CHSH69] who first proposed it as a realizable experiment to show Bell nonlocality. It is given by

$$\mathcal{G}_{\text{CHSH}} \coloneqq \left\{\mathcal{X} = \{0,1\}, \mathcal{Y} = \{0,1\}, \mathcal{A} = \{0,1\}, \mathcal{B} = \{0,1\}, \pi_{\text{CHSH}} = \tfrac{1}{4}, V_{\text{CHSH}}\right\} \tag{82}$$

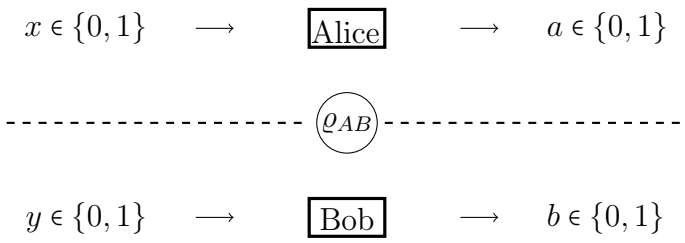


Figure 7: *The CHSH game.*

where the verification function is defined as

$$V_{\text{CHSH}}(a,b,x,y) = \begin{cases} 1 \text{ if } xy + a + b = 0 \mod 2 \\ 0 \text{ otherwise.} \end{cases} \tag{83}$$

In words, if the questions are $(0,0),(0,1)$ or $(1,0)$ Alice and Bob win if they output the same bit. Only if they get the question pair $(1,1)$ should they answer with different bits. We have therefore

$$\Delta_t(\mathcal{G}_{\text{CHSH}}) = \tfrac{1}{4} \sum_{abxy} (-1)^{xy+a+b} p(ab|xy) \tag{84}$$

The CHSH game is one of the most famous nonlocal games due to its simplicity - it involves the minimum of two questions and answers for both Bob and Alice. Moreover, it shows strict separations between the local set and any of the quantum sets as well as between any of the quantum sets and the no-signalling set as we will see below.

Theorem 25. *We have*

$$\omega_c^*(\mathcal{G}_{CHSH}) = \tfrac{3}{4},\ \omega_t^*(\mathcal{G}_{CHSH}) = \tfrac{1}{2} + \tfrac{1}{2\sqrt{2}} \text{ and } \omega_{ns}^*(\mathcal{G}_{CHSH}) = 1 \tag{85}$$

for all $t \in \{q, qs, qa, qc\}$.

Proof. We will first derive an upper bound on $\omega_{qc}^*(\mathcal{G}_{\text{CHSH}})$. Let Alice and Bob hold the measurements $\{A_a^x\}$, $\{B_b^y\}$ fulfilling $[A_a^x, B_b^y]_- = 0$ for all a,b,x,y. Suppose Alice and Bob share the state ϱ_{AB}. Let us define the binary observables

$$A_x := A_0^x - A_1^x \text{ and } B_y := B_0^y - B_1^y. \tag{86}$$

By carrying out the sum in (84) one readily finds,

$$\Delta_{qc}(\mathcal{G}_{\text{CHSH}}) = \tfrac{1}{4}\text{Tr}[(A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1)\varrho_{AB}]. \tag{87}$$

It is convenient to define

$$\mathfrak{B}_{\text{CHSH}} := A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 \tag{88}$$

so we have $\Delta_{qc}(\mathcal{G}_{\text{CHSH}}) \leq \frac{1}{4}\|\mathfrak{B}_{\text{CHSH}}\|_\infty$. Note that by assumption we have projective measurements so the observables A_x, B_y square to the identity. By squaring the operator inside the norm one finds by standard calculations that

$$\mathfrak{B}^2_{\text{CHSH}} = 4\mathbb{1} - [A_0, A_1]_- \otimes [B_0, B_1]_-. \tag{89}$$

The triangle inequality can be used first to get $\|[A_0, A_1]_-\|_\infty, \|[B_0, B_1]_-\|_\infty \leq 2$ after which one has $\|\mathfrak{B}^2_{\text{CHSH}}\|_\infty \leq 8$ and finally $\|\mathfrak{B}_{\text{CHSH}}\|_\infty \leq 2\sqrt{2}$ using Hermiticity of $\mathfrak{B}_{\text{CHSH}}$ and the C^*-identity $\|\mathfrak{B}^2_{\text{CHSH}}\|_\infty = \|\mathfrak{B}_{\text{CHSH}}\|^2_\infty$. Therefore,

$$\Delta_{qc}(\mathcal{G}_{\text{CHSH}}) \leq \tfrac{\sqrt{2}}{2} \tag{90}$$

and hence

$$\omega_{qc}(\mathcal{G}_{\text{CHSH}}) = \tfrac{1}{2} + \tfrac{1}{2}\Delta_{qc}(\mathcal{G}_{\text{CHSH}}) \leq \tfrac{1}{2} + \tfrac{1}{2\sqrt{2}} \tag{91}$$

In the local model, the observables commute so $\mathfrak{B}_{\text{CHSH}} = 4\mathbb{1}$. We get

$$\omega_c(\mathcal{G}_{\text{CHSH}}) \leq \tfrac{1}{2} + \tfrac{1}{2}\Delta_c(\mathcal{G}_{\text{CHSH}}) \leq \tfrac{3}{4} \tag{92}$$

We will now show that these bounds are tight. In the quantum case it suffices to consider tensor product strategies where $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$ and Alice and Bob's shared state is an EPR pair, Φ, upon which they use the observables,

$$A_0 = \sigma_Z,\ A_1 = \sigma_X,\ B_0 = \tfrac{1}{\sqrt{2}}(\sigma_Z + \sigma_X),\ B_1 = \tfrac{1}{\sqrt{2}}(\sigma_Z - \sigma_X). \tag{93}$$

By insertion in (87) one finds a saturation of the upper bound in (90). With this we see that $\omega^*_q(\mathcal{G}_{\text{CHSH}}) = \omega^*_{qc}(\mathcal{G}_{\text{CHSH}})$. In the classical case consider the deterministic strategy given by $p(00|xy) = 1$ for all x, y. Using this in (84) yields the a saturation of the bound 3/4. In the no-signalling case consider the correlation given by the matrix

$$p_{ns} = \tfrac{1}{2}\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right) \tag{94}$$

Since, as noted earlier it suffices to check that for every row of blocks the sum of each row is constant over all the columns of blocks and for every column of blocks, each column must be constant over all rows of blocks. This is indeed the case for (94). One can check that this gives a winning probability of one which concludes the proof.

□

We see that any quantum strategy achieving the quantum game value must consist of anti-commuting measurement operators. After introducing sum of squares (SOS) decompositions as a valuable technical tool we will prove a formal self testing statement for the CHSH game.

5.3 Sum of squares (SOS) decomposition

Let $B = (B_{abxy})$ be a Bell function giving rise to a Bell inequality. Its corresponsding *Bell operator* is defined as

$$\mathfrak{B} := \sum_{abxy} B_{abxy} A_a^x \otimes B_b^y. \tag{95}$$

Note that we could also have chosen to work in the quantum commutation model. Then the tensor product would be replaced by a usual operator composition. In this notation the winning probability is obtained as $\mathrm{Tr}[\mathfrak{B}\varrho_{AB}]$. Suppose the maximal violation of some Bell inequality is β_q. We define the *shifted Bell operator* as $\beta_q \mathbb{1} - \mathfrak{B}$. Note that this is indeed a positive semi-definite operator.

Assume one can find a set of polynomials $\{P_\lambda\}$ in A_a^x and B_b^y such that

$$\beta_q \mathbb{1} - \mathfrak{B} = \sum_\lambda P_\lambda^\dagger P_\lambda. \tag{96}$$

Whenever this is the case we say that the shifted Bell operator admits a sum of squares decomposition. Useful information about a realization achieving the maximal violation can be extracted from such a decomposition. Notice for example that maximal violation i. e. $\mathrm{Tr}[(\beta_q \mathbb{1} - \mathfrak{B})\varrho_{AB}] = 0$ implies $\sum_\lambda \mathrm{Tr}[P_\lambda^\dagger P_\lambda \varrho_{AB}] = 0$ which due to positivity implies

$$\mathrm{Tr}[P_\lambda^\dagger P_\lambda \varrho_{AB}] = 0 \ \forall \lambda \tag{97}$$

In the purified scheme where the realization is given by the pure state $|\psi\rangle$ we have equivalently for all λ,

$$\langle\psi|P_\lambda^\dagger P_\lambda|\psi\rangle = \left\| P_\lambda |\psi\rangle \right\|^2 = 0 \tag{98}$$

which in conclusion yields $P_\lambda |\psi\rangle = 0$ for all λ. From this one can oftentimes derive non-trivial relations between the measurements and state of the realization achieving the maximal violation. We will use an SOS decomposition in the following.

5.4 Self testing properties of the CHSH game

Starting from $\mathfrak{B}_{\mathrm{CHSH}}$ we have in fact shown that in the purified picture we have that for any state $|\psi\rangle$, $\langle\psi|\mathfrak{B}_{\mathrm{CHSH}}|\psi\rangle \leq 2\sqrt{2}$. Again, the fact that the observables are assumed to correspond with projective measurements allows us to write the shifted Bell operator as

$$2\sqrt{2}\mathbb{1} - \mathfrak{B}_{\mathrm{CHSH}} = \tfrac{1}{\sqrt{2}} \left(\tfrac{A_0 + A_1}{\sqrt{2}} - B_0 \right)^2 + \tfrac{1}{\sqrt{2}} \left(\tfrac{A_0 - A_1}{\sqrt{2}} - B_1 \right)^2 \tag{99}$$

which provides an SOS decomposition. We see directly from the discussion in Sec. 5.3 that any realization of maximal violation involving $|\psi\rangle$ and observables A_0, A_1 and B_0, B_1 fulfills

$$\left(\tfrac{A_0 + A_1}{\sqrt{2}} - B_0 \right) |\psi\rangle = 0 \text{ and } \left(\tfrac{A_0 - A_1}{\sqrt{2}} - B_1 \right) |\psi\rangle = 0 \tag{100}$$

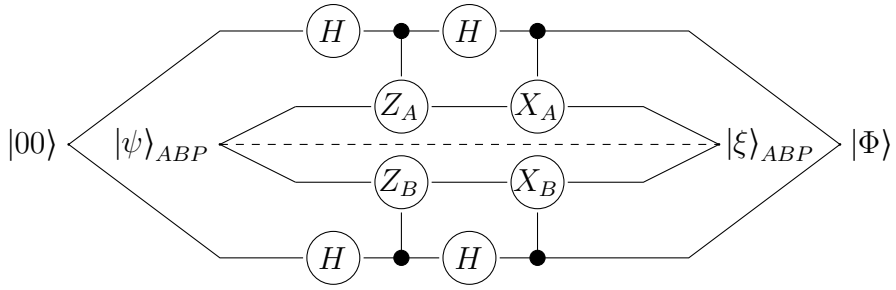


Figure 8: *Partial swap gate to extract canonical state in CHSH game.*

These facts can be used to prove a formal self testing statement about the CHSH game. Its proof consists of using the *partial Swap gate* (given in Figure 8) to show that any physical realization is a local dilation of the canonical realization chosen to be the one that we considered in the proof of Theorem (25) i. e.

$$\left\{\mathbb{C}^2, \mathbb{C}^2, |\Phi\rangle, \{\sigma_Z, \sigma_X\}, \left\{\tfrac{1}{\sqrt{2}}(\sigma_Z + \sigma_X), \tfrac{1}{\sqrt{2}}(\sigma_Z - \sigma_X)\right\}\right\}. \tag{101}$$

The partial Swap gate is used in a large number of self testing proofs [ŠB20]. The first time it was shown to be suitable for self testing purposes was in [MYS12] which shows robust self testing of the CHSH game. We will in the following exposition use the same proof idea however restrict our attention to exact self testing of the state $|\Phi\rangle$.

Theorem 26. *The CHSH game self tests the maximally entangled pair of qubits.*

Proof. Consider a realization of the maximal violation in terms of binary observables given by

$$\mathcal{R} = (\mathcal{H}_A, \mathcal{H}_B, \varrho_{AB}, \{A_0, A_1\}, \{B_0, B_1\}) \tag{102}$$

The first main idea of the proof is to construct operators Z_A, X_A and Z_B, X_B which act on the purification $|\psi\rangle_{ABP}$ of ϱ_{AB} in a similar way as σ_Z, σ_X and $\frac{1}{\sqrt{2}}(\sigma_Z + \sigma_X), \frac{1}{\sqrt{2}}(\sigma_Z - \sigma_X)$ act on Φ. Let

$$Z_A \coloneqq \tfrac{1}{\sqrt{2}}(A_0 + A_1),\ X_A \coloneqq \tfrac{1}{\sqrt{2}}(A_0 - A_1) \text{ and } Z_B \coloneqq B_0,\ X_B \coloneqq B_1. \tag{103}$$

with these we have

$$[Z_A, X_A]_+ |\psi\rangle_{ABP} = 0 \text{ and } [Z_B, X_B]_+ |\psi\rangle_{ABP} = 0 \tag{104}$$

from (100). Moreover, from (100) we have

$$Z_A |\psi\rangle_{ABP} = Z_B |\psi\rangle_{ABP} \text{ and } X_A |\psi\rangle_{ABP} = X_B |\psi\rangle_{ABP}. \tag{105}$$

where we have omitted a tensor product with the identity on the purification space for brevity.

We wish to use Z_A, X_A, Z_B and X_B in the partial swap gate given in Figure 8. This is, however, not immediately possible since Z_A and X_A are not necessarily unitary. We can remedy this by using a *regularization procedure*, which amounts to changing all the zero eigenvalues to one and normalizing. More specifically, if Y is some Hermitian operator with eigen-decomposition $\sum_i y_i |y_i\rangle \langle y_i|$, let $\tilde{Y} = \sum_i \tilde{y}_i |\tilde{y}_i\rangle \langle \tilde{y}_i|$ where $\tilde{y}_i = y_i$ whenever $y_i \neq 0$ and $\tilde{y}_i = 1$ whenever $y_i = 0$. The regularized operator $\hat{Y}$ is then the unitary operator given by $\sum_i \frac{\tilde{y}_i}{|\tilde{y}_i|} |y_i\rangle \langle y_i|$.

The regularized operators $\hat{Z}_A$ and $\hat{X}_A$ are simply given by $\hat{Z}_A = |\tilde{Z}_A|^{-1} Z_A + P_Z$ and similar for $\hat{X}_A$ where P_Z is the projector onto the null spaces of Z_A. We will show that $\hat{Z}_A$ and $\hat{X}_A$ act on $|\psi\rangle$ the same way as Z_A and X_A. Focusing on $\hat{Z}_A$, note that

$$\left\| (\hat{Z}_A - Z_A) |\psi\rangle_{ABP} \right\| = \left\| \hat{Z}_A (\mathbb{1} - \hat{Z}_A^\dagger Z_A) |\psi\rangle_{ABP} \right\| = \left\| (\mathbb{1} - \hat{Z}_A^\dagger Z_A) |\psi\rangle_{ABP} \right\| \tag{106}$$

$$= \left\| (\mathbb{1} - \left(|\tilde{Z}_A|^{-1} Z_A + P_Z \right)^\dagger Z_A) |\psi\rangle_{ABP} \right\| = \left\| (\mathbb{1} - |Z_A|) |\psi\rangle_{ABP} \right\| \tag{107}$$

From the unitarity of Z_B we see that $|Z_B Z_A| = \sqrt{Z_A^\dagger Z_B^\dagger Z_B Z_A} = |Z_A|$. Also, recall the operator inequality $A \leq |A|$. Using these observations the above becomes

$$\left\| (\mathbb{1} - |Z_B Z_A|) |\psi\rangle_{ABP} \right\| \leq \left\| (\mathbb{1} - Z_B Z_A) |\psi\rangle_{ABP} \right\| \tag{108}$$

Now, using (105) we can conclude that the RHS of (108) vanishes, hence $\hat{Z}_A |\psi\rangle_{ABP} = Z_A |\psi\rangle_{ABP}$. A similar argument shows $\hat{X}_A |\psi\rangle_{ABP} = X_A |\psi\rangle_{ABP}$. We can thus proceed to using the partial swap gate with $\hat{Z}_A, \hat{X}_A$ from now on simply denoted Z_A and X_A.

For the sake of brevity we omit the tensor product and let juxtaposition mean tensor product. Also, we will not write units whenever an operator acts trivially on a register. Denote the partial Swap gate in Figure 8, $\mathfrak{S}$. We calculate $\mathfrak{S}[|00\rangle_{A'B'} |\psi\rangle_{ABP}]$ in several steps. The first two Hadamards on the ancilla registers (i. e. $\mathbb{C}^2$) give

$$HH |00\rangle |\psi\rangle_{ABP} = \tfrac{1}{2} \left(|00\rangle + |01\rangle + |10\rangle + |11\rangle \right) |\psi\rangle_{ABP} \tag{109}$$

Applying the two controlled gates $CZ_A \otimes CZ_B$ to this gives

$$\tfrac{1}{2} \left[|00\rangle + Z_B |01\rangle + Z_A |10\rangle + Z_B Z_A |11\rangle \right] |\psi\rangle_{ABP} \tag{110}$$

$$= \tfrac{1}{2} \left[\left(|00\rangle + |11\rangle \right) + Z_B \left(|01\rangle + |10\rangle \right) \right] |\psi\rangle_{ABP} \tag{111}$$

where we have used $Z_A |\psi\rangle_{ABP} = Z_B |\psi\rangle_{ABP}$ and unitarity of Z_B. Note, that

$$HH \left[|00\rangle + |11\rangle \right] = |00\rangle + |11\rangle \text{ and } HH \left[|01\rangle + |10\rangle \right] = |00\rangle - |11\rangle . \tag{112}$$

Another application of HH therefore results in the following after some rewriting,

$$\tfrac{1}{2} \left[\left(|00\rangle + |11\rangle \right) + Z_B \left(|00\rangle - |11\rangle \right) \right] |\psi\rangle_{ABP} \tag{113}$$

$$= \tfrac{1}{2} \left[(\mathbb{1} + Z_B) |00\rangle + (\mathbb{1} - Z_B) |11\rangle \right] |\psi\rangle_{ABP} \tag{114}$$

When applying the controlled gates $CX_A \otimes CX_B$ this becomes

$$\tfrac{1}{2}\left[(\mathbb{1} + Z_B)\,|00\rangle + X_A X_B\,(\mathbb{1} - Z_B)\,|11\rangle\right]|\psi\rangle_{ABP}\,. \tag{115}$$

Using anticommutativity of X_B and Z_B, commutativity of X_A and Z_B, the fact that $X_A\,|\psi\rangle_{ABP} = X_B\,|\psi\rangle_{ABP}$ and lastly unitarity of X_A, (115) becomes

$$\tfrac{1}{2}\left[|00\rangle + |11\rangle\right](\mathbb{1} + Z_B)\,|\psi\rangle_{ABP}\,. \tag{116}$$

Let $|\xi\rangle_{ABP} \coloneqq \frac{\mathbb{1}+Z_A}{\sqrt{2}}\,|\psi\rangle_{ABP}$ to conlcude,

$$\mathfrak{S}\left[|00\rangle\,|\psi\rangle_{ABP}\right] = |\Phi\rangle\,|\xi\rangle_{ABP} \tag{117}$$

which shows that the CHSH game self tests the EPR pair. □

As mentioned earlier the self test can be shown to be robust to noise by using the partial Swap isometry and suitable estimates [MYS12]. Theorem 1 and Theorem 2 of [MYS12] can be concatenated as,

Theorem 27. *([MYS12]). Suppose the physical state, $|\psi\rangle_{ABP}$, and measurements A_0, A_1, B_0 and B_1 are such that*

$$\langle\psi|A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1|\psi\rangle \geq 2\sqrt{2} - \delta \tag{118}$$

for some $0 < \varepsilon < 1$. Then, if we let A'_x and B'_y be the canonical observables, we have

$$\left\|\mathfrak{S}[|00\rangle_{A'B'}\,A_xB_y\,|\psi\rangle_{ABP}] - A'_xB'_y\,|\Phi\rangle_{A'B'}\,|\xi\rangle_{ABP}\right\|_1 \leq 11(\sqrt{2}\delta)^{1/2} + 10(\sqrt{2}\delta)^{1/4} \tag{119}$$

5.5 Linear constraint system games

Another famous example of a nonlocal game showing separation of local and quantum correlations is the *magic square game*. This was independently (implicitly) introduced by Mermin and Peres in [Mer90, Per90]. None of these papers, however, cast the magic square as a game. In fact, in [Mer90] it is falsely claimed that this cannot be done. They merely intended to find simplifications of the proof of the Bell-Kochen-Specker theorem [Bel66, KS68] which proves the contradictory nature of assuming value definiteness and noncontextuality at the same time.

The term "magic square" was coined in [Ara99] and only subsequently in [Ara02] turned into a game. Before moving on to the magic sqaure game, we introduce a more general class of nonlocal games called *linear constraint system games* (LCS) of which the magic square game is a special case.

Definition 28. (*Linear constraint system game*) Let n, d, k be positive integers. Consider n linear equations in k variables denoted $z = (z_1, ..., z_k)$ over $\mathbb{Z}/d\mathbb{Z}$, i. e. a k-by-n matrix

$$C = (c_{ij}) \in \mathbb{M}_{k\times n}[\mathbb{Z}/d\mathbb{Z}] \tag{120}$$

and a vector $v \in (\mathbb{Z}/d\mathbb{Z})^n$ such that $Cz = v$. The linear constraint system game corresponding to this is given by

$$\mathcal{G}_{LCS} := \{\mathcal{X} = [n], \mathcal{Y} = [k], \mathcal{A} = (\mathbb{Z}/d\mathbb{Z})^k, \mathcal{B} = \mathbb{Z}/d\mathbb{Z}, \pi = \tfrac{1}{nk}, V_{LCS}\} \tag{121}$$

where the verification function is

$$V_{LCS}(a,b,x,y) := \begin{cases} 1 \textbf{ if } \sum_{i=1}^{k} c_{ix}a_i = v_x \text{ and } b = a_y \\ 0 \text{ otherwise} \end{cases} \tag{122}$$

•

In words, Alice and Bob win if Alice solves the equation she has been given and Bob outputs the yth variable of Alice's output. Interestingly, there exist unsatisfiable systems of linear constraints for which the corresponding LCS game can in fact be played *perfectly* i. e. with probability 1 using a quantum strategy. Whenever a nonlocal game $\mathcal{G}$ fulfills $\omega_c^*(\mathcal{G}) < \omega_q^*(\mathcal{G}) = 1$ it is called *pseudo-telepathic*.

A subclass of LCS games are the *binary* constraint system (BCS) games i. e. an LCS game with $d = 2$. We will in the subsequent discussion follow [CM14] in which BCS games have been studied in depth. It is convenient to translate $v_j = \{0,1\}$-variable into a $\{-1,1\}$-variable given by $T_j := (-1)^{z_j}$. The parity of some sequence of variables is then given by the product instead of the sum mod 2. Consider the following definition,

Definition 29. (*Operator solution, BCS game*). An *operator solution* to $Cz = v$ (as in Defintion 28 with $d = 2$) is a set of projective binary observables $\{T_1, ..., T_k\}$ such that

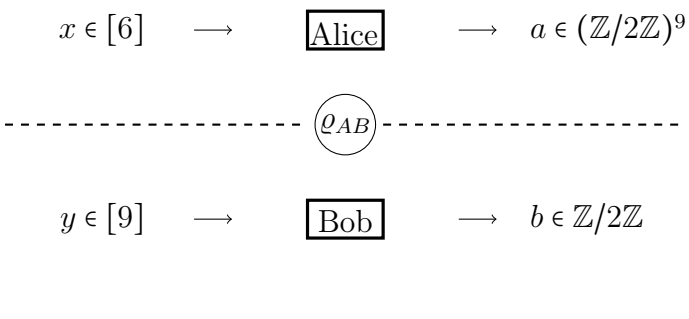
(i) The T_i's are locally compatible. That is, observables appearing in the same constraint commute and

(ii) The observables satisfy each constraint. That is, for each $x \in [n]$ we have $T_1^{c_{x1}} ... T_k^{c_{xk}} = (-\mathbb{1})^{v_x}$.

•

As pointed out in [CM14], this is a relaxation of the classical notion of satisfying the constraints which corresponds to an operator solution restricted to one dimensional observables. The motivation behind introducing operator solutions is that, as shown in [Ara04], the existence of an operator solution implies a perfect quantum strategy using two pairs of maximally entangled states. We will review this result soon in the context of the magic square game.

The magic square game, denoted $\mathcal{G}_{MSG}$, is the prime example of a pseudo-telepathy game. We have summarized the game in Figure 9. It corresponds to the binary constraint system game with $n = 6$ and $k = 9$ and linear constraints as given in 9(b). The set of linear constraints in Figure 9(b) is not satisfiable. This can be



(a) The Bell scenario

$$\begin{array}{ccccccc} z_1 & + & z_2 & + & z_3 & = & 0 \\ + & & + & & + & & \\ z_4 & + & z_5 & + & z_6 & = & 0 \\ + & & + & & + & & \\ z_7 & + & z_8 & + & z_9 & = & 0 \\ \| & & \| & & \| & & \\ 0 & & 0 & & 1 & & \end{array}$$

and $b = a_y$

(b) Winning conditions

Figure 9: *The magic square game*

seen by summing all the elements of the square but in two different ways: First, add all the elements by adding the sum of each row. This is equal to 0. Next, add all the elements by adding the sum of each column. This is equal to 1, a contradiction. So by the earlier comment we must have $\omega_c(\mathcal{G}_{MSG}) < 0$.

Theorem 30. *The magic square game can be played perfectly using the observables given in Figure 10 and a pair of shared maximally entangled states.*

$$\begin{array}{|c|c|c|} \hline z_1 & z_2 & z_3 \\ \hline z_4 & z_5 & z_6 \\ \hline z_7 & z_8 & z_9 \\ \hline \end{array} \sim \begin{array}{|c|c|c|} \hline Z\mathbb{1} & \mathbb{1}Z & ZZ \\ \hline \mathbb{1}X & X\mathbb{1} & XX \\ \hline ZX & XZ & YY \\ \hline \end{array}$$

(a) Alice's assignment of variables

$$\begin{array}{|c|c|c|} \hline z_1 & z_2 & z_3 \\ \hline z_4 & z_5 & z_6 \\ \hline z_7 & z_8 & z_9 \\ \hline \end{array} \sim \begin{array}{|c|c|c|} \hline Z^T\mathbb{1} & \mathbb{1}Z^T & (ZZ)^T \\ \hline \mathbb{1}X^T & X^T\mathbb{1} & (XX)^T \\ \hline (ZX)^T & (XZ)^T & (YY)^T \\ \hline \end{array}$$

(b) Bob's assignment of variables

Figure 10: *Operator solution to the magic square game yields perfect quantum strategy. Note: there is an implicit tensor product when operators are juxtaposed. The transpose is taken in the computational basis.*

Proof. It is straightforward to check that the assignment of observables to variables given in Figure 10(a) provides an operator solution (found first by Peres [Per90]) for the magic square game. One simply checks that the product of each row is indeed $\mathbb{1}$ and the product of each column is $\mathbb{1}$ with the exception of the third column which is equal to $-\mathbb{1}$.

Now, assume Alice and Bob share the state $|\psi\rangle := |\Phi\rangle|\Phi\rangle$. Alice associates the variables T_j to the observables as in Figure 10(a). Upon receiving one of the six linear equations, she then measures her corresponding observables which makes sense since the observables mutually commute. In this way, Alice is ensured to get the right outcome. Bob, upon receiving some input, measures his corresponding observable and we note that Alice and Bob's outcomes are consistent since

$$\langle\psi|T_i \otimes T_i^T|\psi\rangle = \langle\psi|T_i^2 \otimes \mathbb{1}|\psi\rangle = \langle\psi|\psi\rangle = 1, \tag{123}$$

where we have used that $\mathbb{1} \otimes T_i^T |\Phi\rangle = T_i \otimes \mathbb{1} |\Phi\rangle$ in the first equality[2]. □

In fact, the proof idea of the above theorem can easily be generalized to any BCS game in the sense that if one can find an operator solution, one can derive a perfect quantum strategy. The natural question to ask is, if the other direction holds as well. That is, given a perfect strategy, can we derive an operator solution?

The answer to this question turns out to be yes. In [CM14] it is shown that if there exists a strategy within $\mathcal{C}_{qs}$ which wins the game perfectly, one can find an operator solution to the corresponding constaint system. An extension to quantum commuting strategies was made in [CLS17]. In order to explain this further it is necessary to introduce *solution groups*.

It turns out that BCS games can be studied elegantly with group theoretical tools. We can abstract the properties of an operator solution to the level of finitely presented groups as follows,

Definition 31. (*Solution group*) The solution group $\Gamma(C, v)$ of a linear system $Cz = v$ (as in Definition 28) is the group generated by $k+1$ elements $X_1, ..., X_k, J$ satisfying the following,

(i) Each generator is an involution, $X_1^2 = ... = X_k^2 = J^2 = e$.

(ii) J commutes with every generator, $[X_1, J] = ... = [X_k, J] = e$.

(iii) Any pair of generators appearing in the same linear constraint commutes.

(iv) For each $x \in [n]$ $X_1^{c_{x1}} ... X_k^{c_{xk}} = J^{v_x}$.

•

The role of the element J (in Definition 31) is played by $-\mathbb{1}$ in the operator solution we considered in the proof of Theorem 30. Despite the seeming departure from the problem at hand towards a purely abstract construction, the group theoretical view has in fact resulted in a systematic way of studying nonlocal games. The aforementioned result in [CLS17] can now be expressed as

Theorem 32. *([CLS17]) Let $\mathcal{G}$ be a BCS game associated with $Cz = v$. The following are equivalent: (i) $\omega_{qc}(\mathcal{G}) = 1$, (ii) $J \neq e$ in the solution group $\Gamma(C, v)$ and (iii) there exists an operator solution to $Cz = v$.*

It turns out that with tools from representation theory, it is possible to prove self testing results for many BCS games.

Definition 33. (*Unitary representation, unitary ε-representation*, [GH17]). Let G be a finite group, let $\varepsilon > 0$ and let $\mathcal{U}(\mathbb{C}^d)$ denote the group of unitary operators. A *d-dimensional unitary representation of G* is a homomorphism $\sigma : G \to \mathcal{U}(\mathbb{C}^d)$ (i. e. $\sigma(g_1 g_2) = \sigma(g_1)\sigma(g_2)$ for all $g_1, g_2 \in G$). A *d-dimensional unitary*

[2] oftentimes called the mirror lemma for the maximally entangled state.

$$
\begin{array}{ccccccccccccccc}
1 & = & z_3 & + & z_6 & + & z_9 & + & z_{10} & + & z_{13} & + & z_{16} & & \\
 & & + & & + & & + & & + & & + & & & & \\
0 & = & z_2 & + & z_5 & + & z_8 & & z_{11} & + & z_{14} & + & z_{17} & = & 0 \\
 & & + & & + & & + & & + & & + & & & & \\
0 & = & z_1 & + & z_4 & + & z_7 & & z_{12} & + & z_{15} & + & z_{18} & = & 0 \\
 & & \shortparallel & & \shortparallel & & \shortparallel & & \shortparallel & & \shortparallel & & \shortparallel & & \\
 & & 0 & & 0 & & 0 & & 0 & & 0 & & 0 & &
\end{array}
$$

Figure 11: *Glued magic square game*

ε-representation is a map $\sigma : G \to \mathcal{U}(\mathcal{H})$ such that $\left\|\sigma(g_1g_2) - \sigma(g_1)\sigma(g_2)\right\|_{HS} \leq \varepsilon$ for all $g_1, g_2 \in G$.
•

The main idea is that given a solution group $\Gamma(C, v)$ and given that we can obtain a unitary representation of this group, then we can extract an operator solution and hence perfect quantum strategy. Moreover, exploiting the connection between group representations and winning strategies, it is possible to prove self testing results using group theoretical techniques.

The strength of this 'algebraic' method of studying nonlocal games was underlined in [CS17]. There, the authors show that for certain BCS games (including the magic square game) an almost perfect quantum strategy allows the extraction of an approximate unitary representation of the solution group. This is subsequently used to obtain robustness of the self testing statements. A central role in this robustness result is played by a theorem due to Gowers and Hatami,

Theorem 34. *[Gow16] Let G be a finite group, let σ be a d-dimensional unitary $\varepsilon\sqrt{d}$-representation. Then there exists d' with $(1-\varepsilon^2) \leq \frac{d'}{d} \leq \frac{1}{1-2\varepsilon^2}$, an isometry $V : \mathbb{C}^d \to \mathbb{C}^{d'}$ and a d'-dimensional unitary representation σ' of G such that $\left\|\sigma(g) - V^\dagger\sigma'(g)V\right\|_{HS} \leq 31\varepsilon\sqrt{d}$ for all $g \in G$.*

Equipped with this theorem the authors of [CS17] are able to show that for certain well behaved solution groups the corresponding BCS games are guaranteed to be robust self tests.

5.6 Weak self testing

In this section we address the (now resolved) question in [ŠB20] of whether there exists a nonlocal game which self tests a state but not the measurements. Examples include the so-called *glued magic square game* which is constructed by taking two copies of the magic square game as shown in Figure 11. This is shown in [MNP21] to be a self test for a pair of maximally entangled states. However, as shown in [CMMN20], it is not a self test with regards to measurements.

The author of [Kan20] studies a family Bell inequalities, which we here denote

B_{WST}, with three inputs and two outputs on both Alice's and Bob's side which is shown to be maximally violated for every probability point belonging to a line segment in the boundary of $\mathcal{C}_q(3,3,2,2)$. It is shown, that the maximal violation in fact robustly certifies a maximally entangled pair of qubits. This means that, although points along this line segment are not extreme points it is still possible to certify the state. such a phenomenon is called *weak self testing*. Another characteristic of the Bell functionals studied in [Kan20] is, that the endpoints of the maximizing line segment, which are indeed extreme points, actually admit a full self testing statement see Figure 12.

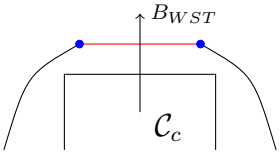


Figure 12: *Illustration of Bell functional B_{WST} exhibiting weak self testing. The red line certifies a state but not measurements. The blue (extreme) points admit full self testing statement.*

Having already established that the CHSH game self tests a pair of maximally entangled qubits, we propose a simplified way of obtaining a weak self testing in the following. Consider the following nonlocal game,

$$\mathcal{G}_\perp := \left\{\mathcal{X} = \{0,1\}, \mathcal{Y} = \{0,1,\perp\}, \mathcal{A} = \{0,1\}, \mathcal{B} = \{0,1\}, \pi_\perp = \tfrac{1}{6}, V_\perp\right\} \tag{124}$$

where $V_\perp$ is given by,

$$V_\perp := \begin{cases} 1 \textbf{ if } y = 0,1 \text{ and } a + b + xy = 0 \bmod 2 \\ 0 \text{ otherwise} \end{cases} \tag{125}$$

In words, Alice and Bob win if Bob receives $y = 0,1$ and they win by the same rules as in the CHSH game. If Bob gets the question $y = \perp$ they lose. The game value in a t-model is given by

$$\omega_t^*(\mathcal{G}_\perp) = \tfrac{2}{3}\omega_t^*(\mathcal{G}_{\text{CHSH}}). \tag{126}$$

The quantum game value is still attained only if the shared state is equivalent with a maximally entangled pair of qubits and the observables A_0 and A_1 as well as B_0 and B_1 anti-commute as for the CHSH game. However it is obviously impossible to say anything about Bobs observable $B_\perp$ corresponding to the question $y = \perp$ which makes a full self testing statement impossible. We do however have weak self testing since $\mathcal{G}_\perp$ self tests a pair of maximally entangled qubits. The winning probability is independent of all the probabilities $p(ab|x, y = \perp)$. This means that any maximizer belongs to a corresponding 8 dimensional affine subspace. We of course still have the no-signalling constraints,

$$p(a|x) = p(a,0|x,\perp) + p(a,1|x,\perp). \tag{127}$$

At optimality Alice's marginal probabilities $p(a|x)$ are fixed. Hence, we have 4 linearly independent linear constraints reducing the number of dimensions from 8 to 4. It would be interesting to investigate whether the boundary of the intersection of this 4 dimensional affine subspace and $\mathcal{C}_q(3,2,2,2)$ contains nonself testing correlations. If this is the case, one could obtain an example of a nonself testing extreme point in this very simple way.

6 Mutual unbiasedness

In this section we take a detour and discuss different notions of unbiasedness in measurements. This will turn out to be necessary in order to understand the subsequent construction of a nonlocal game showing that not all extreme points in $\mathcal{C}_q$ are self tests. We first define the well-known *mutually unbiased bases* (MUBs). Next, we define *mutually unbiased measurements* recently introduced in [TFR+21, FKN22]. Lastly, we introduce a novel weaker notion of unbiasedness we term *mutually orthogonal measurements* due to their corresponding Bloch vector representations consisting of orthogonal Bloch vectors. Throughout we let $\mathcal{H}$ be of dimension d.

6.1 Mutually unbiased bases

Definition 35. (*Mutually unbiased bases (MUBs)*) Let $\{|\psi_i\rangle\}$ and $\{|\varphi_i\rangle\}$ be orthonormal bases of $\mathcal{H}$. If for all $i,j \in [d]$ we have

$$|\langle\psi_i|\varphi_j\rangle|^2 = \tfrac{1}{d} \tag{128}$$

we call these *mutually unbiased bases*.
•

A pair of mutually unbiased bases have the property that if a system is prepared in any eigenstate of one of the bases then a measurement in the other has equiprobable outcomes. A long standing open problem of much importance in all of quantum information science is the existence problem of MUBs. An upper and lower bound on the number of MUBs for a given dimension d is the following [Ben07]: Let $d = p_1^{N_1} \cdot \ldots \cdot p_k^{N_k}$ be the prime number decomposition of the dimension with $p_1^{N_1} < \ldots < p_k^{N_k}$. Then the number of MUBs, $\mathfrak{M}(d)$ obeys,

$$p_1^{N_1} \leq \mathfrak{M}(d) \leq d+1 \tag{129}$$

The above inequality becomes an equality for prime power dimension $d = p^N$. However, for composite dimensions the problem is open. Already in the smallest composite case $d = 6$ case it is conjectured based on strong numerical evidence that the largest set of MUBs contains three bases [Gra04, BH07, BW08, BW09, DEBZ10, RLE11, Che18] (see also [HRZ20]).

One way of studying MUBs is through *complex Hadamard matrices*. These are rescaled unitary matrices with unimodular entries, i. e. a d-by-d matrix H fulfilling

$$\left|H_{ij}\right| = 1 \ (\forall i, j) \text{ and } HH^\dagger = d\mathbb{1}. \tag{130}$$

The importance of complex Hadamard matrices has been well-established in a seminal paper by Werner [Wer01], in which links are drawn to canonical quantum information theoretical concepts such as superdense coding and teleportation. It is convenient to define the following equivalence relation

Definition 36. Two unitary matrices U_0 and U_1 are equivalent, written $U_0 \approx U_1$ if and only if there exist permutation matrices P_0 and P_0 and diagonal unitaries D_0 and D_1 such that

$$U_0 = P_0 D_0 U_1 D_1 P_1. \tag{131}$$

•

It is straightforward to verify that this is an equivalence relation. This equivalence reflects the fact that permutation of basis elements as well as multiplication with phase factors leave the basis in question unchanged. One of the main examples in this thesis requires an equivalence relation on pairs of MUBs.

Definition 37. Two pairs of MUBs assembled into two pairs of unitaries (M_0, M_1) and $(M_0' M_1')$ are equivalent, written

$$(M_0, M_1) \sim (M_0', M_1') \tag{132}$$

if and only if there exist a unitary U, diagonal unitaries, D_0, D_1 and permutation matrices P_0, P_1 such that

$$(M_0', M_1') = (UM_0P_0D_0, UM_1P_1D_1). \tag{133}$$

•

Now, it is clear that any pair of MUBs (M_0, M_1) is equivalent with $(\mathbb{1}, M_0^\dagger M_1)$ It is also clear that a basis, which is mutually unbiased with the computational basis must be given by a complex Hadamard matrix (with a scaling factor of $\frac{1}{\sqrt{d}}$). Hence any pair of MUBs can be brought to its *standard form*, $(\mathbb{1}, H)$ where H is a rescaled, comlpex Hadamard matrix.

Lemma 38. *Let* (M_0, M_1) *and* (M_0', M_1') *be pairs of MUBs. We have* $(M_0, M_1) \sim (M_0', M_1')$ *if and only if* $M_0^\dagger M_1 \approx M_0'^\dagger M_1'$

Proof. First note that $(M_0, M_1) \sim (M_0', M_1')$ if and only if $(\mathbb{1}, M_0^\dagger M_1) \sim (\mathbb{1}, M_0'^\dagger M_1')$ by transitivity of equivalence relations. Now, the latter, by definition is the case if and only if there exist a unitary U, diagonal unitaries, D_0, D_1 and permutation matrices P_0, P_1 such that

$$(U\mathbb{1}P_0D_0, UM_0'^\dagger M_1' P_1 D_1) = (\mathbb{1}, M_0^\dagger M_1). \tag{134}$$

By picking $U = D_0^{-1} P_0^{-1}$ we see that this is the case. We then have

$$M_0^\dagger M_1 = D_0^{-1} P_0^{-1} M_0'^\dagger M_1' P_1 D_1 \tag{135}$$

which means that $M_0^\dagger M_1 \approx M_0'^\dagger M_1'$ □

We also recall the following well-known result (see e. g. Proposition 2.1 in [Haa97]) which will be useful later:

Proposition 39. *For $d = 2, 3$ any two complex Hadamard matrices are equivalent. For $d = 4$, there exists a one parameter family of inequivalent complex Hadamard matrices given by*

$$F(t) := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & ie^{it} & -ie^{it} \\ 1 & -1 & -ie^{it} & ie^{it} \end{pmatrix} \tag{136}$$

for any $t \in [0, \pi)$.

6.2 Weaker notions of unbiasedness

As mentioned earlier, we are interested in weakening the notions of unbiasedness in measurements. The first weakening, introduced in [TFR+21, FKN22], allows one to consider cases where the number of outcomes does not match the dimension of the space.

Definition 40. (*Mutually unbiased measurements, (MUMs).* Let $\{P_a\}_{a\in[n]}$ and $\{Q_b\}_{b\in[n]}$ be n-outcome measurements. If for all $a, b \in [n]$ we have

$$P_a = nP_aQ_bP_a \text{ and } Q_b = nQ_bP_aQ_b \tag{137}$$

we call $\{P_a\}$ and $\{Q_b\}$ *mutually unbiased measurements.*
•

It is clear that (137) becomes (128) if the measurement operators are rank one projectors. Note, that MUMs are projective. This can be seen by summing over the middle index in (139). Moreover, using cyclicity of the trace function we obtain

$$\mathrm{Tr}[P_a] = \mathrm{Tr}[Q_b] = n\mathrm{Tr}[P_aQ_b]. \tag{138}$$

Hence the trace over the different measurement operators is constant and equal to $\frac{d}{n} =: \gamma \in \mathbb{N}$. We introduce therefore the following weaker notion of unbiasedness,

Definition 41. (*Mutually orthogonal measurements, (MOMs)* Let $\{P_a\}_{a\in[n]}$ and $\{Q_b\}_{b\in[n]}$ be n-outcome projective measurements. If for all $a, b \in [n]$ we have

$$\mathrm{Tr}[P_a] = \mathrm{Tr}[Q_b] = n\mathrm{Tr}[P_aQ_b]. \tag{139}$$

we call $\{P_a\}$ and $\{Q_b\}$ *mutually orthogonal measurements.*
•

We have in general that $MUB \subseteq MUM \subseteq MOM$. These inclusions coincide when d is prime (since $\gamma = \frac{d}{n} \in \mathbb{N}$) but they are strict otherwise as the following example shows,

$$P_0 = |0\rangle\langle 0| \otimes \mathbb{1}_2,\ P_1 = |1\rangle\langle 1| \otimes \mathbb{1}_2 \text{ and} \tag{140}$$
$$Q_0 = \mathbb{1}_2 \otimes |0\rangle\langle 0|,\ Q_1 = \mathbb{1}_2 \otimes |1\rangle\langle 1| \tag{141}$$

It is easy to see that these are MOMs but not MUMs. The reason for the name (MOM) is the following observation,

Lemma 42. *(Bloch vector representation of MOMs). Let $\{P_a\}_{a\in[n]}$ and $\{Q_b\}_{b\in[n]}$ be a pair of n-outcome MOMs. Their Bloch vector representations $\{\alpha_a\}_{a\in[n]}, \{\beta_b\}_{b\in[n]} \subseteq \mathcal{B}_d$ fulfill*

$$(1)\ \sum_{i\in[n]} \alpha_a = \sum_{i\in[n]} \beta_b = 0,\ (2)\ \langle \alpha_a, \beta_b\rangle = 0 \text{ and } (3)\ \|\alpha_a\| = \|\beta_b\| = \sqrt{\tfrac{2}{d}(n-1)} \tag{142}$$

for all $a, b \in [n]$. Conversely, assume (142) for two sets of n Bloch vectors $\{\alpha_a\}_{a\in[n]}, \{\beta_b\}_{b\in[n]} \subseteq \mathcal{B}_d$ both spanning $n-1$-dimensions. The unique POVMs associated with these are MOMs.

Proof. Suppose first that $\{P_a\}$ and $\{Q_b\}$ are a pair of MOMs and $\{\alpha_a\}$ and $\{\beta_b\}$ be their Bloch vector representations. Let

$$\gamma := \mathrm{Tr}[P_a] = \mathrm{Tr}[Q_b] = n\mathrm{Tr}[P_a Q_b] \tag{143}$$

which is an integer since the POVMs are projective. Note, that by summing over one of the indices one finds $n\gamma = d$. We have

$$P_a = \gamma(\tfrac{1}{d}\mathbb{1} + \tfrac{1}{2}\tfrac{2}{\gamma}\alpha_a \cdot \sigma) = \gamma\varrho(\alpha_a) \tag{144}$$

where we have used that the trace is constant over all the POVM operators. Similarly $Q_b = \gamma\varrho(\beta_b)$, and we immediately have $\sum_a \alpha_a = 0$ and $\sum_b \beta_b = 0$. Recall that the overlap of states can be calculated in terms of their Bloch vectors (see (17)). Hence

$$\gamma = n\mathrm{Tr}[P_a Q_b] = n\gamma^2\left(\tfrac{1}{d} + \tfrac{1}{2}\langle \alpha_a, \beta_b\rangle\right) = d\gamma\left(\tfrac{1}{d} + \tfrac{1}{2}\langle \alpha_a, \beta_b\rangle\right) \tag{145}$$

which yields $\langle \alpha_a, \beta_b\rangle = 0$ for all a, b. By projectivity we have $\varrho(\alpha_a) = \gamma\varrho(\alpha_a)^2$. Tracing over this we get

$$1 = \gamma\left(\tfrac{1}{d} + \tfrac{1}{2}\|\alpha_a\|^2\right) \tag{146}$$

by using (17) again. Isolating the norm yields $\|\alpha_a\| = \sqrt{\frac{2}{d}(n-1)}$ as desired.

For the other direction, assume $\{\alpha_a\}$ and $\{\beta_b\}$ fulfill (142) and span $n-1$ dimensions. Let $\{P_a\}$ and $\{Q_b\}$ be the unique POVMs corresponding to these. Write

$$A_a = \nu_a^0 \mathbb{1} + \nu_a \cdot \sigma \tag{147}$$

where $\sum_a \nu_a^0 = 1$, $\sum_a \nu_a = 0$ and $\alpha_a = \frac{2}{d\nu_a^0}\nu_a$. From the requirement that $0 = \sum_a \alpha_a$ we get

$$0 = \nu_{a'} + \sum_{a\neq a'} \frac{\nu_{a'}^0}{\nu_a^0}\nu_a = \sum_{a\neq a'} \left(\frac{\nu_{a'}^0}{\nu_a^0} - 1\right)\nu_a \tag{148}$$

which yields $\nu_1^0 = ... = \nu_n^0 = \frac{1}{n}$ assuming $\{\alpha_a\}_{a\neq a'}$ spans $n-1$ dimensions. We have therefore that $\nu_a = \frac{d}{2n}\alpha_a$ and hence

$$P_a = \frac{1}{n}\mathbb{1} + \frac{2d}{n}\alpha_a \cdot \sigma = \frac{d}{n}\left(\frac{1}{d}\mathbb{1} + \frac{1}{2}\alpha_a \cdot \sigma\right) = \gamma\varrho(\alpha_a) \tag{149}$$

where, as before $\gamma = \frac{d}{n}$. Similarly one derives $Q_b = \gamma\varrho(\beta_b)$. We see that $\gamma = \mathrm{Tr}[P_a] = \mathrm{Tr}[Q_b]$. Notice also that

$$\mathrm{Tr}[(\gamma\varrho(\alpha_a))^2] = \gamma^2\left(\frac{1}{d} + \frac{1}{2}\|\alpha_a\|^2\right) = \gamma \tag{150}$$

using again (17) and the assumption on the norm of α_a. Since the spectrum of $\gamma\varrho(\alpha_a)$ is contained in $[0,1]$ the only way in which $\mathrm{Tr}[(\gamma\varrho(\alpha_a))^2] = \mathrm{Tr}[\gamma\varrho(\alpha_a)]$ is if the spectrum is in fact contained in $\{0,1\}$ making $\{P_a\}$ projective. In the same way one concludes that $\{Q_b\}$ must be projective. To finish, notice that

$$\mathrm{Tr}[P_aQ_b] = \gamma^2\left(\frac{1}{d} + \frac{1}{2}\langle\alpha_a, \beta_b\rangle\right) = \frac{\gamma^2}{d} = \frac{\gamma}{n}. \tag{151}$$

□

It turns out that this observation combined with the main theorem of [MS22b] provides a certain type of certification on the measurement operators in the prepare-and-measure scenario known as a quantum random access code which we will return to in Sec. (8).

7 Separation of self testing correlations and exposed points

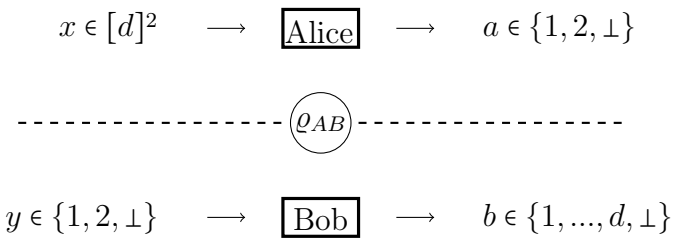
In this section we will in part review the recent result of [TFR+21]. There, as mention before, the authors find a Bell inequality with maximal violation in a unique probability point without being a self test. The uniqueness of the maximizing correlation implies that it, in fact, corresponds to an exposed point of $\mathcal{C}_q$. We will contribute with a nonlocal game with the same property i. e. that its quantum game value is achieved by a unique correlation $p \in \mathcal{C}_q$ without being a self test for its canonical realization.

Let d be a natural number lower bounded by 2. Consider the following game

$$\mathcal{G}_{\mathrm{MUM}} = (\mathcal{X} = [d]^2, \mathcal{Y} = \{1, 2\ \bot\}, \mathcal{A} = \{1, 2\ \bot\}, \mathcal{B} = \{1, 2\ \bot\}, \pi_{\mathrm{MUM}}, V_{\mathrm{MUM}}) \tag{152}$$

The prior is given by

$$\pi_{\mathrm{MUM}}(x, y) = \begin{cases} \kappa & \textbf{if } \ y = 1, 2 \\ \kappa^{\bot} & \textbf{if } \ y = \bot\ . \end{cases} \tag{153}$$



(a) Bell scenario

$y = 1, 2$ and $a = y$ and $b = x_y$
$y = 1, 2$ and $a = \bar{y}$ and $b \neq x_y$
$y = a = b = \perp$

(b) Winning conditions

Figure 13: *The nonlocal game $\mathcal{G}_{MUM}$.*

where $\kappa \neq 0$ and $\kappa^\perp$ fulfill the normalization requirement,

$$2\kappa + \kappa^\perp = \tfrac{1}{d^2} \tag{154}$$

The rules of the game (i. e. the definition of the verification function) are as follows: If Bob receives $y = 1, 2$ then Alice and Bob have two chances of winning:

(i) if Alice's output, a is the same as Bob's input, y, and- Bob's output, b, is the same as the yth dit of Alice's 2-dit input string, or

(ii) if Alice's output is the bit-flipped of y, denoted $\bar{y}$, and Bob's output is different from the yth dit of Alice's 2-dit input string.

One can think of the winning conditions, as each of their outputs simultaneously being consistent or simultaneously being inconsistent with the others input. If Bob receives question $y = \perp$, their only chance of winning is if both Alice and Bob output $\perp$. The game is summarized in Figure 13.

Lemma 43. *Let $\eta_d \coloneqq \frac{\kappa^\perp}{\kappa}$. The winning probability of $\mathcal{G}_{MUM}$ is given by*

$$\omega(\mathcal{G}_{MUM}) = 1 - \tfrac{1}{\eta_d + 2}\left(1 - \tfrac{S}{d^2}\right) \tag{155}$$

where $\mathcal{S}$ is defined as

$$\sum_x \left[-\eta_d \left[p(a = 1|x) + p(a = 2|x) \right] + \sum_{y=1,2} \left[p(a = y, b = x_y|xy) - p(a = \bar{y}, b = x_y|xy) \right] \right]. \tag{156}$$

Proof. It is clear that whenever Bob gets question $y = \perp$ he must answer with $b = \perp$. If he does not, the strategy will be strictly suboptimal. This means, we only have to consider the case where

$$p(a = \perp, b = \perp | x, y = \perp) = p(a = \perp | x) \tag{157}$$

based on the no-signaling constraint. We have the following winning probability,

$$\omega(\mathcal{G}_{\mathrm{MUM}}) = \sum_x \left[\kappa^\perp p(a = \perp | x) + \kappa \sum_{y=1,2} \left[p(a = y, b = x_y|xy) + \sum_{b \neq x_y} p(a = \bar{y}, b|xy) \right] \right] \tag{158}$$

Using the no-signaling condition,

$$p(a=\bar{y}|x) = p(a=\bar{y}, b=x_y|xy) + \sum_{b\neq x_y} p(a=\bar{y}, b|xy), \tag{159}$$

we can rewrite $\omega(\mathcal{G}_{\text{MUM}})$ as

$$\sum_x \Big[\kappa^{\perp} p(a=\perp|x) + \kappa \sum_{y=1,2} \big[p(a=y, b=x_y|xy) + p(a=\bar{y}|x) - p(a=\bar{y}, b=x_y|xy) \big] \Big] \tag{160}$$

We can similarly write the probability of loosing, $\bar{\omega}(\mathcal{G}_{\text{MUM}})$, as

$$\sum_x \Big[\kappa^{\perp} \big(1 - p(a=\perp|x)\big) + \kappa \sum_{y=1,2} \big[p(a=\bar{y}, b=x_y|xy) + p(a=y|x) - p(a=y, b=x_y|xy) \big] \Big] \tag{161}$$

Hence $\Delta(\mathcal{G}_{\text{MUM}})$ is equal to

$$2\sum_x \Big[\kappa^{\perp} p(a=\perp|x) + \kappa \sum_{y=1,2} \big[p(a=y, b=x_y|xy) - p(a=\bar{y}, b=x_y|xy) \big] \Big] - \kappa^{\perp} d^2 \tag{162}$$

where we have used that $\sum_{y=1,2} \big[p(a=\bar{y}|x) - p(a=y|x) \big] = 0$. Using $1 = \sum_a p(a|x)$ and the assumption that $\kappa \neq 0$ we can rewrite $\Delta(\mathcal{G}_{\text{MUM}})$ as follows

$$2\kappa \sum_x \Big[-\eta_d \big[p(a=1|x) + p(a=2|x) \big] + \sum_{y=1,2} \big[p(a=y, b=x_y|xy) - p(a=\bar{y}, b=x_y|xy) \big] \Big] + \kappa^{\perp} d^2 \tag{163}$$

Identifying the definition of $\mathcal{S}$ in (163) we have

$$\Delta(\mathcal{G}_{\text{MUM}}) = 2\kappa\mathcal{S} + \kappa^{\perp} d^2 \tag{164}$$

so after some rewriting one finds the winning probability

$$\omega(\mathcal{G}_{\text{MUM}}) = \tfrac{1}{2} + \kappa\mathcal{S} + \tfrac{1}{2}\kappa^{\perp} d^2 = 1 - \tfrac{1}{\eta_d + 2}\big(1 - \tfrac{\mathcal{S}}{d^2}\big) \tag{165}$$

using (154) in the last equality. □

Observe, that a lower bound on $\omega^*(\mathcal{G}_{\text{MUM}})$ is given by setting $\mathcal{S} = 0$ (corresponding to a strategy where Alice always outputs $a = \perp$). That is,

$$\omega^*(\mathcal{G}_{\text{MUM}}) \geq 1 - \tfrac{1}{\eta_d + 2} \tag{166}$$

We define $\mathcal{S}_t^* := \sup_{p \in \mathcal{C}_t} \mathcal{S}^*$. The following was shown in [TFR+21]. For completeness we give the proof of the quantum bound.

Theorem 44. *[TFR+21]. The following holds,*

$$\mathcal{S}_c^* = 2(d-1)(1-\eta_d) \text{ and } \mathcal{S}_q^* = \tfrac{d-1}{2\eta_d}. \tag{167}$$

Proof. Without loss of generality (using purification and Naimark dilation) let measurements $\{A_a^x\}$, $\{B_b^y\}$ be projective and consider the pure state $|\psi\rangle$. We omit tensor products with identity and calculate first the second term of $\mathcal{S}$ as,

$$\sum_x \langle\psi|A_1^x \otimes B_{x_1}^1 - A_2^x \otimes B_{x_1}^1 + A_2^x \otimes B_{x_2}^2 - A_1^x \otimes B_{x_2}^2|\psi\rangle \tag{168}$$

$$= \sum_x \langle\psi|(A_1^x - A_2^x) \otimes (B_{x_1}^1 - B_{x_2}^2)|\psi\rangle \tag{169}$$

Applying the Cauchy Schwarz inequality in every term gives an upper bound of

$$\sum_x \sqrt{\langle\psi|(A_1^x - A_2^x)^2|\psi\rangle}\sqrt{\langle\psi|(B_{x_1}^1 - B_{x_2}^2)^2|\psi\rangle} \tag{170}$$

$$= \sum_x \sqrt{\langle\psi|A_1^x + A_2^x|\psi\rangle}\sqrt{\langle\psi|(B_{x_1}^1 - B_{x_2}^2)^2|\psi\rangle} \tag{171}$$

$$\leq \sqrt{\sum_x \langle\psi|A_1^x + A_2^x|\psi\rangle}\sqrt{\sum_x \langle\psi|(B_{x_1}^1 - B_{x_2}^2)^2|\psi\rangle}. \tag{172}$$

In the first step we used that Alice measurements are projective. In the last step the Cauchy Schwarz inequality has been applied again but in the form: For $x_i, y_i \geq 0$ one has $\sum_i \sqrt{x_i}\sqrt{y_i} \leq \sqrt{\sum_i x_i}\sqrt{\sum_i y_i}$. The first factor in (172) corresponds exactly to the first term of $\mathcal{S}$. Define $t := \sum_x \langle\psi|A_1^x + A_2^x|\psi\rangle$ then we have

$$\mathcal{S}_q \leq -t\eta_d + \sqrt{t\sum_x \langle\psi|(B_{x_1}^1 - B_{x_2}^2)^2|\psi\rangle} \tag{173}$$

$$= -t\eta_d + \sqrt{t\sum_x \langle\psi|B_{x_1}^1 + B_{x_2}^2 - [B_{x_1}^1, B_{x_2}^2]_+|\psi\rangle} \tag{174}$$

$$= -t\eta_d + \sqrt{t\sum_{x_1} \langle\psi|dB_{x_1}^1 + \mathbb{1} - 2B_{x_1}^1|\psi\rangle} \tag{175}$$

$$= -t\eta_d + \sqrt{2t(d-1)} \tag{176}$$

using projectiveness of Bob's measurements in the first equality and completeness in the second and third. Differentiating with respect to t and setting to zero yields $t = \frac{(d-1)}{2\eta_d^2}$ which reinserted in (176) gives $\frac{d-1}{2\eta_d}$. It is straightforward to chech that this is a maximum. □

Note that $S_c^* < S_q^*$ for any $d \geq 2$ and any $\eta_d \in (0,1)$ so we have a separation of the quantum and classical bounds. Theorem 44 provides the quantum and classical game values of $\mathcal{G}_{\text{MUM}}$,

$$\omega_c^*(\mathcal{G}_{\text{MUM}}) = 1 - \tfrac{1}{\eta_d+2}\left(1 - \tfrac{2(d-1)(1-\eta_d)}{d^2}\right) \text{ and } \omega_q^*(\mathcal{G}_{\text{MUM}}) = 1 - \tfrac{1}{\eta_d+2}\left(1 - \tfrac{d-1}{2\eta_d d^2}\right) \tag{177}$$

Consider the case where $\eta_d = \frac{1}{2}\sqrt{\frac{d-1}{d}}$. Note that η_d tends to $\frac{1}{2}$ from below as $d \to \infty$. The lower bound in this case tends to $\frac{3}{5}$ as $d \to \infty$. We have plotted the game values as a function of d in Figure 14. Notice that both $\omega_c^*(\mathcal{G}_{\text{MUM}})$ and $\omega_q^*(\mathcal{G}_{\text{MUM}})$ go to $\frac{3}{5}$ when $d \to \infty$.

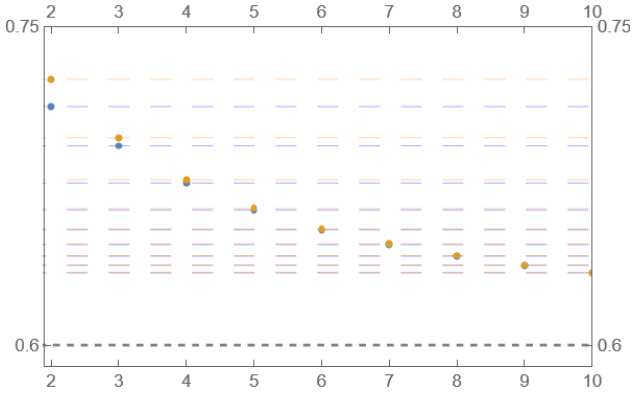


Figure 14: *Local and quantum game values of $\mathcal{G}_{MUM}$ as a function of d. The orange points are $\omega_q^*(\mathcal{G}_{MUM})$. The blue points are $\omega_c^*(\mathcal{G}_{MUM})$.*

7.1 Inequivalent realizations of $\omega_q^*(\mathcal{G}_{\mathbf{MUM}})$

In the following theorem, we have collected several different results of [TFR+21] in the same condensed statement.

Theorem 45. *[TFR+21] Let $\eta_d := \frac{1}{2}\sqrt{\frac{d-1}{d}}$. Assume the shared state between Alice and Bob has full rank marginals.*

(α) The maximal quantum value $\mathcal{S}_q$ certifies:

(i) There exist local isometries which allow Alice and Bob to extract a maximally entangled state of local dimension d.

(ii) Bob's two d-outcome measurements corresponding to $y = 1, 2$ are MUMs.

(β) The certification in (α) is complete i. e. given Bob's measurements corresponding to $y = 1, 2$ are a pair of MUMs and the shared state is maximally entangled there exist measurements for Alice such that $\mathcal{S}_q$ is obtained.

(γ) The characterization in (α) is sufficient to determine the probabilities $p(ab|xy)$ for all $x \in [d]^2$, $y = 1, 2$, $a = 1, 2, \perp$ and $b \in [d]$.

We remark that the assumption that the marginal states be full rank is merely for convenience. As we have seen, we are only able to make certification claims about the measurements on the support of the marginal states. Therefore, if the marginal states are not full rank the Hilbert spaces decompose into direct sums of two terms corresponding to the support and the null space of the marginal states.

We will not recreate the proof of Theorem (45). The important take away is that as long as Bob's measurements corresponding to $y = 1, 2$ are MUMs and the shared state is maximally entangled they can reach $\omega^*(\mathcal{G}_{\text{MUM}})$ for some choice of measurement on Alice's side. And from the shared state being maximally entangled and Bob's measurements being MUMs for $y = 1, 2$ one can recover the correlation table regarding $x \in [d]^2$, $y = 1, 2$, $a = 1, 2, \perp$ and $b \in [d]$.

Let us instead show that two realizations containing the same state (with full-rank marginal on Bob) on identical Hilbert spaces but inequivalent pairs of MUBs on Bob's side in the sense of Definition (37) are inequivalent in the sense of self testing.

Lemma 46. *Let $p \in \mathcal{C}_q$. Assume*

$$\mathcal{R}_p = (\mathcal{H}_A, \mathcal{H}_B, |\varphi\rangle_{AB}, \{A_a^x\}, \{B_b^y\}) \text{ and } \mathcal{R}'_p = (\mathcal{H}_A, \mathcal{H}_B, |\varphi\rangle_{AB}, \{P_a^x\}, \{Q_b^y\}), \quad (178)$$

are realizations. Assume $\varrho_B = Tr_A[|\varphi\rangle\langle\varphi|_{AB}]$ has full rank. Assume also for some $y_0, y_1 \in \mathcal{Y}$ that $\left(\{B_b^{y_0}\}, \{B_b^{y_1}\}\right)$ and $\left(\{Q_b^{y_0}\}, \{Q_b^{y_1}\}\right)$ are two pairs of MUBs. If $\mathcal{R}'_p \hookrightarrow \mathcal{R}_p$ then these are equivalent in the sense of Definition (37).

Proof. We use the fact that the Hilbert spaces are identical in the two realizations and that Bob's marginal state is full rank. Since $\mathcal{R}'_p \hookrightarrow \mathcal{R}_p$ there exists, according to definition 18, a unitary V_B such that

$$V_B B_b^{y_0} |a\rangle\langle a| \left(V_B B_b^{y_0}\right)^\dagger = Q_b^{y_0} |a\rangle\langle a| \left(Q_b^{y_0}\right)^\dagger \text{ and} \quad (179)$$

$$V_B B_b^{y_1} |a\rangle\langle a| \left(V_B B_b^{y_1}\right)^\dagger = Q_b^{y_1} |a\rangle\langle a| \left(Q_b^{y_1}\right)^\dagger \ \forall a. \quad (180)$$

It follows that $\left(Q_b^{y_0}\right)^\dagger V_B B_b^{y_0} =: D_0$ and $\left(Q_b^{y_1}\right)^\dagger V_B B_b^{y_1} =: D_1$ are diagonal unitaries. By isolating V_B and equating we get

$$Q_b^{y_0} D_0 (B_b^{y_0})^\dagger = Q_b^{y_1} D_1 (B_b^{y_1})^\dagger \quad (181)$$

which can be rewritten as

$$(B_b^{y_0})^\dagger B_b^{y_1} = D_0^\dagger (Q_b^{y_0})^\dagger Q_b^{y_1} D_1. \quad (182)$$

The desired now follows from Lemma 38. □

We are now ready to state and prove the main result of this section,

Theorem 47. *The quantum game value $\omega_q^*(\mathcal{G}_{MUM})$ is achieved in an exposed point. However, $\mathcal{G}_{MUM}$ is not a self test.*

Proof. The probabilities $p(ab|x, y = \perp)$ and $p(a, b = \perp |xy)$ at $\omega_q^*(\mathcal{G}_{\text{MUM}})$ are fixed as

$$p(a, b = \perp |x, y \neq \perp) = p(a, b \neq \perp |x, y = \perp) = 0 \text{ and } p(a, b = \perp |x, y = \perp) = p(a|x) \quad (183)$$

From this and Theorem 45(γ) we conclude that the quantum value is achieved by a unique correlation which is therefore an exposed point.

Proposition 39 says that for $d = 4$ there exists a one-parameter family, $F(t)$, of inequivalent Hadamard matrices. Using completeness in Theorem 45(β) we can consider two realizations, $\mathcal{R}_p$ and $\mathcal{R}'_p$ in which Bob's measurements corresponding to $y = 1, 2$ are given by the pairs of MUBs $\left(\mathbb{1}, F(y)\right)$ and $\left(\mathbb{1}, F(y')\right)$ respectively where $y \neq y'$. Lemma 38 tells us that these are inequivalent as pairs of MUBs. With Lemma 46 we can conclude none of $\mathcal{R}'_p$ and $\mathcal{R}_p$ can be locally dilated to the other one and hence $\mathcal{G}_{\text{MUM}}$ cannot be a self test. □

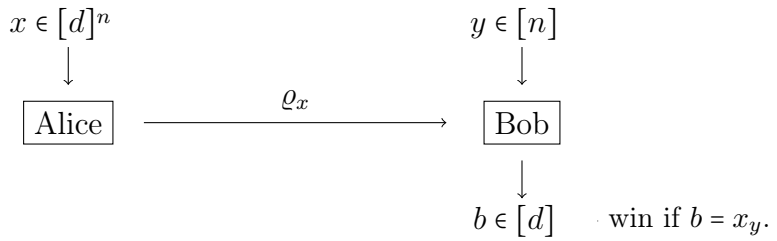


Figure 15: *Quantum random access code.*

8 Semi-device independent self testing

In [TKV+18, FK19] the notion of self-testing is extended to prepare-and-measure (PaM) scenarios. In this setting, we consider a device that prepares a system in one of many possible states. After, the system is transferred to a measurement device that can perform different measurements on the received system. The question now is, to what extent we can characterize the measurement device if we know the probability distribution according to which states are prepared in the preparation device.

If we bound the dimension of the systems at play it turns out that it is possible to give characterizations in certain cases similar to those in the fully device independent scenario. Because of the assumption about the fixed dimension of the physical systems, this certification task has been termed *semi-device independent* certification.

We remark, that in the following discussion, the term "certification" will be used in more loosely. It will be used (as is common in previous work e. g. [FK19]) whenever it is possible to deduce certain relations for the measurements given certain measurement statistics have been observed. A prime example of a PaM scenario is a *quantum random access code* (QRAC) (see [ALMO08] for a more thorough introduction than is given here).

8.1 QRACs

A QRAC is a protocol with which Alice is capable of encoding a classical n-dit string $x \in [d]^n$ into m qudits that she sends to Bob. Bob can then use the protocol to recover the yth dit of x with a probability of at least $p > \frac{1}{d}$ (see Figure 15). The reason for requiring p to be strictly larger than $\frac{1}{d}$ is that this can always be achieved by simply guessing. More formally,

Definition 48. (*QRAC*). An $n^d \xrightarrow{p} m$ QRAC is an encoding map $x \mapsto \varrho_x \in \mathcal{D}(\mathbb{C}^{d^m})$ for all $x \in [d]^n$, and n d-outcome POVMs, $\left\{B_b^y : b \in [d]\right\}_{y\in[n]}$, such that $\mathrm{Tr}[B_b^y \varrho_x] \geq p > \frac{1}{d}$ for all x, y, b
•

The QRAC protocol is illustrated in 15. One can consider several figures of merit.

The most common ones are the worst case success probability (WCSP) and the average success probability (ASP). In a $n^d \to m$ QRAC we will denote the WCSP by p and the ASP by $\bar{p}$ and include this in the notation for the protocol itself i. e. $n \xrightarrow{p} m$ means a protocol with WCSP p and likewise $n \xrightarrow{\bar{p}} m$ means a protocol with ASP $\bar{p}$. We will omit this specification when it is not needed. When $d = 2$ we will sometimes use the term binary QRAC. These have been studied the most.

The definition of a QRAC is given in terms of the WCSP. The reason for this is merely that we would like to make sense of a notion of existence of QRACs. We will however, for the most part consider the ASP. We assume in the following that the input string as well as the requested bit on Bob's side are uniformly distributed. The average success probability ASP of a QRAC is then,

$$\bar{p} := \frac{1}{nd^n} \sum_{bxy} p(b = x_y|xy) = \frac{1}{nd^n} \sum_{bxy} \mathrm{Tr}[B_b^y \varrho_x]. \tag{184}$$

Before we move on to our main result of this section, we will review some well-known facts about the simplest QRACs, namely $n^{d=2} \to 1$ QRACs. Since the prepared states are qubits it is possible to visualize QRACs on the Bloch sphere (see Figure 16).

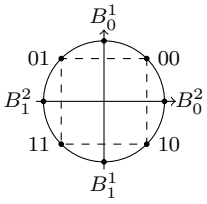


Figure 16: *The optimal* $2^{d=2} \to 1$ *QRAC.*

In the case of a $2^{d=2} \to 1$ QRAC the 4 2-bit strings can be encoded into an inscribed square in a two-section of the Bloch sphere. The binary measurements can then be chosen as antipodal Bloch vectors through the midpoints of the edges as in Figure 16 [ANTSV02]. For a $3^{d=2} \to 1$ QRAC the construction is similar using a cube instead of a square (attributed to Chuang).

Notice, that due to Lemma 42 we can immediately conclude that the measurements of the QRACs constructed above are MOMs. As we saw earlier, since the dimension of the systems is prime, these are automatically MUBs. The ASP of the QRACs constructed above is $\frac{1}{2} + \frac{1}{2\sqrt{n}}$ which turns out to be optimal. Now, one could ask, if it is possible to make the opposite conclusion i. e. based on observing the optimal ASP, can we then conclude that the measurement device performs MUBs? In [TKV+18] the authors confirm that this is indeed the case for the $2^{d=2} \to 1$ QRAC. This result was later improved in [FK19] so that it included any $d \geq 2$ i. e.

Theorem 49. *(MUB certification,[FK19]) Any* $2^d \xrightarrow{\bar{p}} 1$ *QRAC obeys*

$$\bar{p} \leq \frac{1}{2} + \frac{1}{2\sqrt{d}}. \tag{185}$$

The bound can only be attained if Bob's measurements constitute a pair of rank-1 MUBs. Conversely, for any pair of rank-1 MUBs, one can find encoding states such that the upper bound is attained. This certification is noise-robust.

It is interesting to investigate to which extent such a result can be generalized to larger values of m. This could potentially lead to experimental investigations about the existence of MUBs in nonprime power dimensions. If one could upper bound the performance of QRACs given non-existence of a certain number of MUBs and then experimentally show a violation of this bound.

Unfortunately, the result in Theorem 49 is not generalizable to larger QRACs as we will prove. In [MS22b] the following was shown,

Theorem 50. *(Mancinska, S. [MS22b]) Any $n^{d=2} \xrightarrow{\bar{p}} m$ QRAC obeys*

$$\bar{p} \leq \tfrac{1}{2} + \tfrac{1}{2}\sqrt{\tfrac{2^{m-1}}{n}} =: w_{n,m}. \tag{186}$$

This bound is reached only if Bob's measurements are MOMs.

Of course the exact formulation of the Theorem in [MS22b] was different. However, the characterization given in [MS22b] of the measurements of QRACs that reach the bound $w_{n,m}$ corresponds exactly to the MOM property. Unlike, the result in Theorem 49 one cannot make a completeness statement as in Theorem 49 i. e. there exist sets of n MOMs for which it is impossible to reach the upper bound in (186). This is due to certain requirements on the Bloch vector configurations for the encoding states that have to be fulfilled as well (see [MS22b] Corollary 12).

The following optimal binary QRACs are known,

$$\left\{2^{d=2} \xrightarrow{w_{2,1}} 1,\ 3^{d=2} \xrightarrow{w_{3,1}} 1,\ 3^{d=2} \xrightarrow{w_{3,2}} 2\ 4^{d=2} \xrightarrow{w_{4,2}} 2,\ 5^{d=2} \xrightarrow{w_{5,2}} 2,\ 6^{d=2} \xrightarrow{w_{6,2}} 2\right\}. \tag{187}$$

The analytical $3^{d=2} \xrightarrow{w_{3,2}} 2$ QRAC was found in [IR18]. The $5 \xrightarrow{w_{5,2}} 2$ QRAC is numerically obtained in [IR18]. As can easily be shown (we will do this in the Example below), the optimal $4^{d=2} \xrightarrow{w_{4,2}} 2$ QRAC can be constructed by concatenation of two optimal $2^{d=2} \xrightarrow{w_{2,1}} 1$ QRACs. Likewise, the optimal $6^{d=2} \xrightarrow{w_{6,2}} 2$ QRACs can be constructed by concatenation of two optimal $3^{d=2} \xrightarrow{w_{3,1}} 1$ QRACs. This makes it impossible to strengthen the MOM characterization in Theorem 50 to for example MUMs as the following example will show.

Example 51. Consider a $2^{d=2} \to 1$ QRAC with the POVMs $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ associated with measuring the first bit and $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ associated with measuring the second bit. These correspond to a pair of MUBs with which we, according to Theorem 49, can achieve the bound in (185). Let ϱ_{00}, ϱ_{01}, ϱ_{10} and ϱ_{11} be optimal encoding states i. e. such that the bound in (185) is saturated. Concatenating this protocol with itself results in encoding states $\varrho_{x_1x_2} \otimes \varrho_{x_3x_4}$ and POVMs,

$$\{|0\rangle\langle 0| \otimes \mathbb{1}, |1\rangle\langle 1| \otimes \mathbb{1}\},\ \{|+\rangle\langle +| \otimes \mathbb{1}, |-\rangle\langle -| \otimes \mathbb{1}\}, \tag{188}$$

Regime m / n	1 2,3	2 ≤ 6	2 > 6	3 ≤ 15	3 > 15	≥ 4 any n
Strictest bound	$w_{n,m}$	$w_{n,m}$	$w_{n,m}$	Nayak	$w_{n,m}$	Nayak
Tight bound	yes	yes	?*	?	?	?

Figure 17: **Numerical data obtained in [IR18] suggests that bound in (186) ceases to be tight. This is partially explained in [MS22b] (see Corollary 12). By 'Strictest bound' we mean the strictest known bound. By 'Tight bound' we mean whether the strictest knonw bound is tight.*

associated with the first two bits, and

$$\{\mathbb{1} \otimes |0\rangle\langle 0|, \mathbb{1} \otimes |1\rangle\langle 1|\}, \ \{\mathbb{1} \otimes |+\rangle\langle +|, \mathbb{1} \otimes |-\rangle\langle -|\} \tag{189}$$

associated with the last two bits. By this construction one obtains a $4^{d=2} \xrightarrow{w_{2,1}} 2$ and since $w_{2,1} = w_{4,2}$ this is optimal. It is easy to check that these are indeed *not* MUMs but only MOMs.
•

We remark also that certain other general limitations of $n^{d=2} \to m$ QRACs have been established. In [HIN+06] it is shown that an $n^{d=2} \to m$ QRAC exists (in terms of the WCSP being strictly larger than a half) only if $n < 4^m$. In [INRY07] this bound is shown to be tight in the sense that an $n^{d=2} \to m$ QRAC exists if and only if $n \leq 4^m - 1$. Furthermore, [Nay99] shows

Theorem 52. *(Nayak bound,[Nay99]) For any $n^{d=2} \to m$ QRAC, the bound*

$$m \geq (1 - H(p))n \tag{190}$$

holds, where $H(p)$ is the binary entropy function

$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p). \tag{191}$$

For any $n^{d=2} \to m$ QRAC with $m = 1, 2$ the bound in [MS22b] is stricter than the Nayak bound. It is clear, however, that the bound in (186) must exceed the Nayak bound for larger values of m due to the exponential factor in (186). For all $m > 3$ Nayak's bound is tighter. The case of $m = 3$ can be consider a transition case as Nayak's bound is the tightest for n up to 15 whereas for n larger or equal to 16 (186) is the tightest. Furthermore, we remark that the numerical data obtained in [IR18] suggests that the bound in (186) ceases to be tight when $m = 2$ and $n > 6$. This phenomenon is partially explained in [MS22b] (Corollary 12). This discussion is summarized in Figure 17.

By a straightforward generalization of Example 51 one can obtain $(2m)^{d=2} \xrightarrow{w_{2,1}} m$ and $(3m)^{d=2} \xrightarrow{w_{3,1}} m$ QRACs. These turned out to be optimal for $m = 2$. It is tempting to speculate whether concatenation of identical, optimal QRACs in

general results in optimal QRACs. Under the assumption that this is true, it is reasonable to conjecture (as in [MS22b]), that any $n^{d=2} \xrightarrow{\bar{p}} m$ QRAC fulfills

$$\bar{p} \leq \frac{1}{2} + \frac{1}{2}\sqrt{\frac{m}{n}}. \tag{192}$$

If this is the case one could also imagine that the strongest certification that is possible in general for the measurements of a QRAC is the MOM property.

9 Discussion, conclusion and open problems

In this section we collect the results we have obtained in the preceding chapters. We also discuss possible scopes for further research. For the subsequent discussion, it is convenient to make the following definitions:

Definition 53. Let $m_a, m_b, n_a, n_b \in \mathbb{N}$ be the question/answer set cardinalities. We define the following sets:

(i) $\mathcal{C}_{sts}(m_a, m_b, n_a, n_b)$: Set of quantum correlations that self test a state.

(ii) $\mathcal{C}_{st}(m_a, m_b, n_a, n_b)$: Set of quantum correlations that are self tests.

(iii) $\mathcal{C}_{rst}(m_a, m_b, n_a, n_b)$: Set of quantum correlations that are robust self tests.

(iv) $B_{sts}(m_a, m_b, n_a, n_b)$: Set of Bell inequalities that self test a state.

(v) $B_{st}(m_a, m_b, n_a, n_b)$: Set of self testing Bell inequalities.

(vi) $B_{rst}(m_a, m_b, n_a, n_b)$: Set of robust self testing Bell inequalities.

•

Remark, once again, that we will not specify the question and answer set cardinalities when we do not need to. As mentioned earlier, it is shown in [GKW+18] that $\mathcal{C}_{st} \subseteq \mathrm{Ext}(\mathcal{C}_q)$. The leading question of this discussion section will be which other set inclusions one can find among all the different sets we have introduced thus far.

The nonlocal game $\mathcal{G}_{\mathrm{MUM}}$ shows that we in fact have $\mathcal{C}_{st} \subsetneq \mathrm{Ext}(\mathcal{C}_q)$. More precisely, Theorem 47 shows that

$$\mathrm{Exp}\left(\mathcal{C}_q(16,3,3,5)\right) \neq \mathcal{C}_{st}\left((16,3,3,5)\right) \tag{193}$$

We noted also that $\mathcal{G}_{\mathrm{MUM}}$ is still a self test for the maximally entangled state [GKW+18]. Based on this we pose the following question:

Question 54. *Is every extreme point of $\mathcal{C}_q$ a self test for a state, i. e. do we have $Ext(\mathcal{C}_q) \subseteq \mathcal{C}_{sts}$?*

If true, we would even have strict inclusion since, for example, $\mathcal{G}_\perp$ in Sec. 5.6 shows $\mathrm{Ext}(\mathcal{C}_q) \neq \mathcal{C}_{sts}$. It is evident that if we are only looking to self test a state and not the measurements we have a much larger subset of $\mathcal{C}_q$ to choose from. These correlations are not confined to a subset of extreme points. They may, as we have seen be nonextreme. We are not even aware of any proof stating that they must be confined to boundary points. We pose therefore the question

Question 55. *Is every correlation that self tests a state a boundary point in $\mathcal{C}_q$?*

In [MS22a] the authors found a nonlocal game, we denote it here $\mathcal{G}_\vee$, with the property that its game value can be achieved by several inequivalent states thus answering an open question in [Kan20]. It is not clear to us whether $\omega^*(\mathcal{G}_\vee)$ is achieved in an extreme point. One could for example prove that it is achieved by a unique correlation such that it is an exposed point and therefore an extreme point. If this were the case Question 54 would be answered in the negative.

By definition and, for example the weak self testing property of $\mathcal{G}_\perp$, we have the following inclusions,

$$\mathcal{C}_{rst} \subseteq \mathcal{C}_{st} \subsetneq \mathcal{C}_{sts}. \tag{194}$$

The natural question is,

Question 56. *Do $\mathcal{C}_{rst}$ and $\mathcal{C}_{st}$ coincide?*

We have by definition and the above discussion,

$$B_{rst} \subseteq B_{st} \subsetneq B_{sts}. \tag{195}$$

So the counterpart of Question 56 in terms of Bell inequalities is whether the first inclusion in (195) is strict. This turns out to be the case. In [MS22a] the authors exhibit a nonlocal game, let us denote it here by $\mathcal{G}'_\vee$, which is a self test but not robust to noise: The game has the peculiar property that one can get arbitrarily close to the game value, $\omega^*(\mathcal{G}'_\vee)$, by states and measurements far away from states and measurements that are equivalent with the ones that realize $\omega^*(\mathcal{G}'_\vee)$. This result has the following geometric interpretation: Since $\mathcal{G}'_\vee$ is a self test, the maximal violation must happen in an exposed point u. However, we must have that the closure C_{qa} contains at least one other correlation which induces maximality w. Hence, in $\mathcal{C}_{qa}$ the line segment connecting u and w consists of maximizers of the Bell inequality corresponding to $\mathcal{G}'_\vee$ (see Figure 18).

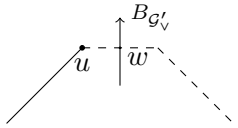


Figure 18: *The maximal violation happens in $u \in \mathcal{C}_q$. However in the closure $\mathcal{C}_{qa}$ maximality happens in a line segment.*

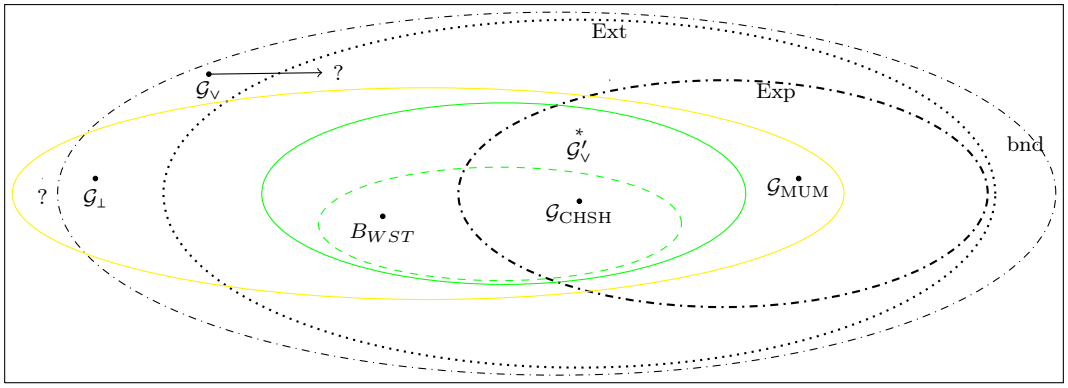


Figure 19: *Summary of inclusions. Yellow ellipse, $\mathcal{C}_{sts}$: Weakly self testing correlations. Green ellipse, $\mathcal{C}_{st}$: Strongly self testing correlations. Green dashed ellipse, $\mathcal{C}_{rst}$: Robustly, strongly self testing correlations. Note: The game $\mathcal{G}'_\vee$ only shows separation at the level of Bell inequalities.*

We have seen that some properties, e. g. closure, of $\mathcal{C}_q$ depend on m_a, m_b, n_a and n_b. In particular $\mathcal{C}_q(2,2,2,2)$ is closed. Based on this observation, is it possible to show that $B_{rst}(2,2,2,2) = B_{st}(2,2,2,2)$?

Recall, that in [Kan20], a Bell inequality, which we in this work denoted B_{WST}, was exhibited which is maximally violated in a line segment. The maximal violation certifies a maximally entangled state. The endpoints of this line segment (corresponding to a nonexposed extreme point) were shown to admit a full, robust self testing statement with respect to correlations.

In Figure 19 we have collected the content of the discussion. We illustrate the differences between the different sets we have introduced with the outer rectangle being $\mathcal{C}_q$. We have included Bell inequalities (many of which have been treated in this thesis), that show all the known set separations. We have also included the game, $\mathcal{G}'_\vee$ although this only shows separation at the level of Bell inequalities. We do not know if there is a separation here (see Question 56) at the level of correlations. We do not know if the game $\mathcal{G}_\vee$ which does not certify a state, is optimized in an extreme point (see Question 54). If true Question 54 would have a negative answer. We do not know if there exist interior points of $\mathcal{C}_q$ that self test a state (see Question 55).

We can conclude that there is no comparability between self testing correlations and the different classes of boundary points (such as extreme points and exposed points) coming from standard convex geometry in general. We only point out that it is still possible that every extreme point self tests a state. It would be interesting to investigate whether it is possible to compare such sets in case m_a, m_b, n_a are sufficiently small.

Acknowledgement. I would like to sincerely thank my supervisors for the help I have received while writing my thesis and for all the very delightful and inspira-

tional discussions we have had along the way. I owe my deepest gratitude to my girlfriend Alice Manganaro for always being by my side.

References

[ALMO08] Andris Ambainis, Debbie Leung, Laura Mancinska, and Maris Ozols. Quantum random access codes with shared randomness, 2008.

[AM16] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540:213–219, 12 2016.

[ANTSV02] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, and Umesh Vazirani. Dense quantum coding and quantum finite automata. *J. ACM*, 49(4):496–511, jul 2002.

[Ara99] P.K. Aravind. Impossible colorings and bell's theorem. *Physics Letters A*, 262(4):282–286, 1999.

[Ara02] P. K. Aravind. A simple demonstration of bell's theorem involving two observers and no probabilities or inequalities, 2002.

[Ara04] P. K. Aravind. Quantum mysteries revisited again. *American Journal of Physics*, 72(10):1303–1307, 2004.

[Bel64] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964.

[Bel66] John S. Bell. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.*, 38:447–452, Jul 1966.

[Ben07] Ingemar Bengtsson. Three ways to look at mutually unbiased bases. *AIP Conference Proceedings*, 889(1):40–51, 2007.

[BH07] Paul Butterley and William Hall. Numerical evidence for the maximum number of mutually unbiased bases in dimension six. *Physics Letters A*, 369(1):5–8, 2007.

[BW08] Stephen Brierley and Stefan Weigert. Maximal sets of mutually unbiased quantum states in dimension 6. *Phys. Rev. A*, 78:042312, Oct 2008.

[BW09] Stephen Brierley and Stefan Weigert. Constructing mutually unbiased bases in dimension six. *Phys. Rev. A*, 79:052316, May 2009.

[CGS17] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. *Nature communications*, 8:15485, May 2017.

[Che18] Lin Chen. Mutually unbiased bases in dimension six containing a product-vector basis. *Quantum Information Processing*, 17,198, 2018.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[CLS17] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017.

[CM14] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming*, pages 320–331, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[CMMN20] David Cui, Arthur Mehta, Hamoon Mousavi, and Seyed Sajjad Nezhadi. A generalization of CHSH and the algebraic structure of optimal strategies. *Quantum*, 4:346, October 2020.

[Col20] Andrea Coladangelo. A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations. *Quantum*, 4:282, June 2020.

[Con76] A. Connes. Classification of injective factors cases II_1, II_∞, III_λ, $\lambda \neq 1$. *Annals of Mathematics*, 104(1):73–115, 1976.

[CS17] Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games, 2017. arXiv:1709.09267.

[CS20] Andrea Coladangelo and Jalex Stark. An inherently infinite-dimensional quantum correlation. *Nature Communications*, 11:3335, 07 2020.

[DEBZ10] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Zyczkowski. On mutually unbiased bases. *International Journal of Quantum Information*, 08(04):535–640, 2010.

[DPP19] Ken Dykema, Vern I. Paulsen, and Jitendra Prakash. Non-closure of the set of quantum correlations via graphs. *Communications in Mathematical Physics*, 365(3):1125–1142, February 2019.

[DW15] John Matthew Donohue and Elie Wolfe. Identifying nonconvexity in the sets of limited-dimension quantum correlations. *Phys. Rev. A*, 92:062120, Dec 2015.

[FK19] Máté Farkas and J ędrzej Kaniewski. Self-testing mutually unbiased bases in the prepare-and-measure scenario. *Phys. Rev. A*, 99:032316, Mar 2019.

[FKN22] Máté Farkas, Jędrzej Kaniewski, and Ashwin Nayak. Mutually unbiased measurements, hadamard matrices, and superdense coding, 2022. arXiv:2204.11886.

[Fu22] Honghao Fu. Constant-sized correlations are sufficient to self-test maximally entangled states with unbounded dimension. *Quantum*, 6:614, January 2022.

[GH17] W T Gowers and O Hatami. Inverse and stability theorems for approximate representations of finite groups. *Sbornik: Mathematics*, 208(12):1784–1817, dec 2017.

[GKW+18] Koon Tong Goh, Jędrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani. Geometry of the set of quantum correlations. *Phys. Rev. A*, 97:022104, Feb 2018.

[Gow16] W T Gowers. Generalizations of fourier analysis, and how to apply them. *American Mathematical Society (AMS)*, 54(1):1–44, Sep 2016. doi: 10.1090/bull/1550.

[Gra04] Markus Grassl. On sic-povms and mubs in dimension 6, 2004. arXiv:quant-ph/0406175.

[Haa97] U. Haagerup. Orthogonal maximal abelian *-subalgebras of the n × n matrices and cyclic *n*-roots. *Operator Algebras and Quantum Field Theory (S. Doplicher et al., eds.)*, pages 296—-322, 1997.

[HIN+06] Masahito Hayashi, Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. (4, 1)-quantum random access coding does not exist. In *2006 IEEE International Symposium on Information Theory*, pages 446–450, 2006.

[HL21] Nicholas Gauguin Houghton-Larsen. A mathematical framework for causally structured dilations and its relation to quantum self-testing, 2021. arXiv:2103.02302.

[HRZ20] Paweł Horodecki, Łukasz Rudnicki, and Karol Zyczkowski. Five open problems in quantum information, 2020.

[HW20] Daniel Hug and Wolfgang Weil. *Lectures on Convex Geometry*. Graduate Texts in Mathematics, 286. Springer International Publishing, Cham, 1st ed. 2020. edition, 2020.

[INRY07] Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. Unbounded-error classical and quantum communication complexity. In Takeshi Tokuyama, editor, *Algorithms and Computation*, pages 100–111, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[IR18] Takashi Imamichi and Rudy Raymond. 'Constructions of Quantum Random Access Codes'. *Asian Quantum Information Symposium (AQIS)*, 2018.

[JNV+21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Mip* = re. *Commun. ACM*, 64(11):131–138, oct 2021.

[Kan17] Jędrzej Kaniewski. Self-testing of binary observables based on commutation. *Phys. Rev. A*, 95:062323, Jun 2017.

[Kan20] Jędrzej Kaniewski. Weak form of self-testing. *Phys. Rev. Research*, 2:033420, Sep 2020.

[Kir93] Eberhard Kirchberg. On non-semisplit extensions, tensor products and exactness of groupc*-algebras. *Inventiones mathematicae*, 112:449–489, 1993.

[KS68] Simon Kochen and Ernst Specker. The problem of hidden variables in quantum mechanics. *Indiana Univ. Math. J.*, 17:59–87, 1968.

[Mas06] Lluís Masanes. Asymptotic violation of bell inequalities and distillability. *Phys. Rev. Lett.*, 97:050503, Aug 2006.

[Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65:3373–3376, Dec 1990.

[MNP21] Laura Mančinska, Thor Gabelgaard Nielsen, and Jitendra Prakash. Glued magic games self-test maximally entangled states, 2021.

[MPS21] Laura Mančinska, Jitendra Prakash, and Christopher Schafhauser. Constant-sized robust self-tests for states and measurements of unbounded dimension, 2021.

[MS22a] Laura Mančinska and Simon Schmidt. A nonrobust self test and games that do not self test states. 2022. unpublished manuscript shared with me in personal communication.

[MS22b] Laura Mančinska and Sigurd Storgaard. The geometry of bloch space in the context of quantum random access codes. *Quantum Information Processing*, 21, 04 2022.

[MY98] Dominic Mayers and Andrew Chi-Chih Yao. Quantum cryptography with imperfect apparatus. *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pages 503–509, 1998.

[MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4(4):273–286, July 2004.

[MYS12] M McKague, T H Yang, and V Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, oct 2012.

[Nay99] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039)*, pages 369–376, 1999.

[Oza13] Narutaka Ozawa. About the connes embedding conjecture. *Japanese Journal of Mathematics*, 8:147–183, 2013.

[Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3):107–108, 1990.

[PR94] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, March 1994.

[RLE11] Philippe Raynal, Xin Lü, and Berthold-Georg Englert. Mutually unbiased bases in six dimensions: The four most distant bases. *Phys. Rev. A*, 83:062303, Jun 2011.

[RTHH16] Ravishankar Ramanathan, Jan Tuziemski, Michał Horodecki, and Paweł Horodecki. No quantum realization of extremal no-signaling boxes. *Phys. Rev. Lett.*, 117:050401, Jul 2016.

[ŠB20] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, September 2020.

[Slo19a] William Slofstra. The set of quantum correlations is not closed. *Forum of Mathematics, Pi*, 7:e1, 2019.

[Slo19b] William Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. *Journal of the American Mathematical Society*, 2019.

[SVW16] Jamie Sikora, Antonios Varvitsiotis, and Zhaohui Wei. Minimum dimension of a hilbert space needed to generate a quantum correlation. *Phys. Rev. Lett.*, 117:060401, Aug 2016.

[SW08] V. B. Scholz and R. F. Werner. Tsirelson's problem, 2008. arXiv:0812.4305.

[TFR+21] Armin Tavakoli, Máté Farkas, Denis Rosset, Jean-Daniel Bancal, and Jędrzej Kaniewski. Mutually unbiased bases and symmetric informationally complete measurements in bell experiments. *Science Advances*, 7(7):eabc3847, 2021.

[TKV+18] Armin Tavakoli, J ędrzej Kaniewski, Tamás Vértesi, Denis Rosset, and Nicolas Brunner. Self-testing quantum states and measurements in the prepare-and-measure scenario. *Phys. Rev. A*, 98:062307, Dec 2018.

[Tsi93] B. S. Tsirelson. Some results and problems on quantum bell-type inequalities. *Hadronic J. Suppl.*, 8(4):329–345, 1993.

[Tsi06a] Tsirelson. 2006. http://qig.itp.uni-hannover.de/qiproblems/33 visited May 8th 2022.

[Tsi06b] Boris Tsirelson. Bell inequalities and operator algebras, 2006. see http://web.archive.org/web/20090414083019/http://www.imaph.tu-bs.de/qi/problems/33.html, last visited May 30th.

[Wer01] R F Werner. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, 34(35):7081–7094, aug 2001.