Some Aspects of Noncommutativity in Polynomial Optimization

Seyyed Hamoon Mousavi Haji

Submitted in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
under the Executive Committee
of the Graduate School of Arts and Sciences

COLUMBIA UNIVERSITY

2023

Abstract

Some Aspects of Noncommutativity in Polynomial Optimization

Seyyed Hamoon Mousavi Haji

Most combinatorial optimization problems from theoretical computer science have a natural framing as optimization of polynomials in commuting variables. Noncommutativity is one of the defining features of quantum mechanics. So it is not surprising that noncommutative polynomial optimization plays an equally important role in quantum computer science. Our main goal here is to understand the relative hardness of commutative versus noncommutative polynomial optimization. At a first glance it might seem that noncommutative polynomial optimization must be more complex. However this is not always true and this question of relative hardness is substantially more subtle than might appear at the outset.

First in this thesis we show that the general noncommutative polynomial optimization is complete for the class Π_2; this class is in the second level of the arithmetical hierarchy and strictly contains both the set of recursively enumerable languages and its complement. On the other hand, commutative polynomial optimization is decidable and belongs to PSPACE. We then provide evidence that for polynomials arising from a large class of constraint satisfaction problems the situation is reversed: the noncommutative polynomial optimization is an easier computational problem compared to its commutative analogue.

A second question we are interested in is about whether we could extract good commutative solutions from noncommutative solutions? This brings us to the second theme of this thesis which is about understanding the algebraic structure of the solutions of noncommutative polynomial

optimization. We show that this structural insight then could shed light on the optimal commutative solutions and thereby paves the path in understanding the relationships between the commutative and noncommutative solutions.

Here we first use the sum-of-squares framework to understand the algebraic relationships that are present between operators in any optimal noncommutative solution of a class of polynomial optimization problems arising from certain constraint satisfaction problems. We then show how we can design approximation algorithms for these problems so that some algebraic structures of our choosing is present. Finally we propose a rounding scheme for extracting good commutative solutions from noncommutative ones.

Table of Contents

List of Figures

List of Tables

Acknowledgements

First and foremost I am extremely grateful to my advisor Henry Yuen whose support never wavered through the years and who set a wonderful example for leading scientific projects with marvelous curiosity, respect, inclusivity, and patience. I started the Ph.D. in January 2019 at the University of Toronto and then moved to Columbia University in the city of New York in February 2021. It was a few very joyful years at the theoretical computer science groups at both these universities and I have the incredibly warm and welcoming graduate students and faculties of these two amazing institutions to thank for it. Among these academic friends I especially like to thank Lily Li, one of my favorite running buddies, and Deeksha Adil. Next, I would like to thank two of my most wonderful collaborators Seyed Sajjad Nezhadi and Taro Spirig. I cannot possibly thank you enough for those happy countless hours we passionately discussed the problems that finally formed the backbone of this thesis. I hope we continue our friendship and collaboration for many years to come. I am also hugely indebted to my coauthors David Cui and Arthur Mehta, and my most recent collaborator Eric Culf. Outside of academia, I have made lifelong friends at the University of Toronto's Triathlon Team and the Dashing Whippets Running Team in New York City. I am so lucky to have run and biked Toronto and New York City with all of you amazing teammates.

Introduction

This thesis studies the problem of noncommutative polynomial optimization. One reason ordinary polynomials play an important role in theoretical computer science is that many combinatorial optimization problems can be formulated as the optimization of polynomials in commuting variables. A famous example is the weighted Max-Cut problem. Framed as a polynomial optimization, Max-Cut is essentially the problem

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} x_i x_j \\ \text{subject to:} \quad & x_i \in \{\pm 1\}. \end{aligned} \tag{0.0.1}$$

Similarly many quantities in quantum information can be formulated as a noncommutative polynomial optimization problem. One prominent such quantity is the entangled value of nonlocal games, another topic of interest of this thesis. Indeed the problem of noncommutative polynomial optimization and the problem of calculating the entangled value of nonlocal games are essentially equivalent. That being said often times it is easier to work with one rather than the other. We see examples where it is easier to work with nonlocal games formulation when trying to understand noncommutative polynomial optimization better, and we will see example the other way around.

Aside from its direct importance in quantum information, noncommutative polynomial optimization can reveal deep insights in the study of classical commutative problems. For example the first step in the famous Goemans-Williamson approximation algorithm for Max-Cut is to solve the easier noncommutative analogue of (0.0.1)

$$\begin{aligned} \text{maximize:} \quad & \operatorname{tr}\big(\textstyle\sum w_{ij} X_i X_j\big) \\ \text{subject to:} \quad & X_i^2 = X_i^* X_i = I. \end{aligned} \tag{0.0.2}$$

Here $\operatorname{tr}(\cdot)$ is the dimension-normalized trace map, $*$ is the adjoint, and variables X_i are allowed to be Hermitian unitary operators of any dimension. The noncommutative problem is clearly a relaxation of the classical problem. Whereas the commutative polynomial optimization (0.0.1) is famously NP-hard, noncommutative polynomial optimization (0.0.2) is easy because it is a semidefinite program in disguise.[1]

Intuitively, however, we expect that the general noncommutative polynomial optimization problem to be hard because variables can be operators of any dimension. At which dimension can we stop searching for the optimal solution to our optimization problem? The answer is we can never be sure. This is the content of the first part of the thesis. In Chapter 1, using tools from the study of nonlocal games, we show that noncommutative polynomial optimization is not only uncomputable but that it is strictly harder than even the halting problem. In contrast, using the existential theory of reals, it is known that commutative polynomial optimization is in PSPACE [1].

A concept that plays a significant role in the first chapter is the notion of self-testing of nonlocal games. This property that certain noncommutative polynomials have is, informally speaking, about the presence of a unique *canoncical* solution. In Chapter 2, we again study self-testing in a subclass of nonlocal games that generalizes the famous CHSH game. This time however we study self-testing from an entirely different angle borrowing tools from noncommutative sum-of-squares framework and representation theory.

As we indicated so far, we want to understand the relative hardness of the commutative versus noncommutative polynomial optimization. This is a theme that derives much of this work. We just saw that in the case of Max-Cut the noncommutative problem is easier to solve. We also mentioned

[1] Although Goemans-Williamson algorithm is never presented in this way in classical theoretical computer science, this framing is very much folklore in quantum information circles through its connection to XOR nonlocal games.

that the noncommutative optimization, in its most general form, is harder that the commutative analogue. So the question of relative hardness is really subtle. There is a regime in which the noncommutative problem is easier and then there is a regime in which the commutative problem is easier. We make attempts in identifying these regimes.

After characterizing the regime where noncommutativity makes computation easier, can we then hope to gain some information about the solutions to the commutative problem from the noncommutative solution? The noncommutative solution consists of a bunch of operators acting on some, possibly large-dimensional, Hilbert space. Can we extract a good classical commutative solution from these operators? This is the second theme underlying this thesis.

Historically, when designing approximation algorithms for commutative polynomial optimization, one relaxes the variables to take values in some vector space. The original domain of the variables is often time a finite field. After solving the relaxation, one then must devise a rounding scheme to obtain a good scalar solution from the vector solution. We propose a different approach: Can we relax the scalars to operators and then round the operators back to scalars? The operator relaxation would be closer to the original domain in two respects. First the value of the operator relaxation is closer to the value of the original problem when compared with the vector relaxation. Secondly the ring of operators preserve some of the algebraic structure of the original domain, in the sense that we can still add and multiply (a property that we loose in the vector relaxation). Could we take advantage of these? This is what we study in Chapter 3.

These all suggest that there is this beautiful twist in the story of commutative versus noncommutative polynomial optimization: noncommutativity is not always a curse and it can sometimes be viewed as a powerful resource not too different from the way randomness and entanglement are viewed as resources when performing computational tasks.

So far we saw one example of this phenomenon: The original Max-Cut problem (0.0.1) is NP-hard, but the noncommutative version (0.0.2) can be solved in polynomial-time. Even more interestingly, the noncommutative solution reveals good classical solutions via rounding techniques. We discuss further examples along this line in Chapter 3. However, studying the literature, we are aware of at least a few other interesting examples of this phenomenon from slightly different angles.

One example of “noncommutativity as a resource” is the self-testing property we mentioned before. Self-testing does not have a satisfying analogue in the commutative world but it has been a rich area of study in quantum information theory. Informally it allows an experimenter to interact classically with a black box quantum system and to test that a specific entangled state was present and a specific set of measurements were performed. Therefore some of the earliest and most widely studied tests of quantumness rely heavily on self-testing results. This fundamental property, present in some nonlocal games, has also led to the introduction of device-independent cryptography among many other applications. This is the positive side of self-testing. On the other hand, self-testing is also the reason why noncommutative polynomial optimization is hard. The core of the argument we present in Chapter 1 for hardness of noncommutative polynomial optimization is indeed based on self-testing. In fact if self-testing was featured in the commutative world, as much as it is present in the noncommutative world, then we could have not capped the complexity of commutative polynomial optimization to PSPACE.

Yet another elegant example of “noncommutativity as a resource” comes from the theory of real algebraic geometry. We know from Hilbert’s 17th Problem and its resolution that positive commutative polynomials may not be sum of squares. On the other hand, a seminal result of Helton [2] shows that positive noncommutative polynomials are always sum of squares. This implies that if $p(X_1, \dots, X_n)$ is any polynomial in noncommuting variables, there is a finite sum-of-square certificate for the value $\max \|p(X_1, \dots, X_n)\|$ where $\| \cdot \|$ is the operator norm. On the other hand if we enforce that X_i’s commute, no such certificate of finite size may exist. In short, noncommutative polynomials seem to be better suited for the sum-of-squares framework and semidefinite programming techniques.[2]

Guided by these observations we mentioned so far, in this thesis we look for computational

[2] We note that Helton’s result does not contradict the undecidability of noncommutative polynomial optimization. The objective function in noncommutative polynomial optimization as we formulated it here involves trace rather than operator norm, for example as in (0.0.2). Helton’s result does not extend to trace positivity of polynomials [3] and therefore more intricate arguments are needed to deal with trace optimization.

settings in which noncommutativity can be exploited as a resource. There are some evidence that a noncommutative variant of Max-2-Lin constraint satisfaction problems (CSP) lie in this sweet spot where noncommutativity actually makes things easier. Max-2-Lin are those CSPs where constraints are linear equations and each constraint only involves two variables.

In Chapter 2, we study the effectiveness of sum-of-squares framework for solving a subclass of noncommutative Max-2-Lin CSPs. In Chapter 3, we develop an algebraic framework for designing approximation algorithms to noncommutative Max-2-Lin CSPs.

So far we gave a quick introduction to themes of this thesis. Let us now give a brief overview of the results and some of the tools that are used.

In the first chapter we investigate the connection between the complexity of nonlocal games and the arithmetical hierarchy, a classification of languages according to the complexity of arithmetical formulas defining them. It was shown by Ji, Natarajan, Vidick, Wright and Yuen [4] that deciding whether the (finite-dimensional) quantum value of a nonlocal game is 1 or at most $\frac{1}{2}$ is complete for the class Σ_1 (i.e., RE). A result of Slofstra implies that deciding whether the commuting operator value of a nonlocal game is equal to 1 is complete for the class Π_1 (i.e., coRE).

We prove that deciding whether the quantum value of a two-player nonlocal game is exactly equal to 1 is complete for Π_2; this class is in the second level of the arithmetical hierarchy and corresponds to formulas of the form "$\forall x \, \exists y \, \phi(x, y)$". This shows that exactly computing the quantum value is strictly harder than approximating it, and also strictly harder than computing the commuting operator value (either exactly or approximately).

We explain how results about the complexity of nonlocal games all follow in a unified manner from a technique known as *compression*. At the core of our Π_2-completeness result is a new "gapless" compression theorem that holds for both quantum and commuting operator strategies. All previous works only study the setting of finite-dimensional quantum strategies; ours is the first to study compression of games in the commuting operator setting. Our compression theorem yields as a byproduct an alternative proof of Slofstra's result [5] that the set of quantum correlations is not closed. We also show how a "gap-preserving" compression theorem for commuting operator strategies would imply that approximating the commuting operator value is complete for Π_1. Eventually we show how these results prove the hardness result we advertised earlier for noncommutative polynomial optimization.

In the second chapter we study self-testing which was also prominently featured in the previous chapter. The most studied self-test is the CHSH game which features a bipartite system with two isolated devices. This game certifies the presence of a single EPR entangled state and the use of anti-commuting Pauli measurements. Most of the self-testing literature has focused on extending these results to self-test for tensor products of EPR states and tensor products of Pauli measurements.

Here, we introduce an algebraic generalization of CHSH by viewing it as a constraint satisfaction problem, exhibiting self-testing properties that are qualitatively different. These provide the first family of games that self-test non-Pauli operators. These games also provide a self-test for states other than the maximally entangled state.

In order to obtain our results, we exploit connections between sum of squares proofs, noncommutative ring theory, and the Gowers-Hatami theorem from approximate representation theory. A crucial part of our analysis is to introduce a sum of squares framework that generalizes the *solution group* of Cleve, Liu, and Slofstra [6]. Finally, we give a game that is not a self-test by "gluing" together two copies of the famous Magic-Square game.

In the last chapter we study approximation algorithms for Max-2-Lin CSPs and their noncommutative analogues. Max-Cut is the simplest example of Max-2-Lin. Goemans-Williamson's algorithm gives the best approximation algorithm for Max-Cut. Tsirelson's theorem gives the best algorithm for solving noncommutative Max-Cut. We examine these two theorems and propose a way of extending them to Max-2-Lin problems beyond Max-Cut.

We mentioned earlier that noncommutative polynomial optimization could reveal some insights in the study of classical commutative problems. In the last section of Chapter 3, we try to understand this phenomenon better. We propose an operator rounding scheme that takes any noncommutative solution to a CSP and produces a classical solution to the original classical CSP. We study the performance of this rounding scheme on Max-2-Lin problems and compare it with the performance of the conventional vector rounding. This seems to suggest that rounding from operators performs better, a comparison that again exhibits the phenomenon of “noncommutaitivity as a resource.”

Chapter 1: Hardness results

This chapter is taken verbatim from our paper "Nonlocal Games, Compression Theorems, and the Arithmetical Hierarchy" [7]. All authors of this work contributed equally.

1.1 Introduction

A nonlocal game describes a scenario in which a (classical) verifier plays a game with two separated, but possibly entangled, players (who we'll call Alice and Bob). In the game, the verifier samples a pair of questions (x, y) from a question distribution μ, sends x to Alice and y to Bob, and then receives answers a and b from the players. The verifier then computes a decision procedure $D(x, y, a, b)$ to determine whether the players win or lose. We assume that Alice and Bob know the question distribution and decision procedure before the game starts, and cooperatively select an entangled strategy to maximize their probability of winning.

Recent results have shown that the optimal winning probability, called the *value*, of a nonlocal game is uncomputable in general. Surprisingly, the study of the complexity of nonlocal games is also intimately tied to questions outside of complexity theory. For example, Slofstra's result about the undecidability of whether a nonlocal game has a perfect quantum strategy (i.e. a strategy that wins with probability 1) was a byproduct of his showing that the set of quantum correlations is not closed [8, 5]. As another example, the complexity-theoretic result $\mathsf{MIP}^* = \mathsf{RE}$ [4] (which implies that there is no algorithm to even *approximate* the quantum value of a nonlocal game) yields negative answers to both Tsirelson's Problem from quantum information theory and Connes' Embedding Problem from operator algebras [9, 10].

These uncomputability results for nonlocal games demonstrate that the space of quantum strategies is terribly complex — no algorithm can optimize over them, even approximately! This is already quite striking, but a closer look at these results indicates that more can be said: different computational problems for nonlocal games can be uncomputable in *incomparable ways*. To explain this we need to define two relevant models of entangled strategies.

Strategies for nonlocal games. The most general model we consider is the class of *commuting operator* strategies. Let $G = (\mathcal{X}, \mathcal{A}, \mu, D)$ denote a nonlocal game with question alphabet $\mathcal{X}$, answer alphabet $\mathcal{A}$, question distribution μ, and decision procedure $D : \mathcal{X} \times \mathcal{X} \times \mathcal{A} \times \mathcal{A} \to \{0, 1\}$. A commuting operator strategy $\mathcal{S}$ for a game G is specified by the following data: a separable Hilbert space $\mathcal{H}$, a unit vector $|\psi\rangle \in \mathcal{H}$ (called the *state*), and sets of *measurements* $A = \{A^x\}_{x \in \mathcal{X}}$ and $B = \{B^y\}_{y \in \mathcal{X}}$ acting on $\mathcal{H}$ satisfying the following:

- For all x, y, the measurements $A^x = \{A^x_a\}_{a \in \mathcal{A}}$ and $B^y = \{B^y_b\}_{b \in \mathcal{A}}$ are sets of bounded positive operators on $\mathcal{H}$, with each set summing to the identity, and
- For all x, y, a, b, the operators A^x_a and B^y_b commute.

Given questions (x, y), the probability that the players respond with answers (a, b) is given by $\langle\psi| A^x_a \, B^y_b |\psi\rangle$. The two conditions on the measurement operators above ensure that this is a valid probability distribution over $\mathcal{A} \times \mathcal{A}$, and furthermore the commutation condition ensures that the strategy is *non-signaling*, meaning that the marginal probability that a player responds with an answer only depends on their question (and not the other player's question).

The *value* of a commuting operator strategy $\mathcal{S} = (|\psi\rangle, A, B)$ in a game G is given by

$$\omega(G, \mathcal{S}) := \sum_{x,y,a,b} \mu(x, y) \cdot \langle\psi| A^x_a B^y_b |\psi\rangle \cdot D(x, y, a, b) \; .$$

The *commuting operator* value of a game G is defined as

$$\omega_{co}(G) := \sup_{\text{commuting operator } \mathcal{S}} \omega(G, \mathcal{S}).$$

Intuitively, the commuting operator value of a game represents the players' maximum success probability allowed under quantum mechanics.

An important subclass of commuting operator strategies are the *finite-dimensional* ones, i.e. where the underlying Hilbert space $\mathcal{H}$ is equal to $\mathbb{C}^d$ for some integer d. We define the *quantum value*[1] of a game G to be

$$\omega_q(G) := \sup_{\text{finite-dimensional } \mathscr{S}} \omega(G, \mathscr{S}).$$

In the finite-dimensional setting, commuting operator strategies coincide with strategies in the *tensor product model*: one can find two finite-dimensional Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$, a bipartite state $|\widetilde{\psi}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, and measurements $\{\widetilde{A}_a^x\}$ on $\mathcal{H}_A$ and $\{\widetilde{B}_b^y\}$ on $\mathcal{H}_B$ such that

$$\langle\psi|A_a^x \, B_b^y|\psi\rangle = \langle\widetilde{\psi}|\widetilde{A}_a^x \otimes \widetilde{B}_b^y|\widetilde{\psi}\rangle \ .$$

For a proof, see [11, Theorem 1]. Tensor product strategies give a natural way to model the behavior of spatially separated players, and this is perhaps the most commonly studied model of strategies for nonlocal games. General commuting operator strategies, on the other hand, do not assume that there is an *a priori* tensor product decomposition of the Hilbert space, but only that the non-signaling property is enforced via commutativity of the players' measurements. The commuting operator model of quantum correlations arise naturally in algebraic formulations of quantum field theory [11, 12].

It is easy to see that $\omega_q(G) \leq \omega_{co}(G)$. Tsirelson's Problem is essentially a question about whether $\omega_q(G) = \omega_{co}(G)$ for all games G; in other words, can all commuting operator strategies (which might be infinite dimensional) be approximated arbitrarily well by finite-dimensional ones [11]? Furthermore, it was shown that Tsirelson's Problem is equivalent to Connes' Embedding Problem, which was a long-standing question in operator algebras about the approximability of von Neumann algebras by finite-dimensional matrix algebras [9, 13, 12, 10]. As previously mentioned, these questions about finite-dimensional approximability of infinite-dimensional objects are intimately connected to questions about computability of the value of nonlocal games.

[1] The reason for this name, as opposed to "finite-dimensional value", is historical: the study of nonlocal games has largely focused on the setting of finite-dimensional strategies.

Computability of nonlocal games. We now define computational problems associated with computing the value of nonlocal games. Fix $0 \le \varepsilon < 1$ and a value type $t \in \{q, co\}$. Define two sets of nonlocal games

$$L_t^{yes} := \{G : \omega_t(G) = 1\} \qquad \text{and} \qquad L_{t,\varepsilon}^{no} := \{G : \omega_t(G) < 1 - \varepsilon\} \,.$$

These two sets are disjoint, and when $\varepsilon = 0$, the union of these two sets is all nonlocal games. These two sets give rise to a decision problem: given a nonlocal game G in the union $L_t^{yes} \cup L_{t,\varepsilon}^{no}$, decide whether G is a "yes" instance or a "no" instance.

When $\varepsilon = 0$, this decision problem corresponds to *exactly* computing either the quantum or commuting operator value. When $\varepsilon > 0$, this problem corresponds to *approximating* the value, because being able to compute $\omega_t(G)$ up to additive $\pm\frac{\varepsilon}{2}$ error allows one to decide whether $G \in L_t^{yes}$ or $G \in L_{t,\varepsilon}^{no}$. Thus we call deciding between L_t^{yes} and $L_{t,0}^{no}$ the *exact t-value problem*, and deciding between L_t^{yes} and $L_{t,\varepsilon}^{no}$ for $\varepsilon > 0$ the *approximate t-value problem* (we usually think of ε as $1/2$, but the specific value is immaterial, as long as it is strictly positive).

We summarize the results known so far about the computability of nonlocal games:

1. In [8], Slofstra showed that the exact co-value problem is hard for the class coRE, which is the complement of RE, the set of recursively enumerable languages. In other words, there exists a computable reduction from Turing machines M to nonlocal games G such that $\omega_{co}(G) = 1$ if and only if M does *not* halt.

   Furthermore, the exact co-value problem is contained in coRE due to the existence of a semidefinite programming hierarchy that converges from above to the commuting operator value of a given nonlocal game [14, 15]. Thus the exact co-value problem is complete for coRE.

2. In [5], Slofstra showed that the exact q-value problem is also hard for coRE. However, no upper bound on the complexity of the exact q-value problem was given.

3. In [4], Ji, Natarajan, Vidick, Wright and Yuen showed that the approximate q-value problem is hard for RE. In other words, there exists a computable reduction from Turing machines M to nonlocal games G such that if M halts then $\omega_q(G) = 1$, otherwise $\omega_q(G) \leq \frac{1}{2}$.

   Furthermore, the approximate q-value problem is contained in RE due to the fact that a brute-force enumeration algorithm can find a finite-dimensional strategy that succeeds with probability arbitrarily close to 1, provided that $\omega_q(G) = 1$. Thus, the approximate q-value problem is complete for RE.

While these results show that the exact q-value, exact co-value, and approximate q-value problems are all undecidable, they are undecidable in different ways. For example, a basic result in computability theory is that the classes RE and coRE are incomparable (i.e. they do not contain each other). Thus the approximate q-value problem cannot be reduced to the exact co-value problem and vice versa.[2] Similarly, because both RE and coRE can be reduced to it, the exact q-value problem must be *strictly* harder than both the approximate q-value and exact co-value problem (in the sense that a Turing machine equipped with the ability to compute the exact co-value of a game provably cannot solve the exact q-value problem).

We note that (a) since the complexities of the q-value and co-value problems are different, but (b) a positive answer to Tsirelson's Problem implies that they are the same, it must be that Tsirelson's Problem (and thus Connes' Embedding Problem) has a negative answer.

These results still leave two main open questions about the complexity of nonlocal games:

1. What is the complexity of the exact q-value problem (i.e. deciding whether $\omega_q(G) \overset{?}{=} 1$).

2. What is the complexity of the approximate co-value problem (i.e. deciding whether $\omega_{co}(G) = 1$ or $\omega_{co}(G) < \frac{1}{2}$)?

In this paper we resolve the first open question by characterizing the complexity of the exact q-value problem:

[2] The notion of reduction that we consider here are *many-one reductions*, i.e., yes instances are mapped to yes instances, and no instances are mapped to no instances.

Theorem 1.1. *The problem of deciding whether $\omega_q(G) = 1$ for nonlocal games G is complete for Π_2.*

The class Π_2 is in the second level of the *arithmetical hierarchy*, which is an infinite hierarchy of complexity classes[3] $\bigcup_{k=0}^{\infty} \Sigma_k$ and $\bigcup_{k=0}^{\infty} \Pi_k$ that characterize the complexity of languages according to *arithmetical formulas* that define them. The class Σ_k consists of all languages reducible to deciding whether a given Σ_k-*sentence* is true. A Σ_k-sentence S is of the form $\exists x_1 \, \forall x_2 \, \exists \cdots \, \phi(x_1, \ldots, x_k)$ for some computable predicate ϕ. Similarly, the class Π_k consists of all languages reducible to deciding a given Π_k-sentence is true; these are sentences of the form $\forall x_1 \, \exists x_2 \, \forall \cdots \, \phi(x_1, \ldots, x_k)$. [4]

At the zeroth ($k = 0$) level, the classes $\Sigma_0 = \Pi_0$ correspond to the set of decidable languages, and the first level classes Σ_1 and Π_1 are simply the well-known classes RE and coRE, respectively. The class Π_2 is in the second level of the arithmetical hierarchy, and contains both Σ_1 and Π_1. It is a well-known fact from computability theory that the levels of the arithmetical hierarchy are all distinct, and furthermore $\Sigma_k \neq \Pi_k$ for all $k \geq 1$.

Although we do not resolve the second open question, it is conjectured that the approximate *co*-value problem is complete for $\mathsf{coRE} = \Pi_1$. A positive resolution of this conjecture would complete the picture of the computability landscape of nonlocal games, depicted in Figure 1.1, and give a pleasing correspondence between different nonlocal game problems and classes in the arithmetical hierarchy.

[3] In computability theory these classes are usually denoted as Σ_k^0 and Π_k^0. For simplicity we have dropped the superscripts.

[4] Although we never use it in this paper, for the benefit of the reader, we recall the equivalent definitions of these classes using Turing machines. In this equivalent definition, Σ_1 (resp. Π_1) is the class of all languages L for which there exists a Turing machine A such that $A(x) = 1$ if and only if $x \in L$ (resp. $x \notin L$). The class Σ_2 (resp. Π_2) is the class of all languages L for which there exists a *Turing machine A with oracle access to the halting problem* such that $A(x) = 1$ if and only if $x \in L$ (resp. $x \notin L$). The kth level classes, for $k > 2$, can be defined similarly. From this definition, it is clear at once that Π_k is the set of languages L whose complement $\overline{L}$ is in Σ_k, and vice versa.

	$\varepsilon = 0$	$\varepsilon > 0$
$\omega_q(G) \pm \varepsilon$	Π_2 (this paper)	Σ_1 [4]
$\omega_{co}(G) \pm \varepsilon$	Π_1 [8]	Π_1 (conjectured)

Figure 1.1: A characterization of the complexity of computing the value of a nonlocal game in terms of the arithmetical hierarchy, depending on whether the quantum or commuting operator value is being considered, and whether the value is being computed exactly or approximately. The top left entry is the main result of this paper, and the lower right entry is conjectured.

We mention that the approximate and exact q- and co-value problems are used in defining the four complexity classes MIP^*, MIP^*_0, MIP^{co} and MIP^{co}_0, respectively. In particular, the above figure corresponds to the results $\mathsf{MIP}^* = \mathsf{RE} = \Sigma_1$, $\mathsf{MIP}^*_0 = \Pi_2$ and $\mathsf{MIP}^{co} \subseteq \mathsf{MIP}^{co}_0 = \mathsf{coRE} = \Pi_1$.

A priori, this tight correspondence between nonlocal games and the arithmetical hierarchy seems quite surprising. On one hand, computing the value of a nonlocal game corresponds to a continuous optimization problem over a space of quantum states and quantum measurements, possibly in infinite dimensions. On the other hand, deciding whether a quantified sentence is true is a discrete problem in symbolic logic ostensibly having nothing to do with quantum physics. Furthermore, the reader may notice that there are several interesting asymmetries in Figure 1.1, illustrating that this correspondence has rich and unexpected behavior: if we assume the conjecture about the approximate co-value problem, then both exact and approximate computation of the commuting operator value are equivalent to deciding Π_1-sentences, whereas for the quantum value, the complexity splits depending on whether we are considering exact or approximate computation.

Connections with noncommutative polynomial optimization. We also point out that the aforementioned complexity results can be viewed as characterizations of the complexity of *noncommutative polynomial optimization*, an important subject in mathematics, physics and computer science [14, 15, 16, 17]. The general formulation of noncommutative polynomial optimization (ncPO for short) is the following: given polynomials $p, q_1, \ldots, q_m$ in n-noncommutative variables

$(x_1, \ldots, x_n)$ over $\mathbb{R}$, compute the value of the following optimization program:

$$\begin{aligned} \sup \quad & \langle \phi | p(X) | \phi \rangle \\ \text{s.t.} \quad & q_i(X) \geq 0 \qquad \text{for } i = 1, \ldots, m \end{aligned}$$

The supremum is taken over all choices of tuples $(\mathcal{H}, X, \phi)$ where $\mathcal{H}$ is a Hilbert space, X is an n-tuple of bounded Hermitian operators acting on $\mathcal{H}$, and $|\phi\rangle$ is a unit vector on $\mathcal{H}$. The notation $p(X)$ and $q_i(X)$ indicates that we evaluate each of the indeterminates x_i with the operator X_i. We consider two different variations of an ncPO program P; if we restrict the supremum to vary only over finite – but unbounded – dimensional Hilbert spaces then we call the program *finite-dimensional* and let $\omega_{\text{fin}}(P)$ denote the value of the program. Otherwise we call the program *infinite-dimensional* and let $\omega_{\infty}(P)$ denote the value.

The complexity results in Figure 1.1 can be recast as the following. Given an ncPO program P and a real number $c \in R$, deciding whether

1. $\omega_{\text{fin}}(P) \geq c$ is complete for Π_2.

2. $\omega_{\infty}(P) \geq c$ is complete for Π_1.

3. $\omega_{\text{fin}}(P) \geq c$ or $\omega_{\text{fin}}(P) < c - \varepsilon$ for fixed $\varepsilon > 0$ is complete for Σ_1.

The reason for this is because on one hand we can encode the t-value of a nonlocal game for $t \in \{q, co\}$ as an ncPO program that is finite-dimensional if $t = q$ and infinite-dimensional if $t = co$; on the other hand the complexity of solving an ncPO program is upper-bounded by Π_2, Π_1, or Σ_1 depending on the variant of the problem. Although this connection is fairly straightforward, for completeness we provide the details in Section 1.8.

We note that, by comparison, the analogous problems for *commutative polynomial optimization* over $\mathbb{R}$ are decidable; this is because deciding whether a semialgebraic set defined by polynomial equalities/inequalities over $\mathbb{R}$ is empty is contained in PSPACE [18].

The main conceptual result of our paper is that all of the complexity statements about nonlocal games expressed in Figure 1.1 can be established in a unified manner via a technique called *nonlocal game compression*. At the heart of the proof of $\mathsf{MIP}^* = \mathsf{RE}$ is a *gap-preserving* compression theorem for the q-value of games. The centerpiece of the present paper is a *gapless* compression theorem that holds for both the q- and co-value of games. First we show that this gapless compression theorem directly gives an alternate proof of the Π_1-completeness of the exact co-value problem [8], as well as an alternate proof of Slofstra's result that the set of quantum correlations is not closed (i.e. there is a nonlocal game G with $\omega_q(G) = 1$, but there is no finite-dimensional strategy with success probability 1) [5].

We then combine our gapless compression theorem with the gap-preserving one of [4] to obtain the Π_2-hardness of the exact q-value problem, establishing Theorem 1.1. Finally, we also show how a gap-preserving compression theorem for the co-value of games would imply that the approximate co-value problem is complete for $\mathsf{coRE} = \Pi_1$.

Another goal of this paper is to give a self-contained proof of a compression theorem that (a) illustrates the key ideas of the gap-preserving compression results of [19, 4], (b) generalizes these ideas to the infinite-dimensional commuting operator setting, and (c) is presented in a language that is more accessible to researchers coming from operator algebras and related areas of mathematics. The proofs of the gap-preserving compression theorems of [19, 4] are quite involved and rely on sophisticated results ranging from self-testing [20, 21] to the quantum soundness of the low-degree test [22, 23] to gap amplification methods [24]. These components are needed for the gap-preserving aspect of their compression theorem. Working in the "gapless regime" allows us to work with much simpler versions of these components (or circumventing them entirely).

In Section 1.1.1 we give an overview of how compression of nonlocal games yields the complexity characterization shown in Figure 1.1. In Section 1.1.2 we give an overview of how our gapless compression theorem is proved. In Section 1.1.3 we explain the *synchronous strategies framework*, which our results are expressed in. This framework gives an elegant way to work with both q- and co-type strategies in a unified manner, and brings out the connection between nonlocal games and operator algebras.

1.1.1 The compression paradigm

Intuitively speaking, a nonlocal game compression procedure for t-type strategies (where $t \in \{q, co\}$) is a computable map `Compress` that takes an infinite sequence $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$ of polynomial-complexity nonlocal games to another infinite sequence $\mathscr{G}' = (G'_n)_{n\in\mathbb{N}}$ such that for every $n \in \mathbb{N}$,

- The optimal success probability of t-strategies in G'_n is related in a predictable way to the optimal success probability of t-strategies in G_n, and
- The *complexity* of the game G'_n is much smaller than that of the original game G_n, where we measure the complexity of a game based on the number of time steps required by the verifier to compute the decision procedure.

This second item is what motivates the name "compression".

The "polynomial-complexity" condition on the input sequence $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$ of games means that the complexity of each game G_n is bounded by $O(n^c)$ for some constant $c > 0$, and the compression procedure `Compress` will depend on this constant. Furthermore, $\mathscr{G}$ and $\mathscr{G}'$ are specified via *Turing machines* which play the role of the verifier for the games in the sequences. Thus the map `Compress` is a map from Turing machines to Turing machines. Importantly, the map `Compress` itself is also computable by a Turing machine.

Depending on which value type $t \in \{q, co\}$ we consider, how the optimal t-strategies of G'_n and G_n are related to each other, and how much smaller the complexity of G'_n is than of G_n, we obtain different compression procedures. The different compression procedures, in turn, allow us to establish the different entries of the correspondence outlined in Figure 1.1.

We now give a high-level sketch of this connection.

Gapped compression for q-type strategies. The $\mathsf{MIP}^* = \mathsf{RE}$ result of [4] relies on the following *gap-preserving* (or *gapped* for short) compression procedure for q-type strategies (i.e. finite-dimensional strategies).

Theorem 1.2 (Gap-preserving compression, informally stated [4])**.** *There exists a computable map* $\texttt{GappedCompress}_q$ *that, given a sequence of games* $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$*, outputs a sequence of games* $\mathscr{G}' = (G'_n)_{n\in\mathbb{N}}$ *such that the complexity of* $\mathscr{G}'$ *is* $O(\log n)$*, and furthermore if the complexity of* $\mathscr{G}$ *is at most* $\mathrm{poly}(n)$*, then for all* $n \in \mathbb{N}$*,*

- *If* $\omega_q(G_n) = 1$*, then* $\omega_q(G'_n) = 1$.
- $\mathcal{E}(G'_n, \frac{1}{2}) \geq \max\left\{\mathcal{E}(G_n, \frac{1}{2})\,,\, 2^n\right\}$.

Here, for a nonlocal game G and real number $0 \leq p \leq 1$, the quantity $\mathcal{E}(G, p)$ is defined to be the minimum dimension of a strategy $\mathscr{S}$ such that $\omega(G, \mathscr{S}) \geq p$. If there is no finite-dimensional strategy that achieves winning probability p, then $\mathcal{E}(G, p)$ is defined to be ∞.

The reason $\texttt{GappedCompress}_q$ is called "gap-preserving" is because if $\omega_q(G_n) = 1$, then $\omega_q(G'_n) = 1$, and otherwise if $\omega_q(G_n) < \frac{1}{2}$, then $\omega_q(G'_n) \leq \frac{1}{2}$. In other words, the gap between 1 versus $1/2$ in the two different possibilities for $\omega_q(G_n)$ is preserved for $\omega_q(G'_n)$. The second "if" follows from the second item of Theorem 1.2: if there are no finite-dimensional strategies for G_n that succeed with probability at least $\frac{1}{2}$, then $\mathcal{E}(G_n, \frac{1}{2}) = \infty$, and therefore $\mathcal{E}(G'_n, \frac{1}{2}) = \infty$, which implies that there is no finite-dimensional strategy for G'_n that has value at least $\frac{1}{2}$.

To show that every arithmetical sentence S of the form $\exists x\, \phi(x)$ can be transformed into an equivalent game G_S (which is essentially equivalent to the statement $\mathsf{MIP}^* = \mathsf{RE}$), the compression procedure of Theorem 1.2 is used to construct an infinite sequence of games $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$ that depends on the sentence S. If $\phi(x)$ is true for some $x \leq n$ (meaning that S is true), then the game G_n has the property that $\omega_q(G_n) = 1$; otherwise G_n is designed to be equivalent to the game G'_{n+1}, the compression of G_{n+1} through the gap-preserving transformation $\texttt{GappedCompress}_q$. In other words, the sequence of games $\mathscr{G}$ is effectively a *self-compressing* sequence of games. By inductively utilizing the guarantees of the gapped compression procedure, we get that in the case that S is true, we have $\omega_q(G_n) = 1$ for all n, and if S is false, $\omega_q(G_n) \leq \frac{1}{2}$ for all n.[5] Finally, the game G_S is then chosen to be the first member G_1 of the sequence $\mathscr{G}$.

[5] The choice of $\frac{1}{2}$ is inconsequential here; everything stated here holds true for any constant that's strictly less than 1.

Where does the poly(n)-complexity assumption on $\mathscr{G}$ and the $O(\log n)$-complexity of $\mathscr{G}'$ consequence of Theorem 1.2 come in? We can imagine that the behavior of the verifier in the game G_n is specified by the following pseudocode:

```
The verifier checks whether $\phi(x)$ is true for some $x \leq n$. If it is, then accept.
Otherwise, compute $\mathscr{G}'$ by running GappedCompress$_q$ on the description of the
  sequence $\mathscr{G}$.
Play the game $G'_{n+1}$, the $(n+1)$-st game of the sequence $\mathscr{G}'$.
```

Pseudocode 1: The game G_n encoding Σ_1-sentences.

For simplicity we assume that $\phi(n)$ is computable in time $O(n)$. Then the complexity of the game G_n can be computed as $O(n^2) + O(1) + O(\log n) = \text{poly}(n)$. The $O(n^2)$ comes from evaluating ϕ on n different inputs; the $O(1)$ comes from the complexity of executing the compression procedure; and the $O(\log n)$ comes from the complexity of the compressed game G'_{n+1}. So the sequence of games $\mathscr{G}$ has complexity poly(n), and thus the consequences of the assumption (the first and second items) are satisfied.

Gapless compression for q- and co-type strategies. We now turn to *gapless* compression procedures. As suggested by the name, these are compression procedures that do not necessarily preserve any gap in the values of the "input" sequence of games. The main technical contribution of this paper is the following gapless compression theorem:

Theorem 1.3 (Gapless compression, informally stated)**.** *For $t \in \{q, co\}$ there exists a computable map* `GaplessCompress`$_t$ *that, given a sequence of games $\mathscr{G} = (G_n)_{n \in \mathbb{N}}$, outputs a sequence of games $\mathscr{G}' = (G'_n)_{n \in \mathbb{N}}$ such that the complexity of $\mathscr{G}'$ is $O(\log n)$, and furthermore if the complexity of $\mathscr{G}$ is at most* poly(n)*, then for all $n \in \mathbb{N}$,*

- *If $\omega_t(G_n) < 1$, then $\omega_t(G'_n) < 1$.*

- *$\omega_t(G'_n) \geq 1 - \alpha(1 - \omega_t(G_n))$, where $0 < \alpha < 1$ is a universal constant.*

- $\mathcal{E}(G'_n, 1) \geq \max\left\{\mathcal{E}(G_n, 1)\,,\, 2^{2n}\right\}$.

Notice that the first and second items imply that $\omega_t(G_n) = 1$ if and only if $\omega_t(G'_n) = 1$. In the case of $t = q$, this gapless compression theorem appears to be a weaker version of Theorem 1.2, except the second item makes it incomparable: whereas the gapped compression theorem only works on games that either have value 1 or at most $\frac{1}{2}$, the gapless compression theorem works for all games. In fact, the compression procedure of Theorem 1.3 is *gap-shrinking*: given a game G_n with value $\omega_t(G_n) < 1$, the compressed game G'_n has value $\omega_t(G_n) < \omega_t(G'_n) < 1$. Intuitively, by repeatedly applying a gapless compress procedure to an initial game with value strictly less than 1, the sequence of compressed games obtained have value that get arbitrarily close to 1.

Gapless compression theorems allow us to show that deciding the truth of sentences S of the form $\forall x\, \phi(x)$ (i.e. Π_1-sentences) can be reduced to deciding whether the quantum (or commuting operator) value of nonlocal games is exactly 1. Analogously to the proof sketched for $\mathsf{MIP}^* = \mathsf{RE}$, we construct a self-compressing sequence of games $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$ that depends on the given sentence $S = \forall x\, \phi(x)$. In pseudocode, the games have the following behavior:

```
The verifier checks whether $\phi(x)$ is false for some $x \leq n$. If it is, then reject.
Otherwise, compute $\mathscr{G}'$ by running GaplessCompress$_t$ on the description of $\mathscr{G}$.
Play the game $G'_{n+1}$, the $(n+1)$-st game of the sequence $\mathscr{G}'$.
```

Pseudocode 2: The game G_n encoding Π_1-sentences.

Again we assume that $\phi(n)$ is computable in $O(n)$ time, implying that the games in the sequence $\mathscr{G}$ have poly(n)-complexity. The difference between this construction of G_n and the previous one is that instead of checking whether $\phi(x)$ is true for some $x \leq n$, the verifier now checks whether it is *false* for some x.

Using the gapless compression theorem, we get that if $\phi(x)$ is true for all x (meaning S is true), then we have $\omega_t(G_n) = \omega_t(G'_{n+1}) \geq 1 - \alpha\,(1 - \omega_t(G_{n+1}))$ for all $n \in \mathbb{N}$. Rearranging we get

$1 - \omega_t(G_n) \leq \alpha(1 - \omega_t(G_{n+1}))$ for all $n \in \mathbb{N}$. So by induction it holds that

$$1 - \omega_t(G_n) \leq \alpha^k(1 - \omega_t(G_{n+k}))$$

for all $k, n \in \mathbb{N}$. Taking the limit as $k \to \infty$, we conclude that $\omega_t(G_n) = 1$ for all $n \in \mathbb{N}$.

On the other hand, if S is false, then there is some n for which $\omega_t(G_n) = 0$. Let n be the smallest such integer. Working backwards, we deduce that $\omega_t(G'_n) < 1$ (by the first item of the gapless compression theorem), so therefore $\omega_t(G_{n-1}) < 1$, which means that $\omega_t(G'_{n-1}) < 1$, and so on. Thus for all $k \leq n$ we have $\omega_t(G_k) < 1$.

Finally, the game G_S is then chosen to be the first member G_1 of the sequence $\mathscr{G}$.

Since deciding the truth of Π_1-sentences is an undecidable problem, this gives an alternate proof of the undecidability of determining whether $\omega_t(G) = 1$ for $t \in \{q, co\}$, first proved by Slofstra [8, 5]. His proof is based on very different techniques based on group theory and approximate representation theory. As mentioned previously, the main result of Slofstra's work is that the set of quantum correlations C_q is not closed. We can also prove this separation as a corollary of our results in section 1.6.3.

Combining gapped and gapless compression. The main application of our gapless compression theorem is to combine it with the gapped compression theorem of [4] to prove Theorem 1.1, which establishes the Π_2-completeness of deciding whether the quantum value of a nonlocal game is equal to 1. The two compression theorems, interleaved together, allow us to transform sentences S of the form $\forall x \, \exists y \, \phi(x, y)$ (i.e. Π_2-sentences) to an equivalent nonlocal game G_S (i.e. S is true if and only if $\omega_q(G_S) = 1$).

Fix a Π_2-sentence $S = \forall x \, \exists y \, \phi(x, y)$. The key idea is that S can be equivalently expressed as $S = \forall n \, S_n$ where n ranges over the positive integers (rather than binary strings) and S_n is the Σ_1-sentence $\exists m \, \phi(n, m)$, where m also ranges over the positive integers. Leveraging the Σ_1-sentences-to-nonlocal games reduction from [4], we get that for all $n \in \mathbb{N}$ there exists a nonlocal game H_n (computable from S_n) such that $\omega_q(H_n) = 1$ if and only if S_n is true. In particular S is true if and only if $\forall n\, \omega_q(H_n) = 1$.

Now we design a sequence of games $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$ encoding the sentence S as follows.

```
Using the reduction from [4], compute the description of the game $H_n$ corresponding to the $\Sigma_1$-sentence $S_n$.
Compute the game sequence $\mathscr{G}' = (G'_n)_{n\in\mathbb{N}}$ by running GaplessCompress$_q$ on the description of $\mathscr{G}$.
With probability $\frac{1}{2}$, play the game $G'_{n+1}$, the $(n+1)$-st game of the sequence $\mathscr{G}'$.
With the remaining probability $\frac{1}{2}$, play the game $H_n$
```

Pseudocode 3: The game G_n encoding Π_2-sentences.

Since the reduction of [4] is polynomial-time computable, the game H_n has $\mathrm{poly}(n)$ complexity. The compressed game G'_{n+1} has $O(\log n)$ complexity, due to the guarantees of the $\mathcal{A}GaplessCompress_q$ procedure. This implies that each game G_n in the sequence $\mathscr{G}$ has $\mathrm{poly}(n)$ complexity. If S is true (meaning that S_m is true for all m) then we can establish the following relationship between $\omega_q(G_n)$ and $\omega_q(G_{n+1})$:

$$\begin{aligned}
\omega_q(G_n) &= \frac{1}{2}\omega_q(G'_{n+1}) + \frac{1}{2}\omega_q(H_n) && \text{(Definition of the game } G_n\text{)}\\
&= \frac{1}{2}\omega_q(G'_{n+1}) + \frac{1}{2} && (S \text{ true} \Rightarrow \omega_q(H_n) = 1 \text{ for all } n)\\
&\geq \frac{1}{2}\Big(1 - \alpha\,(1 - \omega_q(G_{n+1}))\Big) + \frac{1}{2} && \text{(Theorem 1.3)}\\
&= 1 - \frac{\alpha}{2}\Big(1 - \omega_q(G_{n+1})\Big)
\end{aligned}$$

This is equivalent to $1-\omega_q(G_n) \leq \frac{\alpha}{2}\Big(1-\omega_q(G_{n+1})\Big)$ and by induction this means that $1-\omega_q(G_n) \leq \left(\frac{\alpha}{2}\right)^k\Big(1-\omega_q(G_{n+k})\Big)$ for all $k \in \mathbb{N}$. As k goes to infinity, this means that $\omega_q(G_n)$ is arbitrarily close to 1, and thus is equal to 1.

On the other hand, if S is false, then there is some n for which S_n is false and consequently $\omega_q(H_n) < 1$. This means $\omega_q(G_n) < 1$. By the gapless compression theorem (Theorem 1.3) we deduce that $\omega_q(G'_n) < 1$, so therefore $\omega_q(G_{n-1}) < 1$, which means that $\omega_q(G'_{n-1}) < 1$, and so on. Thus for all $k \leq n$ we have $\omega_q(G_k) < 1$.

Finally, the desired game G_S is then chosen to be the first member G_1 of the sequence $\mathscr{G}$.

We observe that for this argument it did not matter that reduction from Σ_1-sentences S_n to games H_n is gapped (in the sense that $\omega_q(H_n) = 1$ if S_n is true and $\omega_q(H_n) \leq \frac{1}{2}$ otherwise). All that mattered was that there was *some* reduction from Σ_1-sentences to nonlocal games such that the game value reflects the truth of the sentence. This raises an interesting question for whether it is possible to prove the Π_2-hardness result using "just" a gapless compression theorem.

Gapped compression for commuting operator strategies? It is still unknown whether the problem of approximating the commuting operator value is as hard as deciding Π_1-sentences, which would mean that exact and approximate computation of the commuting operator value are equivalent in difficulty. Once again, the question boils down to the existence of a gapped compression procedure for commuting operator strategies. Suppose the following conjecture held:

Conjecture 1.4 (Gap-preserving compression for commuting operator strategies)**.** *There exists a computable map $\texttt{GappedCompress}_{co}$ that, given a sequence of games $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$, outputs a sequence of games $\mathscr{G}' = (G'_n)_{n\in\mathbb{N}}$ such that the complexity of $\mathscr{G}'$ is $O(\log n)$, and furthermore if the complexity of $\mathscr{G}$ is at most* $\mathrm{poly}(n)$*, then for all $n \in \mathbb{N}$,*

- *If $\omega_{co}(G_n) = 1$, then $\omega_{co}(G'_n) = 1$.*
- *If $\omega_{co}(G_n) \leq \frac{1}{2}$, then $\omega_{co}(G'_n) \leq \frac{1}{2}$.*

We can then design a sequence of games $\mathscr{G}$ as follows. Let M denote a Turing machine that, given a description of a nonlocal game F (note that this is a single game, rather than a sequence of games), halts if $\omega_{co}(F) < 1$ and otherwise runs forever. The semidefinite programming hierarchies of [14, 15], or the procedure described by [25], can be used to implement M.

```
1 The verifier checks whether $\phi(x)$ is false for some $x \leq n$. If it is, then reject.
2 Compute the description of the nonlocal game $G_1$, the first game of the sequence $\mathscr{G}$.
3 Run $M$ on input $G_1$ for $n$ steps. If it halts, then accept.
4 Otherwise, compute $\mathscr{G}'$ by running $\texttt{GaplessCompress}_{co}$ on the description of $\mathscr{G}$.
5 Play the game $G'_{n+1}$, the $(n+1)$-st game of the sequence $\mathscr{G}'$.
```

Pseudocode 4: The game G_n to decide Π_1-sentences.

Let S denote the sentence $\forall x\, \phi(x)$ for some $O(n)$-time computable predicate ϕ. Then the complexity of $\mathscr{G}$ is poly(n) so the consequences of Theorem 1.4 hold. Suppose S were true. Then Step 1 of Pseudocode 4 would never reject. Suppose that $\omega_{co}(G_1) < 1$. Then by definition, M will halt in some number of steps T. Thus $\omega_{co}(G_n) = 1$ for all $n \geq T$. For $n < T$, we have that $\omega_{co}(G_n) = 1$ if and only if $\omega_{co}(G'_{n+1}) = 1$ (by design of G_n), which is if and only if $\omega_{co}(G_{n+1}) = 1$ (by Theorem 1.4). By an inductive argument we get that $\omega_{co}(G_1) = 1$, which contradicts our assumption. Thus we get $\omega_{co}(G_1) = 1$.

On the other hand, suppose that S was false. Let m denote the least integer such that $\phi(m)$ is false. First, it cannot be the case that M halts in fewer than m steps. If it halted in n steps for $n < m$, then $\omega_{co}(G_n) = 1$ by construction. However, by construction and Theorem 1.4 this means that $\omega_{co}(G_{n-1}) = 1$, and so on, ultimately yielding that $\omega_{co}(G_1) = 1$. This is a contradiction, as the fact that M halts implies that $\omega_{co}(G_1) < 1$.

Next, we see that $\omega_{co}(G_m) = 0$ because $\phi(m)$ is false. By Theorem 1.4, this means that $\omega_{co}(G_{m-1}) \leq \frac{1}{2}$, and so on, ultimately yielding that $\omega_{co}(G_1) \leq \frac{1}{2}$, as desired. Letting $G_S = G_1$, this completes the reduction from the problem of deciding Π_1-sentences to approximate co-value problem.

We discuss a plausible approach to proving Theorem 1.4 in Section 1.1.2.

Finally, we note that there is something bizarre about the use of the Turing machine M in this construction. Regardless of whether S is true or false, in *both cases*, the verifier in the game G_1 never witnesses the Turing machine M halting! Thus, it may appear that M's halt/non-halt behavior is irrelevant to the decision procedures of the games $\{G_n\}$. However, if we remove line 3 from 4, then it is no longer clear how to reason about the value of the game G_1! In particular, when S is true, there is no n for which we can definitively identify the value of G_n, because we have an "infinite recursion" where G_n is the same game as the compression of G_{n+1}, which in turn is the same game as the compression of G_{n+2}, and so on. Thus, inserting M in the description of the games seems to force the sequence of games $\{G_n\}$ to "examine its own (commuting operator) value," which in turn allows us – mathematicians looking in from the outside – to pin down the value of G_n for all n. We find it a fascinating question of whether it is possible to deduce the value of the games $\{G_n\}$ with line 3 removed.[6]

Are compression theorems necessary? We have just demonstrated that, equipped with the appropriate compression procedures, we can characterize the complexity of the quantum and commuting operator value of nonlocal games. Could compression theorems be *necessary*? That is, does knowing that (say) exactly computing the commuting operator value is equivalent to deciding Π_1-sentences imply the existence of a compression procedure like the one given by Theorem 1.3?

In [26], it was shown that $\mathsf{MIP}^* = \mathsf{RE}$ (i.e. the Σ_1-hardness of the approximate q-value problem) implies a gap-preserving compression theorem for quantum strategies (i.e., Theorem 1.2). We show that this equivalence between compression and complexity of nonlocal games is more general:

- The Π_1-hardness of the approximate co-value problem implies a gap-preserving compression theorem for commuting operator strategies.
- The Π_1-hardness of the exact co-value problem implies a gapless compression theorem for commuting operator strategies.
- The Π_2-hardness of the exact q-value problem implies a gapless compression theorem for quantum strategies.

[6] This trick of inserting the Turing machine M into the description of the game is also used by [4] to construct an explicit game whose commuting operator value differs from its quantum value.

We prove these equivalences in Section 1.6.5.

Relation to previous work The idea of using compression in order to obtain complexity lower bounds for nonlocal games was first due to Ji [27]. There, he showed that the complexity of deciding between $\omega_q(G) = 1$ and $\omega_q(G) \leq 1 - 1/\text{poly}(|G|)$ where $|G|$ denotes the description length of the game G is at least as hard as solving NEXP-complete problems. His result, however, only applied to games with more than two players (in fact his result applies for games with 10 players). The techniques used to compress games use a variety of tools from quantum information theory, including quantum error correcting codes and the Feynman-Kitaev history state construction. This compression technique was further developed by [28], who prove a gapless compression theorem that can be *recursively composed* in order to obtain arbitrarily large complexity lower bounds for nonlocal games. The lower bounds obtained by [28] still only apply to games with three or more players, however. This is a fundamental limitation of the compression approach of [27, 28] because they rely on using quantum error-correcting codes to perform *secret sharing*, which require 3 or more parties.

Obtaining complexity lower bounds for *two* player games have wider implications and require new techniques. For example, the connection between Connes' Embedding Problem and the approximate q-value problem only hold for two player games. Compressing two-player nonlocal games was first pioneered by [19] and then further developed by [4] to prove $\mathsf{MIP}^* = \mathsf{RE}$. These works use very different tools such as classical and quantum low-degree tests and probabilistically checkable proofs (PCPs).[7] The gapless compression theorem of this paper is based on a simplified version of these techniques, which allows us to obtain our Π_2-hardness result for two-player games.

In [26], we obtained Π_2-hardness for the exact q-value problem for games with three or more players. This is because we combined the gapless compression theorem of [28] with the gapped compressed theorem of [4]. However as mentioned the requirement to have games with at least three players is intrinsic to the work of [27, 28]. Furthermore, all previous works only study the

[7] View Section 2 of [19] for a more in-depth overview of the differences.

setting of finite-dimensional (i.e. q-type) strategies; ours is the first to study compression of games in the commuting operator setting.

1.1.2 Overview of the gapless compression theorem

We now provide an overview of the proof of Theorem 1.3, our gapless compression theorem. The compression theorem technically is about a procedure for transforming a sequence of games into another, but for simplicity we discuss compression as transforming individual games.

The high-level structure of the compression procedure follows the paradigm first established by [19] and developed further by [4]. Let G denote an "input" game where the question lengths, answer lengths, and complexity of the decision procedure are $\mathrm{poly}(n)$. The game G is transformed into a "compressed" game G' where the complexity of the decision procedure is $\mathrm{poly}\log(n)$. This transformation consists of two steps, the first one called *Question Reduction* and the second called *Answer Reduction*. We describe these two steps next.

Fix an input game $G = (\mathcal{X}, \mathcal{A}, D)$. All games involved use the uniform distribution over questions; for this reason we omit mention of the question distribution when specifying a nonlocal game. Fix a value type $t \in \{q, co\}$.

Question Reduction

The Question Reduction step transforms G into the *Introspection game* $G^{\mathrm{intro}} = (\mathcal{X}^{\mathrm{intro}}, \mathcal{A}^{\mathrm{intro}}, D^{\mathrm{intro}})$ where

$$\log|\mathcal{X}^{\mathrm{intro}}| = O(\log\log|\mathcal{X}|)$$
$$\log|\mathcal{A}^{\mathrm{intro}}| = \mathrm{poly}(\log|\mathcal{A}|)$$
$$\text{Complexity of } D^{\mathrm{intro}} = \mathrm{poly}(\text{Complexity of } D)\ .$$

The Introspection game G^{intro} is equivalent to G in the sense that the value of $\omega_t(G^{\mathrm{intro}}) = 1$ if and only if $\omega_t(G) = 1$.

At an intuitive level, the question lengths are reduced in G^{intro} by asking the players to "ask themselves" – i.e., to introspect – their own questions from $\mathcal{X}$. The players in G^{intro} are each asked to sample a question $x \in \mathcal{X}$ and answer with $a \in \mathcal{A}$ as they would have answered in the original game G. If the players' responses are (x, a) and (y, b), the decision procedure in G^{intro} will check that $D(x, y, a, b) = 1$.

In order for the values of G and G^{intro} to be meaningfully related, we need to ensure that (a) the players sample their introspected questions x and y from the uniform distribution (instead of, say, always picking a fixed (x^*, y^*) for which they have prepared winning answers), and (b) the first player does not have any knowledge of the second player's question y and the second player does not have any knowledge of the first player's question x.

Forcing players to behave honestly according to (a) and (b) crucially relies on a property called *rigidity* that holds for some nonlocal games. A nonlocal game G is rigid if the state and measurement operators of any near optimal strategy for G satisfy very rigid constraints. For introspection, we need a family of games, called *Question Sampling games* where the nth member of this family is denoted by QS_n. Each game has two special questions labeled by measure-standard-basis and measure-orthogonal-basis and players in QS_n are required to respond to these questions with strings in $\{0, 1\}^n$. Furthermore these games exhibit rigidity in the following sense; in any near optimal strategy for QS_n the players must share n EPR pairs, and the player answering the measure-standard-basis (resp. measure-orthogonal-basis) question, must measure their share of entangled state using a measurement that is close, in some metric, to the standard basis measurement (resp. orthogonal basis $\{|+\rangle, |-\rangle\}$ measurement).

For simplicity suppose that the question set for the game G is $\mathcal{X} = \{0, 1\}^n$. Then the Introspection game G^{intro}, at its core, is the QS_n game[8]: to introspect the verifier just asks the player the measure-standard-basis question. The verifier then takes advantage of the other special question, measure-orthogonal-basis, to ensure that the properties (a) and (b) of introspection questions are

[8] To be more precise the game G^{intro} is QS_n extended so that it has a small number of additional special questions. The cross-checks between these special questions force the players to behave "honestly" (i.e., to sample (x, y) from the uniform distribution), or risk losing the game with some nonzero probability.

satisfied. The proof of this fact is a direct consequence of the rigidity property of the Question Sampling game as described earlier.

There are many candidate games for Question Sampling if we only cared about the rigidity property mentioned above. One example is the *parallel-repeated Magic Square game* [29]. What makes the search for a family of games QS_n more challenging is the additional requirement imposed by the property

$$\log|\mathcal{X}^{\mathrm{intro}}| = O(\log\log|\mathcal{X}|).$$

To satisfy this requirement the Question Sampling can have at most $\mathrm{poly}(n)$ questions. So overall QS_n must be a game with $\mathrm{poly}(n)$ questions for which any optimal strategy uses n EPR pairs. Any family of games satisfying this property is said to be *efficiently rigid.* Efficiency is referring to the fact that games with small number of questions are certifying Hilbert spaces of large dimension (2^n in the case of QS_n). The family of games where the nth game is the nth parallel-repeated Magic Square game is not efficiently rigid because the number of questions grows as $2^{O(n)}$. In Section 1.3.2 we introduce a family of games called 2-out-of-n Magic Square and prove it is efficiently rigid.

Introspection first appeared in [19] followed by a more sophisticated version in the $\mathsf{MIP}^* = \mathsf{RE}$ result. To obtain the gapped compression in that paper, the Question Reduction step must also be gap-preserving, i.e., in addition to the above requirements for introspection, it must be that if $\omega_q(G) < 1/2$, then $\omega_q(G^{\mathrm{intro}}) < 1/2$. For gapped introspection, in addition to efficient rigidity, we need to make sure that in any strategy winning QS_n with probability at least $1-\varepsilon$, the measurement for measure-standard-basis question is $\mathrm{poly}(\varepsilon, \log n)$-close (in operator norm) to the standard-basis measurement. The crucial point is that the error function has logarithmic dependence on n. This is what we call an *efficiently robust rigidity* result. The 2-out-of-n Magic Square game is not highly robust because the error function has a polynomial dependence on n. The game used in the $\mathsf{MIP}^* = \mathsf{RE}$ result that exhibits this additional robustness requirement is called the *quantum low-degree-test* [21]. The proof of rigidity for this game is considerably more complicated than the proof of rigidity for the 2-out-of-n Magic Square game. Also, in our setting we only need to introspect games with uniform question distributions. We believe these simplifications in the gapless setting help illuminate the core ideas behind introspection.

Answer Reduction

The Answer Reduction step transforms G into the game $G^{\text{ans}} = (\mathcal{X}^{\text{ans}}, \mathcal{A}^{\text{ans}}, D^{\text{ans}})$ where

$$\log |\mathcal{X}^{\text{ans}}| = \text{poly}(\log |\mathcal{X}|)$$
$$\log |\mathcal{A}^{\text{ans}}| = O(1)$$
$$\text{Complexity of } D^{\text{ans}} = \text{poly}(\log \text{Complexity of } D)\ .$$

The game G^{ans} is equivalent to G in the sense that the value of $\omega_t(G^{\text{ans}}) = 1$ if and only if $\omega_t(G) = 1$.

The idea is to delegate computing the decision procedure $D(x, y, a, b)$ to the players. Then have them certify their computation using a constant sized certificate. In this paper we use the *Cook-Levin reduction*: this is an efficient transformation that maps a Turing machine M and input string w to a 3SAT formula φ_M and variable assignment π_w such that $M(w) = 1$ if and only if π_w satisifes φ_M. Furthermore, w is embedded in the beginning of π_w . Clauses of the 3SAT formula φ_M can be computed hyper-efficiently (which allows us to exponentially reduce the verifiers runtime). We use this to reduce the Turing machine $D_{x,y}$, that computes the decision procedure for fixed questions (x, y), and the players answers (a, b) to a 3SAT formula $\varphi_{x,y}$ and assignment $\pi_{a,b}$. The verifier will now compute a random clause of this formula, and ask the players to provide the assignments specified by $\pi_{a,b}$ to the variables in the clause.

There are three immediate issues we must address in this scheme. First, in our current game no individual player has access to both questions to produce the 3SAT formula $\varphi_{x,y}$. Secondly, if we allow one of the players to have access to both questions, in order to compute $\varphi_{x,y}$, we must ensure that the answers (a, b) (and certificate $\pi_{a,b}$) are produced in such way that a only depends on x and b only depends on y. Lastly, we have to make sure the player in fact returns the corresponding assignments specified by $\pi_{a,b}$ and does not change this depending on the clause we query.

Fortunately, all three issues can be addressed by *oracularization*. This takes our original game and transforms it to a new game G^{orac} where the verifier sends one player a question $x \in \mathcal{X}$ and the other a pair of questions $(x, y) \in \mathcal{X}^2$. When a player receives a single question x we call them an *isolated player*. When a player receives a pair (x, y) we call them an *oracle player*. The players win if the oracle player responds with an answer pair $(a, b) \in \mathcal{A}^2$ such that $D(x, y, a, b) = 1$ and the isolated player responds with answer a (resp. responds with answer b). Intuitively, in G^{orac} an oracle player must "simulate" the behavior of the two players in G, and the isolated player (who only receives half of the oracle question) is used to check that the oracle player's answers (a, b) are produced in a way that a only depends on x and b only depends on y, solving our first two issues.

Now we can go ahead and apply the Answer Reduction protocol on the game G^{orac}, where the oracle player responds with assignments for our clause queries as described before, but the isolated player is asked a random bit of their original answer a (resp. b). In particular we query only from those clauses which contain at least one variable from the beginning of $\pi_{a,b}$ which embeds a (resp. b), we make sure the two players answers match on this assignment. This allows us to continue enforcing the no communication requirement after Answer Reduction. It also ensures that the oracle player is in fact providing assignments to the clause variables from $\pi_{a,b}$. Therefore G^{ans} uses constant sized answers and has exponentially more efficient verifier complexity.

From gapless to gapped compression

We highlight the primary differences between our gapless compression theorem and the gapped compression theorem of [4].

- In $\mathsf{MIP}^* = \mathsf{RE}$, instead of using the Cook-Levin reduction, the Answer Reduction transformation uses *probabilistically checkable proofs* (PCPs) in order to control the amount of gap shrinkage. The soundness of the PCP construction in [4] is based on the soundness of something called the *classical low-degree test* against entangled provers [23], which is a very technically challenging part of their analysis.

- As explained earlier, the Question Reduction step in $\mathsf{MIP}^* = \mathsf{RE}$ uses the robust rigidity of the quantum low-degree test [21]. Contrast this with our gapless compression theorem that does not require a robust rigidity test.
- The proof of $\mathsf{MIP}^* = \mathsf{RE}$ uses a *parallel repetition theorem*. Roughly speaking, parallel repetition theorems state that if the quantum value of a game G is less than 1, then the value of the game G^n, that is obtained from G by playing n instances of G in parallel, decays exponentially with n. This is needed because both the Question Reduction and Answer Reduction transformations shrink the gap by some amount, and parallel repetition is used to amplify the gap back to some constant amount.

In this paper we transfer many of the ideas from [4] to the infinite dimensional setting, allowing us to get a gapless compression theorem for commuting operator strategies. As discussed earlier proving Theorem 1.4 requires a gapped compression theorem for the commuting operator strategies. Just like in the case of q-strategies, we would also need to establish commuting-operator analogues of the three ingredients described above: (1) soundness of the classical low-degree test, (2) soundness of the quantum low-degree test, and (3) a parallel repetition theorem.

The first item has been resolved in a forthcoming paper [30]. The second item requires a proof that the quantum low-degree test is sound against commuting operator strategies. Finally, parallel repetition is well studied in the context of (finite-dimensional) quantum strategies [31, 32, 24] but nothing is known yet in the context of commuting operator strategies (aside from the parallel repetition result of [33], but this only holds for XOR games).

Given the commuting-operator analogues of these tools, however, the Π_1-completeness of the approximate co-value problem should then follow from the argument described in Section 1.1.1.

1.1.3 The synchronous strategies framework

As mentioned, another goal of this paper is to present the proof of the gapless compression theorem (Theorem 1.3) in a way that distills, into their simplest form, the techniques and conceptual components that go into establishing its much more sophisticated cousin, the gap-preserving compression theorem of [4]. To that end, we express and prove all our results in the framework of *synchronous strategies*, a class of strategies first studied by [34]. Working with these strategies simplifies our arguments both notationally as well as conceptually (as compared to working with general nonlocal games and general strategies).

A synchronous strategy $\mathscr{S}$ for a game G is specified by a separable Hilbert space $\mathcal{H}$ (which could be infinite-dimensional), a von Neumann algebra $\mathscr{A}$ on $\mathcal{H}$, a tracial state on the algebra $\mathscr{A}$, [9] and a set of projective measurements $\{M^x\}_{x \in \mathcal{X}}$ in the algebra $\mathscr{A}$ (each M^x is a set of projections $\{M^x_a\}_{a \in \mathcal{A}}$ summing to the identity). Given questions (x, y), the probability of obtaining answers (a, b) is given by $\tau(M^x_a \, M^y_b)$. Thus the probability that the strategy $\mathscr{S}$ succeeds in the game G is given by

$$\sum_{x,y \in \mathcal{X}} \mu(x, y) \sum_{a,b \in \mathcal{A}} D(x, y, a, b)\, \tau\Big(M^x_a \, M^y_b\Big) \,.$$

Readers who are not familiar with von Neumann algebras and tracial states may find the finite-dimensional setting easier to understand. When $\mathcal{H} = \mathbb{C}^r$ for some dimension r, then we can without loss of generality take the algebra $\mathscr{A}$ to be the set $\mathrm{B}(\mathcal{H})$ of all bounded operators on $\mathcal{H}$ (which in finite dimensions is simply the set of all linear operators). In this case there is a *unique* tracial state, which is the normalized trace $\tau(X) = \frac{1}{r}\,\mathrm{tr}(X)$. In terms of strategies for nonlocal games, this corresponds to the players using the same projective measurements for each question and sharing the maximally entangled state $|\Phi\rangle = \frac{1}{\sqrt{r}} \sum_{e=1}^{r} |e\rangle|e\rangle$. Such a strategy has the property that if both players receive the same question $x \in \mathcal{X}$, they always output the same answer $a \in \mathcal{A}$ (this is why these strategies are called "synchronous").

[9] A *von Neumann algebra* $\mathscr{A}$ on a Hilbert space $\mathcal{H}$ is a $*$-subalgebra of $\mathrm{B}(\mathcal{H})$ (the set of bounded operators on $\mathcal{H}$) that contains the identity operator and is closed under the weak operator topology. A *tracial state* τ on the algebra $\mathscr{A}$ is a positive, unital linear functional that satisfies the *trace property*: $\mathrm{TR}\,(AB) = \mathrm{TR}\,(BA)$ for all $A, B \in \mathscr{A}$.

In the infinite-dimensional setting, synchronous strategies give rise to *commuting operator* strategies: for every synchronous strategy $\mathscr{S} = (\tau, \{M^x\})$ with Hilbert space $\mathcal{H}$, there exist another Hilbert space $\mathcal{H}'$, a state $|\psi\rangle \in \mathcal{H}'$, and measurements $\{A^x\}, \{B^x\}$ on $\mathcal{H}'$ for the players respectively such that for all $x, y \in \mathcal{X}$ and $a, b \in \mathcal{A}$, the operators A^x_a and B^y_b commute and we have

$$\tau(M^x_a \, M^y_b) = \langle \psi | A^x_a \, B^y_b | \psi \rangle \ .$$

For a proof, see [34, Theorem 5.5].

Remark 1. *On the need to specify a von Neumann algebra $\mathscr{A}$ as part of the strategy: unlike in the finite-dimensional setting, we cannot without loss of generality take $\mathscr{A}$ to be all of* $\mathrm{B}(\mathcal{H})$*; this is because there may not necessarily be a tracial state on* $\mathrm{B}(\mathcal{H})$.

Synchronous strategies arise naturally when considering *synchronous games*: these are games where the players must output the same answers whenever they receive the same question (i.e. $D(x, x, a, b) = 0$ whenever $a \neq b$). This simple restriction on the rules of the game has the following consequences for optimal strategies:

Theorem 1.5 (Adapted from Theorem 3.2 of [35] and Theorem 3.6 of [36])**.** *Let $G = (\mathcal{X}, \mathcal{A}, \mu, D)$ be a synchronous game such that $\mu(x, x) > 0$ for all $x \in \mathcal{X}$. Then if $\omega_{co}(G) = 1$ then there exists a* synchronous strategy $\mathscr{S} = (\tau, \{M^x\})$ *for G that achieves value* 1. *If furthermore $\omega_q(G) = 1$, then there exists a sequence $\{\mathscr{S}_n\}_{n \in \mathbb{N}}$ of* finite-dimensional *synchronous strategies whose values approach* 1.

Many games studied in quantum information theory and theoretical computer science are synchronous games; for example the games constructed in the proof of $\mathsf{MIP}^* = \mathsf{RE}$ are all synchronous. In this paper, we also focus exclusively on synchronous games. For this reason, we focus on analyzing the *synchronous value* of games: we define

$$\omega^s_{co}(G) := \sup_{\text{synchronous } \mathscr{S}} \omega(G, \mathscr{S}) \qquad \text{and} \qquad \omega^s_q(G) := \sup_{\substack{\text{finite-dimensional} \\ \text{synchronous } \mathscr{S}}} \omega(G, \mathscr{S}) \ .$$

Since synchronous strategies correspond to commuting operator strategies, we have that $\omega^s_{co}(G) \leq \omega_{co}(G)$ and similarly $\omega^s_q(G) \leq \omega_q(G)$; Theorem 1.5 implies that $\omega^s_t(G) = 1$ if and only if $\omega_t(G) = 1$ for $t \in \{q, co\}$. Thus we do not lose any generality by restricting our attention to synchronous strategies. To be more precise, for a synchronous game G, the exact (resp. approximate) t-value problem, i.e., deciding between $\omega_t(G) = 1$ and $\omega_t(G) < 1$ (resp. deciding between $\omega_t(G) = 1$ and $\omega_t(G) \leq 1/2$), is equivalent to the problem of deciding between $\omega^s_t(G) = 1$ and $\omega^s_t(G) < 1$ (resp. deciding between $\omega^s_t(G) = 1$ and $\omega^s_t(G) \leq 1/2$).

The benefits of working within the synchronous games framework is that strategies only require specifying one set of measurements for both players (instead of having to keep track of one for Alice and one for Bob), and furthermore the state τ has the cyclic trace property. Working in the synchronous setting significantly simplified many of our proofs, in particular those of rigidity and introspection. Previous rigidity results needed to characterize the shared state upto isometry and find a concrete representation of the measurement operators as matrices. In the synchronous setting however we are able to completely sidestep these technical issues. We need only to show that certain algebraic relations such as commutation or anticommutation are satisfied by any optimal strategy, which allows for a much cleaner argument. Furthermore, working in the synchronous games framework allows for a unified treatment of both the finite- and infinite-dimensional settings.

This paper builds upon arguments and techniques from a number of previous results. There has been great success in pinning down the algebra of optimal strategies within the synchronous games setting. It is our hope that expressing our results in the language of synchronous games will facilitate connecting our work to the world of functional analysis and operator algebras.

Acknowledgments. We thank Vern Paulsen and William Slofstra for helpful comments. We thank the STOC and QIP referees for their feedback. The research presented in this paper was initiated at the University of Toronto. H.M. acknowledges the support of the Natural Sciences and Engineering Research Council of Canada (NSERC). H.Y. is supported by an NSERC Discovery

Grant, a Google Research Award, and AFOSR award FA9550-21-1-0040.

1.2 Preliminaries

For an integer $d \in \mathbb{N}$ we write $[d]$ to denote $\{1, 2, \ldots, d\}$. For functions $f, g_1, \ldots, g_l : \mathbb{N}^k \to \mathbb{N}$, we write $f \leq \mathrm{poly}(g_1, \ldots, g_l)$ if there exists a constants $C, E \geq 0$ such that for all sufficiently large $a_1, \ldots, a_k$,

$$f(a_1, \ldots, a_k) \leq C \prod_{i=1}^{\ell} g_i(a_1, \ldots, a_k)^E.$$

Let $A(x_1, \ldots, x_k)$ denote a k-input Turing machine, which is a Turing machine with k input tapes, a single work tape, and a single output tape. Then $\mathsf{TIME}_A(x_1, \ldots, x_k)$ denotes the maximum of the description length of A, and the running time of A on input $(x_1, \ldots, x_k)$ (which may be ∞ if A never halts on that input). For an integer $n \in \mathbb{N}$, we let $\mathsf{TIME}_A(n)$ denote the maximum of $\mathsf{TIME}_A(n, x_2, \ldots, x_k)$ over all $x_2, \ldots, x_k \in \{0,1\}^*$ (where n is provided to A in binary).

1.2.1 Algebras, states, and norms

Let $\mathcal{H}$ be a separable Hilbert space and let $\mathrm{B}(\mathcal{H})$ denote the set of bounded linear operators on $\mathcal{H}$. We write $1_{\mathcal{H}}$ to denote the identity operator on $\mathcal{H}$ (and simply write 1 when the Hilbert space is clear from context).

A von Neumann algebra on a Hilbert space $\mathcal{H}$ is a unital $*$-subalgebra of bounded operators $\mathrm{B}(\mathcal{H})$ that is closed in the *weak operator topology*. Given two von Neumann algebras $\mathscr{A}$ and $\mathscr{B}$ on Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ respectively, the tensor product algebra $\mathscr{A} \otimes \mathscr{B}$ is defined to be the closure under the weak operator topology of the $*$-subalgebra generated by $\{A \otimes B \in \mathrm{B}(\mathcal{H}_A \otimes \mathcal{H}_B) : A \in \mathscr{A}, B \in \mathscr{B}\}$.

Let $\mathscr{A} \subseteq \mathrm{B}(\mathcal{H})$ denote a von Neumann algebra on $\mathcal{H}$. We say that a positive linear functional $\tau : \mathscr{A} \to \mathbb{C}$ is

- *Unital* if $\tau(1) = 1$;

- *Normal* if for all families $(P_i)_{i\in I}$ of pairwise orthogonal projections in $\mathscr{A}$, we have $\tau\Big(\sum_{i\in I} P_i\Big) = \sum_{i\in I} \tau(P_i)$;
- *Tracial* if for all $A, B \in \mathscr{A}$, we have $\tau(AB) = \tau(BA)$;

In this paper, τ will always represent a positive linear functional that is tracial, normal, and unital. We call such functionals a *normal tracial state*. For brevity we often drop the "normal" qualifier. For an in-depth reference to von Neumann algebras, we refer the reader to Blackadar's textbook [37].

We record some basic properties of tracial states. First, tracial states satisfy the Cauchy-Schwarz and Hölder inequalities, i.e.

$$|\tau(A^*B)|^2 \leq \tau(A^*A)\,\tau(B^*B) \qquad \text{and} \qquad |\tau(A^*B)| \leq \|A\| \cdot \tau(|B|)$$

where $\|\cdot\|$ denotes the operator norm, and $|B| = \sqrt{B^*B}$. Second, tracial states give rise to a seminorm on $\mathscr{A}$: we define the τ-*norm* of an operator $A \in \mathscr{A}$ to be

$$\|A\|_\tau = \sqrt{\tau(A^*A)} = \sqrt{\tau(AA^*)}.$$

The $\|\cdot\|_\tau$ norm satisfies the triangle inequality: i.e., $\|A+B\|_\tau \leq \|A\|_\tau + \|B\|_\tau$.

If $\mathcal{H}$ is finite dimensional (i.e. isomorphic to $\mathbb{C}^d$) then there is a unique tracial state on the algebra $\mathrm{B}(\mathcal{H})$, which is the *dimension-normalized trace* $\frac{1}{d}\,\mathrm{tr}(A)$. Thus in this case the τ-norm is the normalized Frobenius norm.

Proposition 1.6. *If τ and σ are tracial states on von Neumann algebras $\mathscr{A}$ and $\mathscr{B}$ respectively, then $\tau \otimes \sigma$ is a tracial state on the von Neumann algebra $\mathscr{A} \otimes \mathscr{B}$.*

Proposition 1.7. *Let $A, B \in \mathscr{A}$. Then $\|AB\|_\tau \leq \|A\| \cdot \|B\|_\tau$.*

Proof.

$$\begin{aligned} \|AB\|_\tau &= \sqrt{\tau(BB^*A^*A)} \\ &\leq \sqrt{\|A^*A\| \cdot \tau(BB^*)} && \text{(Hölder)} \\ &= \|A\| \cdot \|B\|_\tau \end{aligned}$$

□

The following proposition allows us to exchange any operator A in any expression CAD with a nearby operator B and obtain a new expression CBD close to the original expression.

Proposition 1.8. *Let $C, D \in \mathscr{A}$ be any operators with $\|C\|, \|D\| \leq 1$. If $A, B \in \mathscr{A}$ and $\|A-B\|_\tau \leq \varepsilon$, then $\|CAD - CBD\|_\tau \leq \varepsilon$ and $|\tau(CAD - CBD)| \leq \varepsilon$.*

Proof. By Proposition 1.7

$$\|C(A-B)D\|_\tau^2 \leq \|C\|^2\|D\|^2\|A-B\|_\tau^2 \leq \|A-B\|_\tau^2.$$

We also have

$$\begin{aligned} |\tau(C(A-B)D)|^2 &= |\tau(DC(A-B))|^2 \\ &\leq \tau(DCC^*D^*)\tau((A-B)^*(A-B)) && \text{(Cauchy-Schwarz)} \\ &\leq \|A-B\|_\tau^2. \end{aligned}$$

In the last line we used that $\tau(DCC^*D^*) \leq 1$. Indeed, if $\|M\| \leq 1$, then by Hölder $|\tau(M)| \leq \|M^*\|\tau(I) \leq 1$. □

In applications of Proposition 1.8 we usually find ourselves in a situation where C and D are products of projections and unitaries. Since the operator norm is submultiplicative, i.e., $\|MN\| \leq \|M\|\|N\|$, the operator norm of any product of projections and unitaries is bounded above by 1. Thus the assumptions of the proposition are readily verified.

Proposition 1.9. *Let U be any unitary. If $|\tau(1-U)| \leq \varepsilon$, then $\|1-U\|_\tau \leq \sqrt{2\varepsilon}$*

Proof.

$$\|1-U\|_\tau^2 = \tau((1-U)^*(1-U)) = \tau(21 - U - U^*) \leq 2|\tau(1-U)|.$$

□

1.2.2 Measurements and distance measures on them

Let $\mathscr{A}$ denote a von Neumann algebra with a normal tracial state τ. Let $M = \{M_a\}_{a\in\mathcal{A}}$ and $N = \{N_a\}_{a\in\mathcal{A}}$ denote sets of operators in $\mathscr{A}$, indexed by a finite set $\mathcal{A}$. Then we measure the distance between M and N, denoted by $\|M-N\|_\tau$, as

$$\|M-N\|_\tau = \sqrt{\sum_{a\in\mathcal{A}} \|M_a - N_a\|_\tau^2}\ .$$

We say that M is *δ-far* from N, denoted by $M_a \approx_\delta N_a$, if $\|M-N\|_\tau \leq \delta$. We also occasionally use the notation $\|M\|_\tau = \sqrt{\sum_{a\in\mathcal{A}} \|M_a\|_\tau^2}$.

Lemma 1.10. *Let $M = \{M_a\}_{a\in\mathcal{A}}$ and and $N = \{N_a\}_{a\in\mathcal{A}}$ denote sets of operators indexed by a finite set $\mathcal{A}$. Then*

$$\|M-N\|_\tau \leq \|M\|_\tau + \|N\|_\tau\ .$$

Proof. We compute:

$$\begin{aligned}
\|M-N\|_\tau^2 &= \sum_{a\in\mathcal{A}} \|M_a - N_a\|_\tau^2 \\
&\leq \Big(\sum_{a\in\mathcal{A}} \|M_a\|^2\Big) + \Big(\sum_{a\in\mathcal{A}} \|N_a\|^2\Big) + 2\Big(\sum_{a\in\mathcal{A}} \|M_a\|_\tau \cdot \|N_a\|_\tau\Big) \\
&\leq \Big(\sum_{a\in\mathcal{A}} \|M_a\|^2\Big) + \Big(\sum_{a\in\mathcal{A}} \|N_a\|^2\Big) + 2\sqrt{\sum_{a\in\mathcal{A}} \|M_a\|_\tau^2} \cdot \sqrt{\sum_{a\in\mathcal{A}} \|N_a\|_\tau^2} \\
&= \Big(\|M\|_\tau + \|N\|_\tau\Big)^2\ .
\end{aligned}$$

The first inequality follows from the triangle inequality of the τ-norm, and the second inequality follows from Cauchy-Schwarz. □

A *positive operator-valued measure (POVM) on $\mathcal{H}$ with outcomes in a finite set $\mathcal{A}$* is a set of positive operators $\{M_a\}_{a\in\mathcal{A}}$ such that $\sum_{a\in\mathcal{A}} M_a = 1$. A projective measurement is a POVM such that each element M_a is a projection. For a projective measurement $M = \{M_a\}$ it holds that $M_a M_b = \delta_{a,b} M_a$ where $\delta_{a,b}$ is Kronecker delta. So operators belonging to the same projective measurement commute. We say two measurements $M = \{M_a\}$ and $N = \{N_b\}$ commute, if $M_a N_b = N_b M_a$ for all a, b.

To denote "data processed" measurements, i.e., apply a function $f : \mathcal{A} \to \mathcal{B}$ to the outcome of a measurement, we use the following notation: $M_{[f]}$ denotes the POVM with elements

$$M_{[f|b]} = \sum_{a:f(a)=b} M_a$$

for all $b \in \mathcal{B}$. As an example, suppose $\mathcal{A} = \{0,1\}^n$ and $\mathcal{B} = \{0,1\}$. Then we write $M_{[a\mapsto a_i]}$ to denote the processed measurement that measures a string a, and then returns the i-th bit of a. To refer to the element of $M_{[a\mapsto a_i]}$ corresponding to outcome $b \in \{0,1\}$, we write $M_{[a\mapsto a_i|b]}$. For a predicate $P : \mathcal{A} \to \{0,1\}$, we also use the notation

$$M_{[a:P(a)]} = \sum_{a:P(a)=1} M_a \ .$$

For example, the operator $M_{[a:f(a)\neq b]}$ denotes the sum over all M_a such that $f(a) \neq b$.

We introduce two important distance measures between POVMs that will be used throughout this paper. All operators referred to in the following are assumed to be elements of a von Neumann algebra $\mathscr{A}$ on which a tracial state τ is defined.

The first distance measure we define is called *inconsistency*. Let M, N denote POVMs with outcomes in a finite set $\mathcal{A}$ (called the *answer set* or *outcome set*). We say that M and N are

δ-inconsistent if

$$\sum_{\substack{a,b\in\mathcal{A}:\\ a\neq b}} \tau(M_a N_b) \leq \delta$$

When the answer set $\mathcal{A}$ is clear from context, we write $M_a \simeq_\delta N_a$ to denote that M and N are δ-inconsistent.

The second distance measurement we introduce is called *closeness*. We say that sets of POVMs M, N are *δ-far* if

$$\|M - N\|_\tau \leq \delta.$$

Similarly, when the answer set $\mathcal{A}$ is clear from context, we write $M_a \approx_\delta N_a$ to denote that M and N are δ-far. Observe that this notion of closeness is also well-defined when the operators M_a, N_a are not necessarily positive. Thus we will also write $M_a \approx_\delta N_a$ to denote closeness of arbitrary operator sets that are indexed by an answer set $\mathcal{A}$.

1.2.3 Utility lemmas about measurements

We now establish several utility lemmas concerning consistency, closeness, and measurements.

Lemma 1.11 (Cauchy-Schwarz for operator sets)**.** *Let $M = \{M_a\}_{a\in\mathcal{A}}$ and $N = \{N_a\}_{a\in\mathcal{A}}$ denote sets of operators (not necessarily POVMs). Then*

$$\Big|\sum_{a\in\mathcal{A}} \tau(M_a \cdot N_a)\Big|^2 \leq \Big(\sum_{a\in\mathcal{A}} \|M_a\|_\tau^2\Big) \cdot \Big(\sum_{a\in\mathcal{A}} \|N_a\|_\tau^2\Big) .$$

Proof. For every $a \in \mathcal{A}$, we have that $|\tau(M_a \cdot N_a)| \leq \|M_a\|_\tau \cdot \|N_a\|_\tau$ by the Cauchy-Schwarz inequality for tracial states. Applying the triangle inequality and Cauchy-Schwarz again we have

$$\Big|\sum_{a\in\mathcal{A}} \tau(M_a \cdot N_a)\Big|^2 \leq \Big(\sum_{a\in\mathcal{A}} \Big|\tau(M_a \cdot N_a)\Big|\Big)^2 \leq \Big(\sum_{a\in\mathcal{A}} \|M_a\|_\tau \cdot \|N_a\|_\tau\Big)^2 \leq \Big(\sum_{a\in\mathcal{A}} \|M_a\|_\tau^2\Big) \cdot \Big(\sum_{a\in\mathcal{A}} \|N_a\|_\tau^2\Big) .$$

□

Lemma 1.12 (Data processing inequality for consistency)**.** *Let $M = \{M_a\}$ and $N = \{N_a\}$ be*

POVMs with outcomes in $\mathcal{A}$ such that $M_a \simeq_\delta N_a$. Let $f : \mathcal{A} \to \mathcal{B}$. Then

$$M_{[f|b]} \simeq_\delta N_{[f|b]} \ .$$

Proof.

$$\sum_{b \neq b' \in \mathcal{B}} \tau(M_{[f|b]} N_{[f|b']}) = \sum_{\substack{b \neq b' \in \mathcal{B} \\ a, a' \in \mathcal{A} \\ f(a) = b, f(a') = b'}} \tau(M_a N_{a'}) \leq \sum_{a \neq a' \in \mathcal{A}} \tau(M_a N_{a'}) \leq \delta.$$

□

Lemma 1.13 (Consistency to closeness)**.** *Let $M = \{M_a\}$ and $N = \{N_a\}$ be POVMs with outcomes in $\mathcal{A}$ such that $M_a \simeq_\delta N_a$. Then $M_a \approx_{\sqrt{2\delta}} N_a$.*

Proof.

$$\begin{aligned}
\sqrt{\sum_a \|M_a - N_a\|_\tau^2} &= \sqrt{\sum_a \tau((M_a - N_a)^2)} \\
&\leq \sqrt{\sum_a \tau(M_a + N_a - M_a N_a)} \\
&= \sqrt{2 - 2 \sum_a \tau(M_a N_a)} \\
&\leq \sqrt{2 \sum_a \tau(M_a(1 - N_a))} \\
&\leq \sqrt{2\delta}.
\end{aligned}$$

The first inequality follows because $M_a - M_a^2 \geq 0$ as $\{M_a\}$ are POVMs. The second inequality follows from Jensen's inequality. □

Lemma 1.14 (Closeness to consistency)**.** *Let $M = \{M_a\}$ be a projective POVM and let $N = \{N_a\}_{a \in \mathcal{A}}$ be a POVM with outcomes in $\mathcal{A}$. Suppose that $M_a \approx_\delta N_a$. Then $M_a \simeq_\delta N_a$.*

Proof. Applying Cauchy-Schwarz twice, we get

$$\begin{aligned}\sum_a \tau(M_a(1 - N_a)) &= \sum_a \tau(M_a(M_a - N_a)) \\ &\leq \sqrt{\sum_a \tau(M_a^2)} \cdot \sqrt{\sum_a \tau((M_a - N_a)(M_a - N_a)^*)} \\ &\leq \delta\end{aligned}$$

where we used that $\sum_a \tau(M_a^2) = 1$. □

Lemma 1.15 (Consistency implies similar probabilities)**.** *Let $M = \{M_a\}$ and $N = \{N_a\}$ be POVMs with outcomes indexed by $\mathcal{A}$. Suppose that $M_a \simeq_\delta N_a$. Then*

$$\sum_{a \in \mathcal{A}} |\tau(M_a - N_a)| \leq 2\delta.$$

Proof. Let $S_x = \{a : \tau(M_a) > \tau(N_a)\}$ and $T_x = \{a : \tau(N_a) \geq \tau(M_a)\}$. Then

$$\sum_{a \in \mathcal{A}} |\tau(M_a - N_a)| = \sum_{a \in S_x} \tau(M_a - N_a) + \sum_{b \in T_x} \tau(N_a - M_a).$$

Then, since $\tau(M_a N_a) \leq \tau(N_a)$, we have

$$\sum_{a \in S_x} \tau(M_a - N_a) \leq \sum_{a \in S_x} \tau(M_a(1 - N_a)) \leq \sum_{a \in \mathcal{A}} \tau(M_a(1 - N_a)) \leq \delta.$$

Similarly $\sum_{b \in T_x} \tau(N_a - M_a) \leq \delta$. This completes the proof. □

Lemma 1.16. *Let $M = \{M_a\}_{a \in \mathcal{A}}, N = \{N_a\}_{a \in \mathcal{A}}$ be sets of operators (not necessarily POVMs), and let $R = \{R_b\}_{b \in \mathcal{B}}$ be a set of operators such that $\sum_b R_b^* R_b \leq 1$. Suppose that $M_a \approx_\delta N_a$. Then $R_b M_a \approx_\delta R_b N_a$ where the answer summation is over $(a, b) \in \mathcal{A} \times \mathcal{B}$. Similarly, if $\sum_b R_b R_b^* \leq 1$, we have $M_a R_b \approx_\delta N_a R_b$.*

Proof. We prove the approximation $R_b M_a \approx_\delta R_b N_a$:

$$\begin{aligned}\sum_{a\in\mathcal{A},b\in\mathcal{B}} \|R_b(M_a - N_a)\|_\tau^2 &= \sum_{a\in\mathcal{A},b\in\mathcal{B}} \tau\Big((M_a - N_a)^* R_b^* R_b (M_a - N_a)\Big) \\ &= \sum_a \tau\Big((M_a - N_a)^* \Big(\sum_b R_b^* R_b\Big)(M_a - N_a)\Big) \\ &\le \sum_a \tau\Big((M_a - N_a)^*(M_a - N_a)\Big) \\ &= \sum_a \|M_a - N_a\|_\tau^2 \\ &\le \delta^2.\end{aligned}$$

where in the first inequality we used the assumption that $\sum_b R_b^* R_b \le 1$. The proof for the approximation $M_a R_b \approx_\delta N_a R_b$ is similar. □

The following lemma states that POVMs that are almost projective (in the sense that each POVM element is close to its square) is close to a projective maesurement. A version of this was first proved in the finite-dimensional setting by [38], improved quantitatively in [23], and recently extended to the setting of von Neumann algebras by de la Salle [39].

Lemma 1.17 (Projectivization of POVMs [39]). *Let $\{M_a\} \subset \mathscr{A}$ be a POVM with outcomes indexed by a finite set $\mathcal{A}$. Suppose that the following holds:*

$$\sum_a \tau(M_a - M_a^2) \le \varepsilon.$$

Then there exists a projective measurement $\{P_a\} \subset \mathscr{A}$ such that

$$P_a \approx_{\delta_{proj}} M_a$$

where $\delta_{proj} = \delta_{proj}(\varepsilon)$ is a function that depends on ε (but independent of $\mathcal{A}$) and goes to zero as $\varepsilon \to 0$.

The next lemma allows us to "paste" multiple approximately-commuting measurements together to form a joint projective measurement.

Lemma 1.18 (Pasting lemma)**.** *Let $\{M^{(1)}, M^{(2)}, \ldots, M^{(K)}\} \subset \mathscr{A}$ be a set of projective measurements with outcomes in a finite set $\mathcal{A}$. Suppose that for all $i \neq j$, we have that*

$$M_a^{(i)} M_b^{(j)} \approx_\varepsilon M_b^{(j)} M_a^{(i)}$$

where the answer summation is over $(a, b) \in \mathcal{A}^2$. Then there exists a projective measurement $R = \{R_{\vec{a}}\} \subset \mathscr{A}$ with outcomes in $\mathcal{A}^K$ such that for all $i \in [K]$,

$$R_{[\vec{a} \mapsto a_i | b]} \approx_{\delta_{pasting}} M_b^{(i)}$$

where $\delta_{pasting} = \delta_{pasting}(K, \varepsilon)$ is a function that goes to 0 *as* $\varepsilon \to 0$.

We prove Theorem 1.18 in Section 1.7.

1.2.4 Nonlocal games, strategies, and verifiers

Nonlocal games. A *nonlocal game* G is a tuple $(\mathcal{X}, \mathcal{A}, \mu, D)$ where $\mathcal{X}$ is a finite *question set*, $\mathcal{A}$ is a finite *answer set*, μ is a probability distribution over $\mathcal{X} \times \mathcal{X}$, and $D : \mathcal{X} \times \mathcal{X} \times \mathcal{A} \times \mathcal{A} \to \{0, 1\}$ is a function called the *decision predicate*. A game G is *synchronous* if for all $x \in \mathcal{X}$, $D(x, x, a, b) = 1$ if and only if $a = b$. We call a question pair $(x, y) \in \mathcal{X} \times \mathcal{X}$ *trivial* if $D(x, y, a, b) = 1$ for all $(a, b) \in \mathcal{A} \times \mathcal{A}$; otherwise we call (x, y) *nontrivial*.

In this paper, we only consider games that are synchronous and whose question distribution is uniform over the question set; thus we denote games G by tuples $(\mathcal{X}, \mathcal{A}, D)$.

Strategies. A *tracial strategy* $\mathscr{S}$ for a game $G = (\mathcal{X}, \mathcal{A}, \mu, D)$ is a pair $(\tau, \{M^x\}_{x \in \mathcal{X}})$ where there is a separable Hilbert space $\mathcal{H}$ such that $\{M^x\}$ is a set of POVMs on $\mathcal{H}$ with outcomes in $\mathcal{A}$, and τ is a normal tracial state on a von Neumann algebra $\mathscr{A}$ containing the set $\{M_a^x\}_{x,a}$. The *value* of a tracial strategy $\mathscr{S}$ in G is defined as

$$\omega(G, \mathscr{S}) = \sum_{x,y \in \mathcal{X}} \mu(x, y) \sum_{a,b \in \mathcal{A}} D(x, y, a, b)\, \tau(M_a^x\, M_b^y)$$

A tracial strategy $\mathscr{S}$ is called *synchronous* if $\{M^x\}$ are projective measurements. A tracial strategy $\mathscr{S}$ is *finite dimensional* if $\mathcal{H} = \mathbb{C}^d$ for some d. A tracial strategy $\mathscr{S}$ *commutes on a set* $C \subseteq \mathcal{X} \times \mathcal{X}$ if for all $(x, y) \in C$ measurements M^x and M^y commute, i.e., $M_a^x M_b^y = M_b^y M_a^x$ for all $a, b \in \mathcal{A}$.

The *synchronous commuting operator value* of a synchronous game G, denoted by $\omega_{co}^s(G)$, is defined as the supremum of $\omega(G, \mathscr{S})$ over all synchronous strategies $\mathscr{S}$ for G. The *synchronous quantum value* of G, denoted by $\omega_q^s(G)$, is defined the same except the supremum is restricted to finite-dimensional synchronous strategies.

The *entanglement requirement* $\mathcal{E}\Big(G, \alpha\Big)$ for a game G and $\alpha \in [0, 1]$ is the minimum dimension of any finite-dimensional synchronous strategy $\mathscr{S}$ for G with quantum value at least α. If no such strategy exists then $\mathcal{E}\Big(G, \alpha\Big) = \infty$.

We introduce the notion of an oracularizable strategy; the significance of this notion is that the answer reduction transformation (discussed in Section 1.5) requires games to have oracularizable strategies. "Oracularizability" is an invariant maintained by our compression procedure (as well as the compression procedures of [19, 4]).

Definition 1.19 (Oracularizable strategy)**.** *A synchronous strategy $\mathscr{S}$ for a synchronous game G is* oracularizable *if the strategy commutes on the set of nontrivial questions of G.*

Verifiers. We introduce the notion of a *verifier*, which gives a uniform way to describe infinite sequences of nonlocal games.

Definition 1.20 (Verifiers)**.** *Let $\mathscr{G} = (G_n)_{n \in \mathbb{N}}$ denote an infinite sequence of synchronous games where $G_n = (\mathcal{X}_n, \mathcal{A}_n, D_n)$ and the sets $\mathcal{X}_n = \{0, 1\}^{\ell_n}, \mathcal{A}_n \subset \{0, 1\}^*$ for some polynomial-time computable function ℓ_n of n. A* verifier $\mathscr{V}$ for $\mathscr{G}$ *is a pair (D, C) of Turing machines where D is a* 5*-input Turing machine and C is a* 3*-input Turing machine, such that for all $n \in \mathbb{N}$, the following* *hold:*

1. *$D(n,x,y,a,b) = D_n(x,y,a,b)$ for all $(x,y) \in \mathcal{X}_n \times \mathcal{X}_n$ and $(a,b) \in \mathcal{A}_n \times \mathcal{A}_n$, and*

2. *$C(n,x,y) = 1$ if and only if $(x,y) \in \mathcal{X}_n \times \mathcal{X}_n$ is a nontrivial question pair for G_n.*

The Turing machines C and D are respectively called a question checker *(or simply just a* checker*) and* decider *for $\mathscr{G}$. When n is written on the first input tape of D and C, the Turing machines discard any string that comes after the ℓ_n'th bit in the second and third input tapes.*

Verifiers play a crucial role in the compression theorems of this paper and [4], as they allow for an effective method ("effective" in the computability sense) for encoding infinite sequences of nonlocal games.

Remark 2. *Although we have defined the games in the sequence $\mathscr{G}$ corresponding to a verifier $\mathscr{V}$ to have questions and answers consisting of binary strings, we often treat the questions and answers as sets with more structure, such as tuples. There, we implicitly assume an efficiently computable representation of set elements as binary strings is fixed.*

We note that the Turing machine D in the definition of verifier $\mathscr{V}$ for an infinite sequence $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$ of games already implicitly specifies the set of nontrivial questions for each G_n. For our compression procedure, however, it will be necessary to be able to quickly compute whether a question pair is nontrivial, and having a separate Turing machine C for this is helpful for separately keeping track of the decision procedure complexity versus the complexity of deciding the set of nontrivial questions.

1.2.5 Asymptotics and approximation bounds

We end the preliminaries section with a short discussion of asymptotics in the analyses of the Rigidity, Question Reduction and Answer Reduction sections. The bounds and approximations in this paper are functions of two quantities: one is the *game index n*, which indicates the n-th element of an infinite sequence $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$ of games; we take n to go to infinity and use n to measure sizes of question/answer alphabets, as well as the time complexity of the deciders. The other quantity is ε where $1 - \varepsilon$ is a lower bound on the synchronous quantum or synchronous commuting operator value of a nonlocal game G under consideration. We treat ε as a quantity that goes to 0.

All of our approximations in this paper will generally depend on both n and ε. From the assumption that the value of the game is at least $1 - \varepsilon$ we will derive consequences for a pair of measurements $\{M_a\}, \{N_a\}$. For example we may prove that $M_a \approx_{\delta(n,\varepsilon)} N_a$ where $\delta : \mathbb{N}\times\mathbb{R}^+ \to \mathbb{R}^+$ is any function that is continuous in the second argument and is such that $\delta(n, 0) = 0$ for all n. We call such functions *proper error functions*. We usually let the dependence on n to be implicit and simply write $\delta(\varepsilon)$ for proper error functions.

Every instance of δ in this paper should be understood as a function that is different from all the previous instances of δ except for the aforementioned two properties. For example if $M_a \approx_{\delta(\varepsilon)} N_a$ and $N_a \approx_{\delta(\varepsilon)} P_a$ by the triangle inequality we have

$$\sum_a \|M_a - P_a\|^2 \leq 2\sum_a \|M_a - N_a\|^2 + 2\sum_a \|N_a - P_a\|^2$$

so we can write $M_a \approx_{\delta(\varepsilon)} P_a$; every occurrence of $\delta(\varepsilon)$ in these three approximations can be a different proper error function.

As such in this paper we usually do not keep track of the specific approximation bounds. For POVMs $\{M_a\}$ and $\{N_a\}$ we will often write $M_a \approx N_a$ to denote $M_a \approx_{\delta(\varepsilon)} N_a$ for some proper error function $\delta(\varepsilon)$. We also use the notation $M \approx N$, for any two operators M, N, to indicate that $\|M - N\|_\tau \to 0$ as $\varepsilon \to 0$. Similarly we may write $\tau(M) \approx \tau(N)$ to indicate that $\tau(M - N) \to 0$ as $\varepsilon \to 0$. We recommend reading the proof of Theorem 1.21 carefully to get used to these conventions. The proof contains techniques that are used over and over in this paper.

Averaging argument. A simple but prevailing idea in many of the proofs in this paper is the observation that, if a strategy in a game G has a value at least $1 - \varepsilon$, then the winning probability conditioned on any event that has a nonzero probability is at least $1 - \delta(\varepsilon)$ for some error function

δ that has some dependence on the probability of the conditioning event (we usually ignore this dependence). So for example since the probability distribution on questions is uniform in all our games, the event that players receive a fixed question pair (x, y) has probability $1/|\mathcal{X}|^2$ where $\mathcal{X}$ is the question set of the game. Then the probability of winning conditioned on players receiving question pair (x, y) is at least $1 - |\mathcal{X}|^2\varepsilon = 1 - \delta(\varepsilon)$. We usually abbreviate this by simply saying "by an averaging argument, the probability of winning conditioned on players receiving question pair (x, y) is $1 - \delta(\varepsilon)$." Since we are working in the gapless regime, we do not need to keep track of the dependence of δ on $|\mathcal{X}|$ which allows us to just simply write $\delta(\varepsilon)$.

The implication of cross-checks between nontrivial question pairs. We explain another proof technique that appears repeatedly in the following sections of the paper. Suppose $\{q, r, qr\} \in \mathcal{X}$ are three questions in a game G (qr is a single question different from q and r). The answer to questions q, r, qr are expected to be in three sets $\mathcal{A}, \mathcal{B}, \mathcal{A} \times \mathcal{B}$, respectively. Furthermore suppose that the winning condition dictates that $D(q, qr, a, (a', b')) = 1$ iff $a = a'$ and that $D(r, qr, b, (a', b')) = 1$ iff $b = b'$. Clearly (q, qr) and (r, qr) are nontrivial question pairs in this game.

Now one very useful observation is that if $(\tau, \{N^x\}_{x\in\mathcal{X}})$ is any strategy that wins this game with probability at least $1 - \varepsilon$, then it must be that

$$N^q_a N^r_b \approx_{\delta(\varepsilon)} N^r_b N^q_a,$$

or in other words the measurements N^q and N^r approximately commute. To see this, first note that by an averaging argument the probability of winning conditioned on receiving question pair (q, qr) is $1 - \delta(\varepsilon)$. This fact can be stated as follows

$$1 - \delta(\varepsilon) \leq \sum_{a\in\mathcal{A}, b\in\mathcal{B}} \tau(N^q_a N^{qr}_{a,b}) = \sum_{a\in\mathcal{A}} \tau(N^q_a N^{qr}_{a,\cdot})$$

where $N^{qr}_{a,\cdot}$ is the marginal measurement projection $\sum_{b\in\mathcal{B}} N^{qr}_{a,b}$. We can rewrite this as

$$N^q_a \simeq_{\delta(\varepsilon)} N^{qr}_{a,\cdot} \ .$$

By an application of Theorem 1.13 we get

$$N^q_a \approx_{\delta(\varepsilon)} N^{qr}_{a,\cdot} \ .$$

By the symmetry we similarly get

$$N^r_b \approx_{\delta(\varepsilon)} N^{qr}_{\cdot,b} \ .$$

where $N^{qr}_{\cdot,b}$ is the marginal measurement projection $\sum_{a\in\mathcal{A}} N^{qr}_{a,b}$.

Using Theorem 1.8, we get

$$N^q_a N^r_b \approx_{\delta(\varepsilon)} N^{qr}_{a,\cdot} N^r_b \ .$$

With another application of Theorem 1.8, we get

$$N^{qr}_{a,\cdot} N^r_b \approx_{\delta(\varepsilon)} N^{qr}_{a,\cdot} N^{qr}_{\cdot,b} \ .$$

By the triangle inequality we can combine these to get

$$N^q_a N^r_b \approx_{\delta(\varepsilon)} N^{qr}_{a,\cdot} N^{qr}_{\cdot,b} \ .$$

Since projection operators belonging to the same projective measurement commute, we have

$$N^{qr}_{a,\cdot} N^{qr}_{\cdot,b} = N^{qr}_{\cdot,b} N^{qr}_{a,\cdot} \ .$$

Finally by two more applications of Theorem 1.8 and the triangle inequality, we get the desired result

$$N^q_a N^r_b \approx_{\delta(\varepsilon)} N^r_b N^q_a \ .$$

1.3 Nonlocal game rigidity

A fundamental component of compression theorems are the use of nonlocal games with specific *rigidity* properties. Informally speaking, a nonlocal game G is rigid if the state and measurement operators of an optimal strategy for G must satisfy very rigid constraints – even to the point of being uniquely specified up to conjugation by isometries.

The most well-known example of a rigid game is the CHSH game [40], named after physicists Clauser, Horne, Shimony and Holt. In this game Alice and Bob receive questions $x, y \in \{0, 1\}$ and answer with bits $a, b \in \{0, 1\}$. They win if and only if $a + b = xy \mod 2$.

It is well-known that the CHSH game satisfies $\omega_q(CHSH) = \omega_{co}(CHSH) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$, and the optimum is achieved by a simple two-dimensional strategy (that we call the *canonical strategy*) where the players share the entangled state $|\text{EPR}\rangle = (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)/\sqrt{2}$, and Alice and Bob's measurement operators are defined to be the following: for all $a, b \in \{0, 1\}$,

1. A^0_a is the projection onto the eigenspace of $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ with eigenvalue $(-1)^a$.
2. A^1_a is the projection onto the eigenspace of $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with eigenvalue $(-1)^a$.
3. B^0_b is the projection onto the eigenspace of $(Z + X)/\sqrt{2}$ with eigenvalue $(-1)^b$.
4. B^1_b is the projection onto the eigenspace of $(Z - X)/\sqrt{2}$ with eigenvalue $(-1)^b$.

(The CHSH game is not a synchronous game and optimal strategies for CHSH are not synchronous, so in general Alice and Bob will have different measurement operators for each question).

It turns out that *any* finite-dimensional strategy achieving the optimum value for CHSH must be *equivalent* to the canonical strategy just described: if the state $|\psi\rangle$ belongs to $\mathcal{H}_A \otimes \mathcal{H}_B$ for finite-dimensional Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$,[10] then there exist isometries V_A, V_B acting on $\mathcal{H}_A, \mathcal{H}_B$

[10] A standard result in the theory of nonlocal games is that any finite-dimensional strategy can be expressed as a tensor-product strategy [11, Theorem 1].

respectively such that $(V_A \otimes V_B)|\psi\rangle = |EPR\rangle \otimes |\phi\rangle$ for some auxiliary state $|\phi\rangle$, and furthermore under the isometries the players' measurement operators are equal to the canonical measurements described above. Since we can only characterize quantum strategies up to local isometries (i.e. applying local isometries to a strategy cannot change its success probability), this shows that the canonical strategy is essentially the unique strategy achieving the optimum winning probability for CHSH.

Furthermore, the rigidity of the CHSH game is *robust*: strategies that are approximately optimal for CHSH must be approximately equivalent, up to local isometries, to the canonical strategy. The rigidity of the CHSH game has been studied extensively in quantum information theory and has found applications to quantum cryptography and quantum complexity theory; see [41] for a survey of self-testing and its applications.

In this paper, we propose a more abstract formulation of nonlocal game rigidity: we say that a game G is rigid if there is a set of *algebraic relations* that are (approximately) satisfied by the measurement operators in any strategy $\mathscr{S}$ for G that (approximately) attains the optimal value. We no longer worry about characterizing the state vector or finding a concrete representation of the measurement operators as matrices.

For example, the rigidity of the CHSH game can be formulated as follows: any quantum strategy where their shared state is $|\psi\rangle$ and Alice's and Bob's projective measurements are $\{A^x_a\}$ and $\{B^y_b\}$ respectively that achieves value $\omega_{co}(CHSH)$ in the CHSH game must generate *anti-commuting observables*: defining the self-adjoint unitary operators $U^0 = A^0_0 - A^0_1$ and $U^1 = A^1_0 - A^1_1$, we must have that $U^0 U^1 |\psi\rangle = -U^1 U^0 |\psi\rangle$; the same holds with Bob's operators. Furthermore, this anti-commutation relation establishes that the Hilbert space must have dimension at least 2.

Establishing anti-commutation relations between the observables induced by an optimal strategy is usually the first step in "traditional" proofs of CHSH rigidity; this step is key to proving that the state and measurements are isometric to $|EPR\rangle$ and the Pauli Z and X observables, respectively. In this paper, however, we solely focus on the algebraic relations between the measurement operators – these are the only properties that are needed for our applications. This allows us to shortcut some of the complexity of typical arguments for nonlocal game rigidity.

Aside from providing simplifications, we believe that this algebraic perspective on rigidity will be beneficial for studying nonlocal games and their connections to subjects such as approximate representation theory and operator algebras.

1.3.1 The Magic Square game

We illustrate how rigidity results can be formulated in the synchronous games framework using the *Mermin-Peres Magic Square game* (often called *Magic Square game* for short) [42, 43, 44]. Rigidity of Magic Square is first proved in [45]. The Magic Square is a game where the players' goal is to convince the verifier that they can assign values to the cells of a 3 × 3 grid such that the sum of cells within a row or column is even, except in the last column, where the sum should be odd. Of course, it is impossible to deterministically assign values satisfying these constraints, but when the players use a quantum strategy it appears as if they are performing the impossible.

We can view the Magic Square game as corresponding to a system of linear equations over $\mathbb{Z}_2$: let $s_{11}, \dots, s_{33}$ denote variables for the nine squares of the 3 × 3 grid, as depicted below:

s_{11}	s_{12}	s_{13}
s_{21}	s_{22}	s_{23}
s_{31}	s_{32}	s_{33}

There are three constraints for the rows and three constraints for the columns:

$$\begin{aligned} s_{11} + s_{12} + s_{13} &= 0 \qquad & s_{11} + s_{21} + s_{31} &= 0 \\ s_{21} + s_{22} + s_{23} &= 0 \qquad & s_{12} + s_{22} + s_{32} &= 0 \\ s_{31} + s_{32} + s_{33} &= 0 \qquad & s_{13} + s_{23} + s_{33} &= 1 \end{aligned}$$

In the standard formulation of the Magic Square game, one player is chosen to be a *constraint player*, meaning that they receive a random equation $e = \{s_{i_1 j_1}, s_{i_2 j_2}, s_{i_3 j_3}\}$ from this linear system. The other player is chosen to be the *variable player*, meaning that they receive a random variable

s_{ij} from the equation e. The constraint player is supposed to respond with an assignment from $\{0,1\}$ to each of the variables in their received equation, and the variable player is supposed to respond with an assignment to their variable. The players win if the constraint players' assignment satisfies the given equation and if the variable player's assignment is consistent with the constraint player's answers (i.e. the constraint player's assignment for the other player's received variable must match the variable player's response).

We only deal with games with uniform question distributions in this paper, so the variant of the Magic Square game (which we abbreviate as MS) that we consider is where the questions to Alice and Bob are uniformly and independently chosen from $\mathcal{X}_{\text{MS}} = \mathcal{X}_{\text{eqs}} \cup \mathcal{X}_{\text{vars}}$ where

$$\begin{aligned} \mathcal{X}_{\text{eqs}} &= \{r_1, r_2, r_3, c_1, c_2, c_3\}, \\ \mathcal{X}_{\text{vars}} &= \{s_{11}, s_{12}, s_{13}, s_{21}, s_{22}, s_{23}, s_{31}, s_{32}, s_{33}\}. \end{aligned}$$

Here r_i (resp. c_j) stands for the equation associated with the ith row $\{s_{i1}, s_{i2}, s_{i3}\}$ (resp. jth column $\{s_{1j}, s_{2j}, s_{3j}\}$). For every constraint e in the Magic Square linear system, let $\mathcal{A}_e$ denote the set of functions f_e that map variables in e to $\{0,1\}$. The answer set is $\mathcal{A}_{\text{MS}} = \mathcal{A}_{\text{eqs}} \cup \mathcal{A}_{\text{vars}}$ where $\mathcal{A}_{\text{eqs}}$ is the the union of $\mathcal{A}_e$ over all constraints e, and $\mathcal{A}_{\text{vars}} = \{0,1\}$. The decision procedure $D_{\text{MS}}(x,y,a,b)$ for the Magic Square game is described by the following table: if (x,y) (resp. (y,x), as the game is symmetric) is one of the nontrivial question pairs listed, then the players win if and only if the winning condition for the answers (a,b) (resp. (b,a)) is satisfied. Otherwise, if the question pair is nontrivial, the players automatically win.

Nontrivial Question Pair (x,y)	**Winning Condition on Answers** (a,b)
$x = y$	$a = b$
$x \in \mathcal{X}_{\text{eqs}}, y \in \mathcal{X}_{\text{vars}}$ and y is a variable in equation x	$a \in \mathcal{A}_{\text{eqs}}$ satisfies equation x and $a(y) = b$

Table 1.1: The nontrivial question pairs and winning conditions for the Magic Square game.

We now define a value-1 synchronous strategy for the Magic Square game. Let $\mathcal{H}$ be a Hilbert space and for each variable s_{ij} let O^{ij} denote a self-adjoint unitary operator (called an *observable*) acting on $\mathcal{H}$. Suppose that by arranging them into a 3×3 grid, the observables satisfy the following algebraic relations:

1. (**R1**) The product of observables in a row or column multiply to 1, except in the last column, where they multiply to -1.

2. (**R2**) Two observables in the same row or column commute with each other;

3. (**R3**) Two observables not in the same row or column anti-commute with each other.

First, we note that it is possible to find such a set of observables satisfying these algebraic relations (see Figure 1.2 for an example of unitary operators acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$).

$Z \otimes 1$	$1 \otimes Z$	$Z \otimes Z$
$1 \otimes X$	$X \otimes 1$	$X \otimes X$
$Z \otimes X$	$X \otimes Z$	$XZ \otimes ZX$

Figure 1.2: An example of optimal observables for the Magic Square game, where the X and Z operators are the same as in the canonical CHSH strategy.

Second, we note that relation **R3** is actually a consequence of relations **R1** and **R2**. For example to obtain $O^{11}O^{22} = -O^{22}O^{11}$ one could repeatedly apply **R1** and **R2** in the following order

$$\begin{aligned}(O^{11}\ O^{22})^2 &= (O^{12}\ O^{13})(O^{23}\ O^{21})(O^{21}\ O^{31})(O^{32}\ O^{12}) \\ &= O^{12}(O^{13}\ O^{23})(O^{21}\ O^{21})(O^{31}\ O^{32})O^{12} \\ &= -O^{12}\ O^{33}\ O^{33}\ O^{12} = -1. \end{aligned} \tag{1.3.1}$$

However we include **R3** because the anti-commutation relation turns out to be the most important one in our applications of rigidity.

Given a set $O = \{O^{ij}\}$ of observables satisfying relations **R1**, **R2**, and **R3**, we can define the synchronous strategy $\mathcal{S} = (\tau, \{M^x\})$ where τ is a tracial state on the von Neumann algebra generated by the observables $\mathcal{O}$. For a variable question s_{ij}, define the measurement operator $M_b^{s_{ij}}$ to be the projection onto the eigenspace of O^{ij} with eigenvalue $(-1)^b$. To aid notation we abbreviate $M_b^{s_{ij}}$ as M_b^{ij}. The operator M_a^e corresponding to a constraint question $e \in \mathcal{X}_{\text{eqs}}$ is the product

$$\prod_{s_{ij} \in e} M^{ij}_{a(s_{ij})} \tag{1.3.2}$$

where the product is over variables s_{ij} occurring in equation e, and a is an assignment to variables in e. Notice that because of relation **R2**, if $s_{i_1 j_1}, s_{i_2 j_2} \in e$ then

$$\begin{aligned} M_{b_1}^{i_1 j_1} \; M_{b_2}^{i_2 j_2} &= 1/4(1 + (-1)^{b_1} O^{i_1 j_1})(1 + (-1)^{b_2} O^{i_2 j_2}) \\ &= 1/4(1 + (-1)^{b_2} O^{i_2 j_2})(1 + (-1)^{b_1} O^{i_1 j_1}) \\ &= M_{b_2}^{i_2 j_2} \; M_{b_1}^{i_1 j_1} \end{aligned}$$

for every $b_1, b_2 \in \{0, 1\}$. So the order of the product in Equation (1.3.2) doesn't matter, and thus M_a^e is also a projection.

It is easy to verify that this strategy for the Magic Square game attains winning probability 1; this relies on the relations **R1** and **R2**. Let us verify this in a few simple steps. Conditioned on players receiving a trivial question pair, the players winning probability is 1 (as in this case players win regardless of their answers). Conditioned on receiving the same question, the players respond with the same answer with probability 1 because $\mathcal{S}$ is a projective strategy. Indeed conditioned on receiving question pair (s_{ij}, s_{ij}), the probability of winning is

$$\tau(M_0^{ij} \; M_0^{ij}) + \tau(M_1^{ij} \; M_1^{ij}) = \tau(M_0^{ij} + M_1^{ij}) = \tau(1) = 1.$$

Similarly conditioned on question pair $(e, e) \in \mathcal{X}_{\text{eqs}} \times \mathcal{X}_{\text{eqs}}$, the probability of winning is

$$\sum_{a \in \mathcal{A}_e} \tau(M_a^e M_a^e) = \sum_{a \in \mathcal{A}_e} \tau(M_a^e) = \tau(1) = 1.$$

Finally, conditioned on receiving question pair (r_i, s_{ij}), the probability that the constraint player's assignment for s_{ij} matches the variable player's answer to s_{ij} is

$$\begin{aligned}
\sum_{a \in \mathcal{A}_{r_i}} \tau(M^{r_i}_a \, M^{ij}_{a(s_{ij})}) &= \sum_{b \in \mathcal{A}_{\mathrm{vars}}} \sum_{\substack{a \in \mathcal{A}_{r_i} \\ a(s_{ij}) = b}} \tau(M^{r_i}_a \, M^{ij}_b) \\
&= \sum_{b \in \mathcal{A}_{\mathrm{vars}}} \tau(M^{ij}_b \, M^{ij}_b) = \sum_{b \in \mathcal{A}_{\mathrm{vars}}} \tau(M^{ij}_b) = \tau(1) = 1
\end{aligned}$$

and the probability that the constraint player's assignment satisfies equation r_i is

$$\begin{aligned}
\sum_{\substack{a \in \mathcal{A}_{r_i} \\ a(s_{i1}) + a(s_{i2}) + a(s_{i3}) = 0}} \tau(M^{r_i}_a) &\geq \sum_{a \in \mathcal{A}_{r_i}} (-1)^{a(s_{i1}) + a(s_{i2}) + a(s_{i3})} \tau(M^{r_i}_a) \\
&= \sum_{a \in \mathcal{A}_{r_i}} (-1)^{a(s_{i1}) + a(s_{i2}) + a(s_{i3})} \tau(M^{i1}_{a(s_{i1})} \, M^{i2}_{a(s_{i2})} \, M^{i3}_{a(s_{i3})}) \\
&= \tau(O^{i1} \, O^{i2} \, O^{i3}) = \tau(1) = 1.
\end{aligned}$$

A similar calculation holds for question pairs (c_j, s_{ij}). Since conditioned on any question pair the winning probability is 1, we conclude that $\omega(\mathrm{MS}, \mathscr{S}) = 1$. It should also be clear that this strategy is oracularizable, meaning that measurements corresponding to nontrivial question pairs commute. Finally, letting O^{ij} be the Pauli observables in Figure 1.2, we obtain a finite dimensional oracularizable perfect synchronous strategy for the Magic Square game defined over the Hilbert space $\mathbb{C}^4$.

We now establish the rigidity of the Magic Square game. Let $\mathscr{S} = (\tau, \{M^x\})$ denote a synchronous strategy for the Magic Square game. Each $\{M^{ij}_b\}_{b \in \mathcal{A}_{\mathrm{MS}}}$ is a projective measurement with outcomes $b \in \mathcal{A}_{\mathrm{MS}}$. Without loss of generality, we assume that the measurements corresponding to variable questions s_{ij} only produce either 0 or 1 as answers, i.e.,

$$M^{ij}_0 + M^{ij}_1 = 1 \; . \tag{1.3.3}$$

This is because for variable questions we can always define M_1^{ij} to be the orthogonal projection $1 - M_0^{ij}$, and this cannot decrease the winning probability. Similarly, without loss of generality, we assume that the projective measurement $\{M_a^e\}_{a \in \mathcal{A}_{\mathrm{MS}}}$ corresponding to constraint question e only produces assignments in $\mathcal{A}_e$, that is $\sum_{a \in \mathcal{A}_e} M_a^e = 1$.

For every variable $s_{ij} \in \mathcal{X}_{\mathrm{vars}}$, define the observable

$$O^{ij} = M_0^{ij} - M_1^{ij} \ .$$

Note that O^{ij} is a self-adjoint unitary operator (because of the assumption in eq. (1.3.3)) and that M_b^{ij} is a projection onto an eigenspace of O^{ij}.

The rigidity of the Magic Square game is expressed in the following way: if $\mathcal{S}$ is an (approximately) optimal strategy for the Magic Square game, then the observables must (approximately) satisfy the algebraic relations **R1**, **R2**, and **R3**.

Theorem 1.21 (Rigidity of Magic Square)**.** *Let $\mathcal{S} = (\tau, \{M^x\})$ be a synchronous strategy such that $\omega(\mathrm{MS}, \mathcal{S}) \geq 1 - \varepsilon$. Let $\{O^{ij}\}$ denote the observables associated to the strategy. Then*

1. *(**R1**) The product of observables in a row or column approximately multiply to* 1*, except in the last column, where they approximately multiply to* -1*:*

$$\begin{aligned} O^{i1}\, O^{i2}\, O^{i3} &\approx_{\delta(\varepsilon)} 1 \quad \textit{for } i = 1, 2, 3, \\ O^{1j}\, O^{2j}\, O^{3j} &\approx_{\delta(\varepsilon)} 1 \quad \textit{for } j = 1, 2, \\ O^{13}\, O^{23}\, O^{33} &\approx_{\delta(\varepsilon)} -1 \ . \end{aligned}$$

2. *(**R2**) Two observables in the same row or column approximately commute with each other, that is for all $i, j, k \in [3]$*

$$\begin{aligned} O^{ij}\, O^{ik} &\approx_{\delta(\varepsilon)} O^{ik}\, O^{ij} \ , \\ O^{ji}\, O^{ki} &\approx_{\delta(\varepsilon)} O^{ki}\, O^{ji} \ . \end{aligned}$$

3. *(**R3**) Two observables not in the same row or column anti-commute with each other, so for example*

$$O^{11}\,O^{22} \approx_{\delta(\varepsilon)} -O^{22}\,O^{11}\;, O^{12}\,O^{21} \approx_{\delta(\varepsilon)} -O^{21}\,O^{12}\;,$$

In all of these approximations δ is some proper error function such that $\delta(\varepsilon) \leq 32|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}$.

Proof. We saw earlier that **R3** is implied by **R1** and **R2**. This is also the main idea behind the proof here. We first show that $\{O^{ij}\}$ approximately satisfies **R1** and **R2**, then we use a derivation similar to (1.3.1), to conclude that **R3** is approximately satisfied.

We can deduce a number of consistency conditions from the fact that the strategy $\mathcal{S}$ succeeds with probability at least $1-\varepsilon$. First, by a simple averaging argument, since every question pair $(x, y) \in \mathcal{X}_{\mathrm{MS}} \times \mathcal{X}_{\mathrm{MS}}$ is sampled uniformly at random, the winning probability conditioned on players receiving any fixed question pair (x, y) is at least $1 - |\mathcal{X}_{\mathrm{MS}}|^2$.

As a notation aid, let $R^i_a = M^{r_i}_a$ denote a row measurement operator and $C^j_a = M^{c_j}_a$ denote a column measurement operator. By the winning conditions in Table 1.1, the constraint and variable players' answers must be consistent with high probability. In other words $\sum_{a\in\mathcal{A}_{r_i}} \mathrm{TR}\left(R^i_a\, M^{ij}_{a(s_{ij})}\right)$ is at least as large as the probability of winning conditioned on players receiving question pair (r_i, s_{ij}) for every $i, j \in [3]$. So from our remark earlier, we have

$$\sum_{a\in\mathcal{A}_{r_i}} \mathrm{TR}\left(R^i_a\, M^{ij}_{a(s_{ij})}\right) \geq 1 - |\mathcal{X}_{\mathrm{MS}}|^2\varepsilon\;. \tag{1.3.4}$$

For every row measurement operator R^i_a we define marginal projection operators: for $j \in [3]$ and $b \in \{0, 1\}$ define

$$R^{ij}_b = \sum_{a\in\mathcal{A}_{r_i}:\; a(s_{ij})=b} R^i_a$$

where the summation is over assignments a that assigns value b to variable s_{ij}. This is a projection and notice that for all assignments a to variables in r_i, we have

$$R^i_a = R^{i1}_{a(s_{i1})} \cdot R^{i2}_{a(s_{i2})} \cdot R^{i3}_{a(s_{i3})}\;.$$

It is also clear that $\{R_b^{ij}\}_{b\in\{0,1\}}$ forms a projective measurement. We can similarly define, for all columns j and variables s_{ij}, projective measurement $\{C_b^{ji}\}$ consisting of operators

$$C_b^{ji} = \sum_{a\in\mathcal{A}_{c_j}:\ a(s_{ij})=b} C_a^j.$$

We can rewrite (1.3.4) in terms of projective measurements $\{R_b^{ij}\}_{b\in\{0,1\}}$ as follows

$$1 - |\mathcal{X}_{\mathrm{MS}}|^2\varepsilon \leq \sum_{a\in\mathcal{A}_{r_i}} \mathrm{TR}\left(R_a^i\, M_{a(s_{ij})}^{ij}\right) = \sum_{b\in\mathcal{A}_{\mathrm{vars}}}\ \sum_{\substack{a\in\mathcal{A}_{r_i}:\\ a(s_{ij})=b}} \mathrm{TR}\left(R_a^i\, M_b^{ij}\right) = \sum_{b\in\mathcal{A}_{\mathrm{vars}}} \mathrm{TR}\left(R_b^{ij}\, M_b^{ij}\right).$$

Using the notation for consistency between measurements, we can equivalently express this as

$$R_b^{ij} \simeq_{|\mathcal{X}_{\mathrm{MS}}|^2\varepsilon} M_b^{ij}\ ,$$

where the answer set is $\mathcal{A}_{\mathrm{vars}} = \{0,1\}$. By Theorem 1.13, we convert consistency to closeness to obtain

$$R_b^{ij} \approx_{|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} M_b^{ij}\ ,$$

and with a similar argument for columns we get that

$$C_b^{ji} \approx_{|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} M_b^{ij}\ .$$

At this point it will be more convenient for us to work with observables, rather than projection operators. We have already defined observable O^{ij} for each variable s_{ij}; we now define observables corresponding to the (marginal) constraint operators: for all $i, j \in [3]$, define

$$R^{ij} = R_0^{ij} - R_1^{ij} \qquad \text{and} \qquad C^{ji} = C_0^{ji} - C_1^{ji}\ .$$

The closeness between constraints and variable projective measurements can be expressed also in terms of observables using the triangle inequality

$$\|O^{ij} - R^{ij}\|_\tau^2 \leq 2\|M_0^{ij} - R_0^{ij}\|_\tau^2 + 2\|M_1^{ij} - R_1^{ij}\|_\tau^2 \leq 4|\mathcal{X}_{\mathrm{MS}}|^2\varepsilon.$$

The same holds for columns, therefore overall we have proved that

$$O^{ij} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} R^{ij} \;, \tag{1.3.5}$$

$$O^{ij} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} C^{ji}. \tag{1.3.6}$$

Now using these relations, we can prove that variable observables in the same row or column approximately commute. This follows from a few simple steps. First, by the triangle inequality, for every $i, j, k \in [3]$ we can write

$$\begin{aligned}\|O^{ij}\, O^{ik} - O^{ik}\, O^{ij}\|_\tau^2 &\leq 2\|O^{ij}\, O^{ik} - R^{ij}\, R^{ik}\|_\tau^2 + 2\|R^{ij}\, R^{ik} - R^{ik}\, R^{ij}\|_\tau^2 + 2\|R^{ik}\, R^{ij} - O^{ik}\, O^{ij}\|_\tau^2 \\ &= 2\|O^{ij}\, O^{ik} - R^{ij}\, R^{ik}\|_\tau^2 + 2\|R^{ik}\, R^{ij} - O^{ik}\, O^{ij}\|_\tau^2 \;. \end{aligned}\tag{1.3.7}$$

where we used the equality $R^{ij}\, R^{ik} = R^{ik}\, R^{ij}$ which follows from the fact that projections R_b^{ij} and R_c^{ik} are marginals of the same projective measurement $\{R_a^i\}_{a\in\mathcal{A}_{r_i}}$ and projections belonging to the same projective measurement commute. By Theorem 1.8, from (1.3.5), we get that $O^{ij}O^{ik} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} R^{ij}O^{ik}$. Again by Theorem 1.8, from (1.3.5), we get that $R^{ij}O^{ik} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} R^{ij}R^{ik}$. So by triangle inequality we have

$$\|O^{ij}\, O^{ik} - R^{ij}\, R^{ik}\|_\tau^2 \leq 2\|O^{ij}O^{ik} - R^{ij}O^{ik}\|_\tau^2 + 2\|O^{ij}R^{ik} - R^{ij}R^{ik}\|_\tau^2 \leq 16|\mathcal{X}_{\mathrm{MS}}|^2\varepsilon.$$

This is true for all $i, j, k \in [3]$, so in particular it also holds that

$$\|R^{ik}\, R^{ij} - O^{ik}\, O^{ij}\|_\tau^2 \leq 16|\mathcal{X}_{\mathrm{MS}}|^2\varepsilon.$$

Now plugging these in (1.3.7) we get that

$$\|O^{ij}\, O^{ik} - O^{ik}\, O^{ij}\|_\tau^2 \leq 32|\mathcal{X}_{\mathrm{MS}}|^2\varepsilon.$$

An identical argument can be applied to columns, so overall we proved

$$O^{ij}\, O^{ik} \approx_{4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} O^{ik}\, O^{ij}\ , \tag{1.3.8}$$

$$O^{ji}\, O^{ki} \approx_{4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} O^{ki}\, O^{ji}\ , \tag{1.3.9}$$

for every $i, j, k \in [3]$.

As mentioned in Section 1.2.5, in this paper we do not need to keep track of the specific approximation bounds. As such, instead of carrying around subscripts like $4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}$ in our approximations, we opt to instead write $O^{ij} \approx_{\delta(\varepsilon)} R^{ij}$ where δ is some error function such that $\delta(\varepsilon) \to 0$ as $\varepsilon \to 0$. For example in the rest of this paper the argument above will be abbreviated as follows: From $O^{ij} \approx_{\delta(\varepsilon)} R^{ij}$ for all $i, j \in [3]$ and repeated applications of Theorem 1.8, we obtain

$$O^{ij}\, O^{ik} \approx_{\delta(\varepsilon)} R^{ij}\, R^{ik} = R^{ik}\, R^{ij} \approx_{\delta(\varepsilon)} O^{ik}\, O^{ij}\ ,$$

so by the triangle inequality

$$O^{ij}\, O^{ik} \approx_{\delta(\varepsilon)} O^{ik}\, O^{ij}\ ,$$

where $\delta(\varepsilon)$ are proper error functions. It is only in this proof that, for the benefit of the reader who sees these approximations for the first time, we tried to give the arguments in full details and kept track of all the error functions.

So far we obtained consequences of the fact that in a strategy with large winning probability the constraint and variable players' answers are consistent with high probability. There are some other relations that must hold in any approximately optimal strategy. For instance, with high probability, the measurement outcome of a constraint measurement $\{M_a^e\}_{a\in\mathcal{A}_e}$ must be a satisfying assignment for the constraint e. Let us make this more precise. The probability of winning conditioned on players receiving question pair (r_i, s_{ij}) is at least $1 - |\mathcal{X}_{\mathrm{MS}}|^2\varepsilon$. By winning conditions in Table 1.1, if players win on question pair (r_i, s_{ij}), then the assignment by the player receiving question r_i must satisfy constraint r_i. So we can write

$$\sum_{\substack{a\in\mathcal{A}_{r_i}\\ a(s_{i1})+a(s_{i2})+a(s_{i3}))=0}} \mathrm{TR}\left(R^i_a\right) \geq 1 - |\mathcal{X}_{\mathrm{MS}}|^2\varepsilon.$$

Now from the fact that $\{R^i_a\}_{a\in\mathcal{A}_{r_i}}$ is a projective measurement, we get that

$$\sum_{a\in\mathcal{A}_{r_i}} (-1)^{a(s_{i1})+a(s_{i2})+a(s_{i3})}\mathrm{TR}\left(R^i_a\right) \geq 1 - 2|\mathcal{X}_{\mathrm{MS}}|^2\varepsilon,$$

and in terms of observables this can be equivalently written as

$$\mathrm{TR}\left(R^{i1}R^{i2}R^{i3}\right) \geq 1 - 2|\mathcal{X}_{\mathrm{MS}}|^2\varepsilon\ .$$

By Theorem 1.9, we get that

$$R^{i1}\,R^{i2}\,R^{i3} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} 1 \quad \text{for } i = 1, 2, 3\ . \tag{1.3.10}$$

Doing the same for columns we get

$$C^{j1}\,C^{j2}\,C^{j3} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} 1 \quad \text{for } j = 1, 2$$

and

$$C^{31}\,C^{32}\,C^{33} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} -1$$

Now by (1.3.5) and (1.3.10), and repeated applications of Theorem 1.8 and the triangle inequality, for every $i \in [3]$, we obtain

$$\begin{aligned}\|O^{i1}\, O^{i2}\, O^{i3}\|_\tau^2 &\leq 2\|O^{i1}\, O^{i2}\, O^{i3} - R^{i1}\, O^{i2}\, O^{i3}\|_\tau^2 + 2\|R^{i1}\, O^{i2}\, O^{i3} - R^{i1}\, R^{i2}\, O^{i3}\|_\tau^2 \\ &\quad + 2\|R^{i1}\, R^{i2}\, O^{i3} - R^{i1}\, R^{i2}\, R^{i3}\|_\tau^2 + 2\|R^{i1}\, R^{i2}\, R^{i3} - 1\|_\tau^2 \\ &\leq 32|\mathcal{X}_{\mathrm{MS}}|^2\varepsilon.\end{aligned}$$

Therefore we have

$$O^{i1}\, O^{i2}\, O^{i3} \approx_{4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} 1 \quad \text{for } i = 1, 2, 3, \tag{1.3.11}$$

and following the same argument for columns

$$O^{1j}\, O^{2j}\, O^{3j} \approx_{4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} 1 \quad \text{for } j = 1, 2, \tag{1.3.12}$$

$$O^{13}\, O^{23}\, O^{33} \approx_{4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} -1\ . \tag{1.3.13}$$

Finally to prove the approximate anticommutation $O^{11}\ O^{22} \approx -O^{22}O^{11}$, we follow the idea in the derivation 1.3.1: We start with $(O^{11}\ O^{22})^2$ and step by step, using relations (1.3.11)-(1.3.13), substitute O^{11} and O^{22} by unitaries that are nearby. By repeated applications of triangle inequality and Theorem 1.8 and the approximate relations we established so far, we can write

$$\begin{aligned}(O^{11}\ O^{22})^2 &\approx_{16|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} (O^{12}\ O^{13})(O^{23}\ O^{21})(O^{21}\ O^{31})(O^{32}\ O^{12}) \\ &= O^{12}(O^{13}\ O^{23})(O^{21}\ O^{21})(O^{31}\ O^{32})O^{12} \\ &= O^{12}(O^{13}\ O^{23})(O^{31}\ O^{32})O^{12} \\ &\approx_{8|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} -O^{12}\ O^{33}\ O^{33}\ O^{12} \\ &= -1,\end{aligned}$$

So altogether, with another application of triangle inequality, we obtain

$$\|(O^{11}\,O^{22})^2 + 1\|_\tau \leq 32|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}.$$

Now since $O^{11}O^{22}$ is a unitary and the τ-norm is unitarily invariant, we conclude that

$$\|O^{11}O^{22} + O^{22}O^{11}\|_\tau \leq 32|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}.$$

By symmetry, an almost identical argument can be applied to prove anticommutation relations for all other pairs of observables not in the same row or column. □

As mentioned, the rigidity of the Magic Square and CHSH games are important stepping stones for a number of results in quantum complexity theory and quantum cryptography. A crucial component of obtaining strong lower bounds on the complexity of approximating the value of nonlocal games has been through developing nonlocal games with *highly efficient* rigidity properties.

We measure efficiency via the tradeoff between the complexity of the game versus the complexity of the algebraic relations that (approximately) optimal strategies must satisfy. For example, the Magic Square game has $|\mathcal{X}_{\mathrm{MS}}|^2 = 15^2$ question pairs and a similar number of answer pairs, and (approximately) optimal strategies must give rise to two pairs of (approximately) anti-commuting observables $\{O^{11}, O^{22}\}$ and $\{O^{21}, O^{12}\}$, and furthermore these pairs must be *independent* in the sense that they (approximately) commute with each other. This implies that when the probability of winning is sufficiently close to 1, the dimension of the Hilbert space must be at least 4. We say that the Magic Square game *certifies* the existence of two independent anti-commuting observables and certifies a Hilbert space of dimension at least 4. This is a consequence of the following general statement:

Proposition 1.22. *Let $\mathscr{A}$ denote a von Neumann algebra on a separable Hilbert space $\mathcal{H}$ with a tracial state τ, and let $A^{(1)}, \ldots, A^{(n)}, B^{(1)}, \ldots, B^{(n)} \in \mathscr{A}$ denote self-adjoint unitary operators (i.e. observables). Suppose for some $\varepsilon \geq 0$ the following approximate commutation and anticommuta-*

tion relations hold:

$$\forall\, i, \qquad A^{(i)}B^{(i)} \approx_\varepsilon -B^{(i)}A^{(i)}$$

$$\forall\, i \neq j, \qquad A^{(i)}A^{(j)} \approx_\varepsilon A^{(j)}A^{(i)}\,, \qquad B^{(i)}B^{(j)} \approx_\varepsilon B^{(j)}B^{(i)}\,, \qquad A^{(i)}B^{(j)} \approx_\varepsilon B^{(j)}A^{(i)}\,.$$

Then, for all sufficiently small ε, it holds that $\dim \mathcal{H} \geq (1-\delta(\varepsilon))2^n$ *where $\delta(\varepsilon)$ is some proper error function.*

Proof. There is nothing to prove when $\mathcal{H}$ is infinite dimensional. So assume that $\mathcal{H}$ is finite dimensional. By Theorem 4.4.1 in [46], every finite dimensional von Neumann algebra is a direct sum of $B(\mathcal{H}^i)$ where $\mathcal{H}^i$ are finite dimensional Hilbert spaces. So without loss of generality we may assume $\mathscr{A} = B(\mathcal{H})$ and that $\tau(\cdot) = \mathrm{tr}(\cdot)/\dim \mathcal{H}$ is the dimension-normalized trace.

Let $\Pi_b^{(i)}$ be the projection onto $(-1)^b$-eigenspace of $A^{(i)}$. For every $s \in \{0,1\}^n$ let

$$M_s := \Big(\prod_{i=1}^{n} \Pi_{s_i}^{(i)}\Big)\Big(\prod_{i=1}^{n} \Pi_{s_i}^{(i)}\Big)^*\,.$$

These operators are clearly positive semidefinite and a simple inductive argument shows that $\sum_{s\in\{0,1\}^n} M_s = 1$. Therefore $\{M_s\}_{s\in\{0,1\}^n}$ is a POVM.

From approximate commutation relations between $A^{(i)}$s we get that any pair $\Pi_a^{(i)}$ and $\Pi_b^{(j)}$ must approximately commute. Therefore by repeated applications of Theorem 1.8, we get that

$$M_s^2 \approx_{\delta(\varepsilon)} M_s.$$

By Theorem 1.8 again, we obtain that $\tau(M_s - M_s^2) \leq \delta(\varepsilon)$ for every s. So by Theorem 1.17, there exists a projective measurement $\{P_s\}_{s\in\{0,1\}^n} \subset \mathscr{A}$ such that $P_s \approx_{\delta(\varepsilon)} M_s$.

By approximate anticommutation, we get $B^{(i)}\,A^{(i)}\,B^{(i)} \approx_{\delta(\varepsilon)} -A^{(i)}$. We can express this in terms of projective measurement $\{\Pi_0^{(i)}, \Pi_1^{(i)}\}$

$$B^{(i)}\,\Pi_0^{(i)}\,B^{(i)} - B^{(i)}\,\Pi_1^{(i)}\,B^{(i)} \approx_{\delta(\varepsilon)} \Pi_1^{(i)} - \Pi_0^{(i)}.$$

Using the relation $\Pi_0^{(i)} + \Pi_1^{(i)} = 1$, we conclude that

$$B^{(i)}\, \Pi_0^{(i)}\, B^{(i)} \approx_{\delta(\varepsilon)} \Pi_1^{(i)}. \tag{1.3.14}$$

Now if we define unitary operators $U_{s,t} := \prod_{i=1}^{n} (B^{(i)})^{s_i+t_i}$, it is straightforward to show that

$$U_{s,t}\, M_s\, U_{s,t}^{*} \approx_{\delta(\varepsilon)} M_t$$

for every $s, t \in \{0,1\}^n$ using (1.3.14) and approximate commutation and anticommutations between A and B operators. This immediately implies that

$$\tau(M_t) \approx_{\delta(\varepsilon)} \tau(U_{s,t}\, M_s\, U_{s,t}^{*}) = \tau(M_s).$$

Now since projections $\{P_s\}$ are close to operators $\{M_s\}$ we also have $\tau(P_s) \approx_{\delta(\varepsilon)} \tau(P_t)$ for every s, t.

From $\tau(\sum_s P_s) = \tau(1) = 1$ and the fact that $\tau(P_s) \approx \tau(P_t)$ for every $s, t \in \{0,1\}^n$, we get that $\tau(P_s) \approx_{\delta(\varepsilon)} 2^{-n}$. In other words we have

$$(1 - \delta(\varepsilon))2^{-n} \leq \tau(P_s) \leq (1 + \delta(\varepsilon))2^{-n}$$

for every s. For all ε sufficiently small, we have $\delta(\varepsilon) < 1$, and thus $\tau(P_s) > 0$. Since P_s is a projection and it is nonzero it must be that $\mathrm{tr}(P_s) \geq 1$ so $\tau(P_s) = \mathrm{tr}(P_s)/\dim \mathcal{H} \geq 1/\dim \mathcal{H}$. We can write

$$1/\dim \mathcal{H} \leq \tau(P_s) \leq (1 + \delta(\varepsilon))2^{-n}$$

from which we conclude that

$$\dim \mathcal{H} \geq \frac{2^n}{1 + \delta(\varepsilon)} \geq (1 - \delta(\varepsilon))2^n.$$

□

It is possible to construct games that certify a larger Hilbert space. An example is the *n-fold parallel repetition* of the Magic Square game, which is a nonlocal game where the verifier plays n independent instances of the Magic Square game simultaneously with the two players. This game is also rigid, and it certifies $2n$ pairs of independent anti-commuting observables and consequently, by the proposition we just proved, certifies a Hilbert space of dimension 2^{2n}. However the complexity of the game also scales commensurately with the dimension: the number of questions and answers grows as $2^{O(n)}$.

Are there games that certify a d-dimensional Hilbert space using much fewer than d questions/answer pairs? Chao, Reichardt, Sutherland and Vidick [47] and Natarajan and Vidick [21] showed that there exist families of games $\{G_n\}$ where the n-th game G_n certifies a 2^n-dimensional space using $\mathrm{poly}(n)$ question/answer pairs. The rigidity result of [21] is also highly *robust*, in the sense that strategies for G_n that succeed with probability $1-\varepsilon$ must be $\delta(\varepsilon)$-close to satisfying the target algebraic relations, for some function $\delta(\varepsilon)$ that has a mild (e.g., logarithmic) dependence on n. The existence of games with efficient and robust rigidity properties is a key component of the gap-preserving compression theorem of [4].[11]

For our gapless compression result, we only need games with efficient rigidity properties (i.e., small game certifying a large Hilbert space), not necessarily highly robust ones. In this paper we use a family of games that we call *2-out-of-n Magic Square*, which is inspired by the family of games introduced in [47], which we call 2-out-of-n CHSH. We describe the 2-out-of-n Magic Square games next.

1.3.2 The 2-out-of-n Magic Square game

Fix an integer $n > 0$. The basic idea behind the 2-out-of-n Magic Square game, abbreviated 2-OF-n-MS, is that the players are asked to play n simultaneous instances of the Magic Square

[11] In fact, the result of [4] implies that one can construct games with m questions/answers that certify d-dimensional Hilbert spaces, and d can be an arbitrarily large (computable) function of m!

game, but the verifier only asks the players for their responses for 2 instances. Define the question set $\mathcal{X}_{2\text{-OF-}n\text{-MS}} = \{(i,j) \in [n]^2 : i \neq j\} \times \mathcal{X}_{\mathrm{MS}}^2$, and the answer set $\mathcal{A}_{2\text{-OF-}n\text{-MS}} = \mathcal{A}_{\mathrm{MS}}^2$. The decision predicate $D_{2\text{-OF-}n\text{-MS}}(q,r,a,b)$ is specified as follows, via its nontrivial question pairs and the corresponding winning conditions for the answers.

Nontrivial Question Pair (q,r)	**Winning Condition on Answers** (a,b)
$q = r$	$a = b$
$q = (i,j,x_i,x_j), r = (k,\ell,y_k,y_\ell)$ where $\{i,j\} \cap \{k,\ell\} \neq \emptyset$, and for all w in the intersection, (x_w,y_w) is a nontrivial question pair for MS	$D_{\mathrm{MS}}(x_w,y_w,u_w,v_w) = 1$ for all $w \in \{i,j\} \cap \{k,\ell\}$ where $a = (u_i,u_j), b = (v_k,v_\ell)$

Table 1.2: The nontrivial question pairs and winning conditions for the 2-OF-n-MS.

In other words, each player gets asked to generate answers for two instances of the Magic Square game, but do not know what instances the other player is asked about. If there is an instance i that is asked to both players, then their questions and answers for instance i must satisfy the Magic Square decision predicate.

It is easy to see that the 2-OF-n-MS has a perfect synchronous strategy: let $\mathcal{S}_{\mathrm{MS}} = (\tau, \{M^x\})$, where τ is a tracial state on some von Neumann algebra $\mathscr{A}$ on a Hilbert space $\mathcal{H}$, denote the perfect strategy for the Magic Square game described above. Then define the synchronous strategy $\mathcal{S}_{2\text{-OF-}n\text{-MS}} = (\tau^{\otimes n}, \{M^{i,j,x,y}\})$, where $M^{i,j,x,y} = \{M_{a,b}^{i,j,x,y}\}_{a,b \in \mathcal{A}_{\mathrm{MS}}}$ is the projective measurement defined such that

$$M_{a,b}^{i,j,x,y} := 1 \otimes \cdots \otimes 1 \otimes M_a^x \otimes 1 \otimes \cdots \otimes 1 \otimes M_b^y \otimes 1 \otimes \cdots \otimes 1 \in \mathscr{A}^{\otimes n}$$

in which M_a^x and M_b^y are acting on the ith and jth copy of $\mathcal{H}$, respectively. Intuitively if a player receives the question (i,j,x,y) they perform independent Magic Square measurements corresponding to questions x and y on the i-th and j-th copy of $\mathcal{H}$, respectively, and respond with their measurement outcomes. Clearly, the players’ will win the instances that are shared between them. The oracularizability of this strategy follows from the oracularizablity of the honest strategy of the Magic Square game and the construction above: for example if (x_i, y_i) is a nontrivial question pair in the Magic Square game, then measurements M^{i,j,x_i,x_j} and M^{i,k,y_i,y_k} commute for all $j \neq k$ since measurements M^{x_i} and M^{y_i} commute by the oracularizability of the honest Magic Square strategy from the previous section.

The next lemma expresses the rigidity properties of the 2-OF-n-MS. Let $\{M_{a,b}^{i,j,x,y}\}_{a,b\in\mathcal{A}_{\mathrm{MS}}}$ denote a measurement corresponding to a question $(i,j,x,y) \in \mathcal{X}_{2\text{-OF-}n\text{-MS}}$. Define the marginal measurement operator

$$M_a^{i,x} = \sum_b M_{a,b}^{i,\mathrm{succ}(i),x,x}$$

where the sum is over answers $b \in \mathcal{A}_{\mathrm{MS}}$ and $\mathrm{succ}(i) = \begin{cases} i+1, & i<n, \\ 1, & i=n. \end{cases}$

Note that for all $(i,x) \in [n] \times \mathcal{X}_{\mathrm{MS}}$, the set $\{M_a^{i,x}\}_{a\in\mathcal{A}_{\mathrm{MS}}}$ forms a projective measurement. Just like with strategies for the Magic Square game, when x is a variable question in the Magic Square game (i.e. it is s_{cd} for some $c,d \in [3]$), we assume without loss of generality that

$$M_0^{i,s_{cd}} + M_1^{i,s_{cd}} = 1$$

for all $i \in [n], c,d \in [3]$. For each variable s_{cd} define the corresponding observable

$$O^{i,c,d} = M_0^{i,s_{cd}} - M_1^{i,s_{cd}} .$$

Lemma 1.23 (Rigidity of the 2-OF-n-MS)**.** *Let $\mathcal{S} = (\tau, \{M^x\})$ be a synchronous strategy such that $\omega(2\text{-OF-}n\text{-MS}, \mathcal{S}) \geq 1-\varepsilon$. For all $i \in [n]$ define*

$$A^{(2i-1)} = O^{i,1,1}\, , B^{(2i-1)} = O^{i,2,2}\, ,$$
$$A^{(2i)} = O^{i,1,2}\, , B^{(2i)} = O^{i,2,1}\, .$$

Then

$$\forall\, k \in [2n], \qquad A^{(k)}B^{(k)} \approx_\delta -B^{(k)}A^{(k)}$$

$$\forall\, k, l \in [2n] \textit{ and } k \neq l, \qquad A^{(k)}A^{(l)} \approx_\delta A^{(l)}A^{(k)}\,, \qquad B^{(k)}B^{(l)} \approx_\delta B^{(l)}B^{(k)}\,, \qquad A^{(k)}B^{(l)} \approx_\delta B^{(l)}A^{(k)}$$

where $\delta(n, \varepsilon) = \mathrm{poly}(n) \cdot \mathrm{poly}(\varepsilon)$ *is a proper error function.*

Proof. Fixing $i \in [n]$ and $x, y \in \mathcal{X}_{\mathrm{MS}}$, the probability of winning the instance i Magic Square game, conditioned on players receiving questions $(i, \mathrm{succ}(i), x, x)$ and $(i, \mathrm{succ}(i), y, y)$ is at least $1 - |\mathcal{X}_{\text{2-OF-}n\text{-MS}}|^2\varepsilon$, thus

$$\sum_{a,b} \tau(M_a^{i,x}\ M_b^{i,y}) D_{\mathrm{MS}}(x, y, a, b) \geq 1 - |\mathcal{X}_{\text{2-OF-}n\text{-MS}}|^2\varepsilon.$$

So conditioned on every question pair (x, y), the strategy $(\tau, \{M^{i,x}\}_{x\in\mathrm{MS}})$ wins in the Magic Square game with probability at least

$$1 - |\mathcal{X}_{\text{2-OF-}n\text{-MS}}|^2\varepsilon = 1 - \mathrm{poly}(n, \varepsilon).$$

Therefore by Theorem 1.21, for every $i \in [n]$, we have

$$A^{(2i-1)}\,B^{(2i-1)} \approx_{\mathrm{poly}(n,\varepsilon)} -B^{(2i-1)}\,A^{(2i-1)}\,, A^{(2i)}\,B^{(2i)} \approx_{\mathrm{poly}(n,\varepsilon)} -B^{(2i)}\,A^{(2i)}\,,$$
$$A^{(2i-1)}\,A^{(2i)} \approx_{\mathrm{poly}(n,\varepsilon)} A^{(2i)}\,A^{(2i-1)}\,, B^{(2i-1)}\,B^{(2i)} \approx_{\mathrm{poly}(n,\varepsilon)} B^{(2i)}\,B^{(2i-1)}\,,$$
$$A^{(2i-1)}\,B^{(2i)} \approx_{\mathrm{poly}(n,\varepsilon)} B^{(2i)}\,A^{(2i-1)}\,, B^{(2i-1)}\,A^{(2i)} \approx_{\mathrm{poly}(n,\varepsilon)} A^{(2i)}\,B^{(2i-1)}\,.$$

It is only left to prove that when $k, l \in [2n]$ and $|k - l| > 1$, it holds that

$$A^{(k)}A^{(l)} \approx_\delta A^{(l)}A^{(k)}\,, \qquad B^{(k)}B^{(l)} \approx_\delta B^{(l)}B^{(k)}\,, \qquad A^{(k)}B^{(l)} \approx_\delta B^{(l)}A^{(k)}.$$

We prove the stronger statement that $M_a^{i,x}\, M_b^{j,y} \approx_\delta M_b^{j,x}\, M_a^{i,y}$ for all $i, j \in [n], i \neq j, x, y \in$

$\mathcal{X}_{\mathrm{MS}}, a, b \in \mathcal{A}_{\mathrm{MS}}$.

We give the proof for the case where $j \neq \mathrm{succ}(i)$ and $i \neq \mathrm{succ}(j)$. The proof for the other cases follow the same idea. The proof is based on the cross-check between nontrivial question pair $(i, \mathrm{succ}(i), x, x)$ and (i, j, x, y) on one hand and the cross-check between nontrivial question pair (i, j, x, y) and $(j, \mathrm{succ}(j), y, y)$ on the other hand. We derive consequences of the fact that, conditioned on players receiving questions $(i, \mathrm{succ}(i), x, x)$ and (i, j, x, y), they win instance i of the Magic Square with high probability. Similarly we derive consequences of the fact that, conditioned on players receiving questions $(j, \mathrm{succ}(j), y, y)$ and (i, j, x, y), they win instance j of Magic Square with high probability. The consequences we derive are then used to prove the desired approximate commutation relations.

Recall that by the winning conditions of the Magic Square game, if players win (in the Magic Square game) when receiving the same question, then they must have responded with the same answer. This can be expressed as

$$\sum_{a \in \mathcal{A}_{\mathrm{MS}}} \sum_{b,c \in \mathcal{A}_{\mathrm{MS}}} \tau(M_{a,b}^{i,\mathrm{succ}(i),x,x} \, M_{a,c}^{i,j,x,y}) \geq 1 - |\mathcal{X}_{2\text{-OF-}n\text{-MS}}|^2 \varepsilon \,,$$

or in other words

$$\sum_{a \in \mathcal{A}_{\mathrm{MS}}} \tau(M_a^{i,x} \sum_c M_{a,c}^{i,j,x,y}) \geq 1 - |\mathcal{X}_{2\text{-OF-}n\text{-MS}}|^2 \varepsilon \,.$$

In terms of consistency relations this can be expressed as $M_a^{i,x} \simeq_\delta \sum_c M_{a,c}^{i,j,x,y}$.

Similarly we have

$$\sum_{b \in \mathcal{A}_{\mathrm{MS}}} \sum_{c,d \in \mathcal{A}_{\mathrm{MS}}} \tau(M_{b,c}^{j,\mathrm{succ}(j),y,y} \, M_{d,b}^{i,j,x,y}) \geq 1 - |\mathcal{X}_{2\text{-OF-}n\text{-MS}}|^2 \varepsilon \,,$$

or in other words

$$\sum_{a \in \mathcal{A}_{\text{MS}}} \tau(M_b^{j,y} \sum_d M_{d,b}^{i,j,x,y}) \geq 1 - |\mathcal{X}_{\text{2-OF-}n\text{-MS}}|^2 \varepsilon \; .$$

In terms of consistency relations this can be expressed as $M_b^{j,y} \simeq_\delta \sum_c M_{c,b}^{i,j,x,y}$.

Using Theorem 1.13 we turn the consistency relations to the following closeness relations

$$M_a^{i,x} \approx_\delta \sum_c M_{a,c}^{i,j,x,y} \; , M_b^{j,y} \approx_\delta \sum_d M_{d,b}^{i,j,x,y} \; ,$$

where δ is some proper error function. Now using Theorem 1.8, we can write

$$\begin{aligned} M_a^{i,x} \, M_b^{j,y} &\approx \Big(\sum_c M_{a,c}^{i,j,x,y}\Big)\Big(\sum_d M_{d,b}^{i,j,x,y}\Big) \\ &= \Big(\sum_d M_{d,b}^{i,j,x,y}\Big)\Big(\sum_c M_{a,c}^{i,j,x,y}\Big) \\ &\approx M_b^{j,y} \, M_a^{i,x}, \end{aligned}$$

where the equality follows from the fact that projection operators belonging to the same projective measurement commute. □

Theorem 1.22 immediately implies that any strategy that succeeds for the 2-OF-n-MS with probability $1 - \varepsilon$ must be on a Hilbert space of dimension at least $(1 - \text{poly}(n)\text{poly}(\delta))2^{2n}$, which is nontrivial for $\delta < 1/\text{poly}(n)$. Furthermore, this game is highly efficient because the number of questions and answers grows only *polynomially* with n. Observe that

$$|\mathcal{X}_{\text{2-OF-}n\text{-MS}}| = n^2 \cdot |\mathcal{X}_{\text{MS}}|^2 \; , \qquad |\mathcal{A}_{\text{2-OF-}n\text{-MS}}| = |\mathcal{A}_{\text{MS}}|^2 \; ,$$

which means that the total number of question and answer pairs for the 2-OF-n-MS is $O(n^4)$, where we treat the question and answer sizes of the Magic Square game as constant.

1.3.3 The Question Sampling game

For readers who are familiar with quantum information theory, the 2-OF-n-MS can be understood in the following way. In the honest strategy for 2-OF-n-MS the two players share the state $|\mathrm{EPR}\rangle^{\otimes 2n}$ (i.e. $2n$ maximally entangled Bell pairs), and if we assume the perfect strategy for the Magic Square game is the one coming from Figure 1.2, the observables $A^{(1)}, \dots, A^{(2n)}, B^{(1)}, \dots, B^{(2n)}$, defined in Theorem 1.23, are $A^{(i)} = Z_i$ and $B^{(i)} = X_i$ where Z_i (resp. X_i) represents the $2n$-qubit operator with the Z (resp. X) Pauli operator acting on the i-th qubit and identity everywhere else. Then by the rigidity of 2-OF-n-MS, in any approximately optimal strategy, there are observable that are close to these Pauli operators. These Pauli operators act nontrivially only on a single qubit. However for the question reduction in Section 1.4, we need access to the measurements that simultaneously measure blocks of qubits. To achieve this goal, in this section, we extend the 2-OF-n-MS by including a few additional questions. By doing so, and as it becomes clear in a moment, we guarantee that any optimal strategy for the extended game must be using these block-qubit measurement operators.

We now introduce a family of synchronous games called *Question Sampling games*, denoted by $\mathrm{QS} = \{\mathrm{QS}_n\}_{n\in\mathbb{N}}$. The n-th Question Sampling game QS_n is an extension of the 2-OF-n-MS where there are four additional questions S_A, S_B, E_A, E_B, where S and E stand for *sample* and *erase*, respectively. The answers for these additional questions are n-bit strings.

In the honest strategy for the Question Sampling game (which we formally introduce in a moment), the S_A (resp. S_B) measurement is supposed to correspond to measuring the first n (resp. second n) EPR pairs in the standard basis, whereas the E_A (resp. E_B) measurement is supposed to correspond to measuring the first n (resp. second n) EPR pairs in a complementary basis.

The rigidity of the 2-OF-n-MS (Theorem 1.23) implies that measurements of strategy with high winning probability give rise to $2n$ pairs of (approximately) anticommuting observables $(A^{(i)}, B^{(i)})_{i\in[2n]}$, and the observables (approximately) commute across different pairs. This rigidity guarantee is also present for the Question Sampling game QS_n, but furthermore the measurements corresponding to the additional questions also satisfy the following:

- The measurements corresponding to S_A (resp. S_B) are approximately consistent with "simultaneously measuring" the observables $A^{(1)}, \dots, A^{(n)}$ (resp. $A^{(n+1)}, \dots, A^{(2n)}$) to produce an n-bit string answer.
- The measurements corresponding to E_A (resp. E_B) are approximately consistent with "simultaneously measuring" the observables $B^{(1)}, \dots, B^{(n)}$ (resp. $B^{(n+1)}, \dots, B^{(2n)}$) to produce an n-bit string answer.

Here, "approximate consistency" is used in the sense defined in Section 1.2.2. Furthermore, since the observables referred to in each item above only approximately commute with each other, the notion of simultaneous measurement is only meant in an approximate sense; we formalize this below in Theorem 1.24.

We now formally define the game $\mathrm{QS}_n = (Q_n, \mathcal{X}_n, D_{\mathrm{QS}_n})$. Its question set is defined to be $Q_n = \mathcal{X}_{2\text{-OF-}n\text{-MS}} \cup \{S_A, S_B, E_A, E_B\}$, and thus $|Q_n| = \mathrm{poly}(n)$. Its answer set is defined to be $\mathcal{X}_n = \mathcal{A}_{2\text{-OF-}n\text{-MS}} \cup \{0,1\}^n$, and thus $|\mathcal{X}_n| = O(2^n)$.

Remark 3. *The Question Sampling game and the Introspection game, appearing in the next section, are the only games in this paper for which we use the symbol Q (instead of $\mathcal{X}$) to refer to the question set. In fact, for the Question Sampling game the letter $\mathcal{X}$ is reserved for the answer set. The reason for this convention is because, as the name suggests, the Question Sampling game is meant to sample a question pair (x, y) for another game (this should become clearer in the section on Introspection games).*

The nontrivial questions and winning conditions of the decision procedure $D_{\mathrm{QS}_n}(q, r, x, y)$ are specified as follows (note that the answers are now denoted (x, y)). We only consider the case of even n. The case of odd n is slightly more tedious to write down.

Nontrivial Question Pair (q,r)	**Winning Condition on Answers** (x,y)
$q = r$	$x = y$
(q,r) is a nontrivial question for 2-OF-n-MS	$D_{2\text{-OF-}n\text{-MS}}(q,r,x,y) = 1$
$q = (i,j,s_{11},.) \in \mathcal{X}_{2\text{-OF-}n\text{-MS}}$ where $i \leq \frac{n}{2}, j > \frac{n}{2}$, and $r = S_A$	$x = (a_i,a_j) \in \mathcal{A}^2_{\text{MS}}, y \in \{0,1\}^n$, and $y_{2i-1} = a_i$
$q = (i,j,s_{12},.) \in \mathcal{X}_{2\text{-OF-}n\text{-MS}}$ where $i \leq \frac{n}{2}, j > \frac{n}{2}$, and $r = S_A$	$x = (a_i,a_j) \in \mathcal{A}^2_{\text{MS}}, y \in \{0,1\}^n$, and $y_{2i} = a_i$
$q = (i,j,s_{11},.) \in \mathcal{X}_{2\text{-OF-}n\text{-MS}}$ where $i > \frac{n}{2}, j \leq \frac{n}{2}$, and $r = S_B$	$x = (a_i,a_j) \in \mathcal{A}^2_{\text{MS}}, y \in \{0,1\}^n$, and $y_{2(i-\frac{n}{2})-1} = a_i$
$q = (i,j,s_{12},.) \in \mathcal{X}_{2\text{-OF-}n\text{-MS}}$ where $i > \frac{n}{2}, j \leq \frac{n}{2}$, and $r = S_B$	$x = (a_i,a_j) \in \mathcal{A}^2_{\text{MS}}, y \in \{0,1\}^n$, and $y_{2(i-\frac{n}{2})} = a_i$
$q = (i,j,s_{22},.) \in \mathcal{X}_{2\text{-OF-}n\text{-MS}}$ where $i \leq \frac{n}{2}, j > \frac{n}{2}$, and $r = E_A$	$x = (a_i,a_j) \in \mathcal{A}^2_{\text{MS}}, y \in \{0,1\}^n$, and $y_{2i-1} = a_i$
$q = (i,j,s_{21},.) \in \mathcal{X}_{2\text{-OF-}n\text{-MS}}$ where $i \leq \frac{n}{2}, j > \frac{n}{2}$, and $r = E_A$	$x = (a_i,a_j) \in \mathcal{A}^2_{\text{MS}}, y \in \{0,1\}^n$, and $y_{2i} = a_i$
$q = (i,j,s_{22},.) \in \mathcal{X}_{2\text{-OF-}n\text{-MS}}$ where $i > \frac{n}{2}, j \leq \frac{n}{2}$, and $r = E_B$	$x = (a_i,a_j) \in \mathcal{A}^2_{\text{MS}}, y \in \{0,1\}^n$, and $y_{2(i-\frac{n}{2})-1} = a_i$
$q = (i,j,s_{21},.) \in \mathcal{X}_{2\text{-OF-}n\text{-MS}}$ where $i > \frac{n}{2}, j \leq \frac{n}{2}$, and $r = E_B$	$x = (a_i,a_j) \in \mathcal{A}^2_{\text{MS}}, y \in \{0,1\}^n$, and $y_{2(i-\frac{n}{2})} = a_i$

Table 1.3: The nontrivial question pairs and winning conditions for the n-th Question Sampling game. We used dot for example in $(i,j,s_{11},.) \in \mathcal{X}_{2\text{-OF-}n\text{-MS}}$ to indicate that the fourth coordinate does not matter as long as the quadruple is a valid question in $\mathcal{X}_{2\text{-OF-}n\text{-MS}}$.

We now to describe an oracularizable synchronous strategy for QS_n with value 1. Let $\mathscr{S}_{\text{MS}} = (\tau, \{M^q\}_{q\in\mathcal{X}_{\text{MS}}})$ be the honest strategy for the Magic Square game on the Hilbert space $\mathcal{H}_{\text{MS}} = \mathbb{C}^4$ and let $\mathscr{S}_{2\text{-OF-}n\text{-MS}} = (\tau^{\otimes n}, \{M^q\}_{q\in\mathcal{X}_{2\text{-OF-}n\text{-MS}}})$ be its extension to a perfect oracularizable synchronous strategy for the 2-OF-n-MS as defined in Section 1.3.2. We extend this to a perfect finite-dimensional oracularizable synchronous strategy $\mathscr{S}_{\text{QS}_n}$ for QS_n.

For every $y \in \{0,1\}^n$ define

$$\begin{aligned}
M^{S_A}_y &:= M^{s_{11}}_{y_1} M^{s_{12}}_{y_2} \otimes M^{s_{11}}_{y_3} M^{s_{12}}_{y_4} \otimes \cdots \otimes M^{s_{11}}_{y_{n-1}} M^{s_{12}}_{y_n} \otimes 1_{\mathbb{C}^{2n}},\\
M^{S_B}_y &:= 1_{\mathbb{C}^{2n}} \otimes M^{s_{11}}_{y_1} M^{s_{12}}_{y_2} \otimes M^{s_{11}}_{y_3} M^{s_{12}}_{y_4} \otimes \cdots \otimes M^{s_{11}}_{y_{n-1}} M^{s_{12}}_{y_n},\\
M^{E_A}_y &:= M^{s_{22}}_{y_1} M^{s_{21}}_{y_2} \otimes M^{s_{22}}_{y_3} M^{s_{21}}_{y_4} \otimes \cdots \otimes M^{s_{22}}_{y_{n-1}} M^{s_{21}}_{y_n} \otimes 1_{\mathbb{C}^{2n}},\\
M^{E_B}_y &:= 1_{\mathbb{C}^{2n}} \otimes M^{s_{22}}_{y_1} M^{s_{21}}_{y_2} \otimes M^{s_{22}}_{y_3} M^{s_{21}}_{y_4} \otimes \cdots \otimes M^{s_{22}}_{y_{n-1}} M^{s_{21}}_{y_n}.
\end{aligned}$$

Note that measurements $M^{s_{11}}$ and $M^{s_{12}}$ (and similarly $M^{s_{22}}$ and $M^{s_{21}}$) of the honest Magic Square strategy commute as they belong to the same row. It is easily verified that $\{M^{S_A}_y\}, \{M^{S_B}_y\}, \{M^{E_A}_y\}, \{M^{E_B}_y\}$

are projective measurements and that $\mathcal{S}_{\mathrm{QS}_n} = (\tau^{\otimes n}, \{M^q\}_{q \in Q_{\mathrm{QS}_n}})$ is a synchronous strategy for QS_n.[12]

Next we show that $\mathcal{S}_{\mathrm{QS}_n}$ wins with probability 1. Fix an $i \leq \frac{n}{2}, j > \frac{n}{2}, t \in \mathcal{X}_{\mathrm{MS}}$. Conditioned on players receiving the nontrivial question pair $((i, j, s_{11}, t), S_A)$, which corresponds to the third row in Table 1.3, the probability of winning is

$$\sum_{a \in \mathcal{A}_{\mathrm{MS}}} \sum_{y \in \{0,1\}^n} \tau(M^{i,j,s_{11},t}_{y_{2i-1},a} M^{S_A}_y) = \sum_{y \in \{0,1\}^n} \tau(M^{i,s_{11}}_{y_{2i-1}} M^{S_A}_y) = \sum_{y \in \{0,1\}^n} \tau(M^{S_A}_y) = 1,$$

in which $M^{i,s_{11}}_{y_{2i-1}}$ is defined to be the marginal

$$M^{i,s_{11}}_{y_{2i-1}} \coloneqq \sum_{a \in \mathcal{A}_{\mathrm{MS}}} M^{i,j,s_{11},t}_{y_{2i-1},a} = 1^{i-1}_{\mathcal{H}_{\mathrm{MS}}} \otimes M^{s_{11}}_{y_{2i-1}} \otimes 1^{n-i-1}_{\mathcal{H}_{\mathrm{MS}}}.$$

It is similarly verified that the probability of winning conditioned on any other question pair is 1.

Since $\mathcal{S}_{2\text{-OF-}n\text{-MS}}$ is oracularizable in 2-OF-n-MS, to verify the oracularizability of $\mathcal{S}_{\mathrm{QS}_n}$ we just need to check commutativity between measurements for S_A, S_B, E_A, E_B on one hand and measurements for (i, j, q_i, q_j) on the other hand. This follows very easily from the construction of the measurements

$$M^{S_A}, M^{S_B}, M^{E_A}, M^{E_B}$$

Finally we note that in the honest strategy $\tau(M^{S_A}_x M^{S_B}_y) = 2^{-2n}$ (and similarly $\tau(M^{E_A}_x M^{E_B}_y) = 2^{-2n}$) for all $x, y \in \{0,1\}^n$. We see in a moment that approximately optimal strategies approximately satisfy these relations.

Let $\mathcal{S} = (\tau, \{M^q\}_{q \in Q_{\mathrm{QS}_n}})$ be a synchronous strategy for the Question Sampling game. For

[12] If we take the Magic Square strategy from Figure 1.2, these formulas simplify to

$$\begin{aligned} M^{S_A}_y &= |y\rangle\langle y| \otimes 1, \\ M^{S_B}_y &= 1 \otimes |y\rangle\langle y|, \\ M^{E_A}_y &= H^{\otimes n}|y\rangle\langle y|H^{\otimes n} \otimes 1, \\ M^{E_B}_y &= 1 \otimes H^{\otimes n}|y\rangle\langle y|H^{\otimes n}, \end{aligned}$$

where $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is the Hadamard transform.

convenience we use the notational shorthand

$$
\begin{aligned}
S_x^A &= M_x^{S_A} \qquad \text{and} \qquad S_x^B = M_x^{S_B} \\
E_x^A &= M_x^{E_A} \qquad \text{and} \qquad E_x^B = M_x^{E_B}
\end{aligned}
$$

for all $x \in \{0,1\}^n$. We also define a family of observables derived from these measurements as follows. For all $u \in \{0,1\}^n$,

$$
\begin{aligned}
O_u^{S_A} &= \sum_{x \in \{0,1\}^n} (-1)^{u \cdot x} S_x^A \qquad \text{and} \qquad O_u^{S_B} = \sum_{x \in \{0,1\}^n} (-1)^{u \cdot x} S_x^B \\
O_u^{E_A} &= \sum_{x \in \{0,1\}^n} (-1)^{u \cdot x} E_x^A \qquad \text{and} \qquad O_u^{E_B} = \sum_{x \in \{0,1\}^n} (-1)^{u \cdot x} E_x^B \,.
\end{aligned}
$$

Note that by construction these are self-adjoint unitaries, and therefore observables. We call S^A, S^B (resp. E^A, E^B) *sampling measurements* (resp. *erasure measurements*), and O^{S_A}, O^{S_B} (resp. O^{E_A}, O^{E_B}) *sampling observables* (resp. *erasure observables*) . In what follows we write $\overline{A} = B, \overline{B} = A$.

Theorem 1.24 (Rigidity of the Question Sampling game)**.** *Let $\mathscr{S} = (\tau, \{M^q\}_{q \in Q_n})$ be a synchronous strategy such that $\omega(\mathrm{QS}_n, \mathscr{S}) \geq 1 - \varepsilon$. Then for all $W \in \{A, B\}$,*

1. *The sampling (resp. erasure) measurements almost commute with one another, that is for every $x, y \in \{0,1\}^n$*

$$
S_x^A S_y^B \approx S_y^B S_x^A \qquad \textit{and} \qquad E_x^A E_y^B \approx E_y^B E_x^A \,.
$$

2. *Sampling measurements S_W almost commute with erasure measurements $E_{\overline{W}}$, that is, for every $x, y \in \{0,1\}^n$,*

$$
S_x^W E_y^{\overline{W}} \approx E_y^{\overline{W}} S_x^W .
$$

3. *The erasure observables O^{E_W} approximately permute the sampling measurements S^W and vice versa. That is, for every $u, x \in \{0,1\}^n$,*

$$O_u^{E_W} S_x^W O_u^{E_W} \approx S_{x+u}^W \qquad \textit{and} \qquad O_u^{S_W} E_x^W O_u^{S_W} \approx E_{x+u}^W \ .$$

   where the arithmetic in the subscript is bitwise XOR.

4. *Finally, for all $x, y \in \{0,1\}^n$,*

$$\tau(S_x^W) \approx 2^{-n} \qquad \textit{and} \qquad \tau(S_x^W S_y^{\overline{W}}) \approx 2^{-2n} \ ,$$
$$\tau(E_x^W) \approx 2^{-n} \qquad \textit{and} \qquad \tau(E_x^W E_y^{\overline{W}}) \approx 2^{-2n} \ .$$

We explained the usage of $\approx$ in Section 1.2.5. For a detailed example see the proof of Theorem 1.21.

Proof. By the winning conditions of the game, for all $i \leq n/2$ and $j > n/2$, we have

$$\begin{aligned} 1 - \delta(\varepsilon) &\geq \sum_{b,c \in \{0,1\}} \sum_{\substack{x \in \{0,1\}^n: \\ x_{2i-1} = b}} \mathrm{TR}\left(S_x^A M_{b,c}^{i,j,s_{11},s_{11}}\right) \\ &= \sum_{b \in \{0,1\}} \mathrm{TR}\left(S^A_{[x \mapsto x_{2i-1}|b]}\left(\sum_{c \in \{0,1\}} M_{b,c}^{i,j,s_{11},s_{11}}\right)\right). \end{aligned}$$

By the proof of rigidity of 2-OF-n-MS we have $M_b^{i,s_{11}} \approx \sum_{c \in \{0,1\}} M_{b,c}^{i,j,s_{11},s_{11}}$ where $M_b^{i,s_{11}}$ is the marginal $\sum_{c \in \{0,1\}} M_{b,c}^{i,\mathrm{succ}(i),s_{11},s_{11}}$ as defined in the previous section. So we can rewrite our earlier inequality as

$$\sum_{b \in \{0,1\}} \mathrm{TR}\left(S^A_{[x \mapsto x_{2i-1}|b]} M_b^{i,s_{11}}\right) \geq 1 - \delta(\varepsilon) \ .$$

Using Theorem 1.13 we can write this as closeness relation

$$S^A_{[x \mapsto x_{2i-1}|b]} \approx M_b^{i,s_{11}}.$$

With a similar argument we obtain

$$S^A_{[x\mapsto x_{2i}|b]} \approx M^{i,s_{12}}_b .$$

Now using the identity

$$S^A_x = \prod_{i=1}^{n} S^A_{[y\mapsto y_i|x_i]}$$

and repeated applications of Theorem 1.8, we obtain

$$S^A_x \approx \prod_{i=1}^{n/2} M^{i,s_{11}}_{x_{2i-1}} M^{i,s_{12}}_{x_{2i}} .$$

With a similar argument we obtain

$$S^B_x \approx \prod_{i=1}^{n/2} M^{i+n/2,s_{11}}_{x_{2i-1}} M^{i+n/2,s_{12}}_{x_{2i}} ,$$

$$E^A_x \approx \prod_{i=1}^{n/2} M^{i,s_{22}}_{x_{2i-1}} M^{i,s_{21}}_{x_{2i}} ,$$

$$E^B_x \approx \prod_{i=1}^{n/2} M^{i+n/2,s_{22}}_{x_{2i-1}} M^{i+n/2,s_{21}}_{x_{2i}} .$$

Now by the definition of the sampling and erasure observables, we have

$$O^{S_A}_u \approx (A^{(1)})^{u_1}(A^{(2)})^{u_2}\cdots(A^{(n)})^{u_n} ,$$

$$O^{S_A}_u \approx (A^{(n/2+1)})^{u_1}(A^{(n/2+2)})^{u_2}\cdots(A^{(n)})^{u_n} ,$$

$$O^{E_A}_u \approx (B^{(1)})^{u_1}(B^{(2)})^{u_2}\cdots(B^{(n)})^{u_n} ,$$

$$O^{E_A}_u \approx (B^{(n/2+1)})^{u_1}(B^{(n/2+2)})^{u_2}\cdots(B^{(n)})^{u_n} ,$$

where $A^{(i)}$ and $B^{(j)}$ are as defined in Theorem 1.23. Properties 1-3 now follow easily from the rigidity of 2-OF-n-MS in Theorem 1.23.

Finally, we prove 4 using 1-3. We have $O_x^{E_W} S_x^W O_x^{E_W} \approx S_{0^n}^W$ for every $x \in \{0,1\}^n$. Applying Proposition 1.8, we obtain $\tau(O_x^{E_W} S_x^W O_x^{E_W}) \approx \tau(S_{0^n}^W)$. By cyclicity of tracial states we have $\tau(S_x^W) \approx \tau(S_{0^n}^W)$. Now

$$1 = \tau(\sum_x S_x^W) \approx 2^n \tau(S_{0^n}^W),$$

from which we get that $\tau(M_{0^n}^{S_W}) \approx 2^{-n}$. Similarly $\tau(S_x^W) \approx 2^{-n}$ for $x \neq 0^n$.

Similar to the above line of reasoning, by repeated applications of Theorem 1.8 we have

$$\begin{aligned}
1 &= \sum_{x,y} \tau(S_x^W S_y^{\overline{W}}) \\
&= \sum_{x,y} \tau((O_x^{E_W})^2 (O_y^{E_{\overline{W}}})^2 S_x^W S_y^{\overline{W}}) \\
&\approx \sum_{x,y} \tau(O_x^{E_W} S_x^W O_x^{E_W} O_y^{E_{\overline{W}}} S_y^{\overline{W}} O_y^{E_{\overline{W}}}) \\
&\approx \sum_{x,y} \tau(S_{0^n}^W S_{0^n}^{\overline{W}}) \\
&= 2^{2n} \tau(S_{0^n}^W S_{0^n}^{\overline{W}}).
\end{aligned}$$

In the first approximation we used the fact that W operators approximately commute with $\overline{W}$ operators. The proof for erasure measurements is identical. □

Corollary 1.25 (Entanglement bound for Question Sampling). *Let $\mathcal{S} = (\tau, \{M^q\}_{q \in Q_n})$ be a synchronous strategy for* QS_n *over a von Neumann algebra $\mathscr{A} \subset B(\mathcal{H})$. If $\omega(\mathrm{QS}_n, \mathcal{S}) \geq 1 - \varepsilon$ for sufficiently small $\varepsilon > 0$, then* $\dim(\mathcal{H}) > (1 - \delta(n, \varepsilon))2^{2n}$.

Furthermore there exists a projection $\Pi \in \mathscr{A}$ such that $\tau(\Pi) \approx 2^{-2n}$ and $\Pi \approx S_{0^n}^A S_{0^n}^B$.

Proof. The inequality $\dim(\mathcal{H}) > (1 - \delta(n, \varepsilon))2^n$ is immediate from Theorem 1.23 and Theorem 1.22. We now prove Π exists. Let $M = S_{0^n}^A S_{0^n}^B S_{0^n}^A$ and note that $\{M, 1 - M\}$ is a POVM. Indeed we have $0 \leq S_{0^n}^A (1 - S_{0^n}^B) S_{0^n}^A \leq 1 - M$ in positive semidefinite ordering. Since $S_{0^n}^A$ and $S_{0^n}^B$

approximately commute, we can write

$$
\begin{aligned}
M^2 &= S^A_{0^n} S^B_{0^n} S^A_{0^n} S^A_{0^n} S^B_{0^n} S^A_{0^n} \\
&\approx S^A_{0^n} S^B_{0^n} S^A_{0^n} \\
&= M.
\end{aligned}
$$

Therefore we also have $(1 - M)^2 = 1 - 2M + M^2 \approx 1 - M$. So we can apply Lemma 1.17 to obtain a projection $\Pi \in \mathscr{A}$ such that $\Pi \approx S^A_{0^n} S^B_{0^n} S^A_{0^n}$. Now again since $S^A_{0^n}$ and $S^B_{0^n}$ approximately commute, we get that $\Pi \approx S^A_{0^n} S^B_{0^n}$. An application of Proposition 1.8 gives us $\tau(\Pi) \approx \tau(S^A_{0^n} S^B_{0^n})$. The result $\tau(\Pi) \approx 2^{-2n}$ now follows from item 4 in the preceding theorem.

□

We finish this section by stating a technical lemma. The lemma holds in a more general setting but here we restricted attention only to the Question Sampling game.

Lemma 1.26. *Let $\mathscr{S} = (\tau, \{M^q\}_{q \in Q_n})$ be a synchronous strategy for QS_n over a von Neumann algebra $\mathscr{A} \subset B(\mathcal{H})$ and suppose $\omega(\mathrm{QS}_n, \mathscr{S}) \geq 1 - \varepsilon$. Also let Π be the projection in the preceding corollary and let $\widehat{\mathcal{H}}$ be the subspace Π projects onto. Then the set of operators*

$$
\widehat{\mathscr{A}} = \{\Pi M \Pi : M \in \mathscr{A}\} \subset B(\widehat{\mathcal{H}})
$$

is a von Neumann algebra with unit Π. Furthermore, the functional $\sigma : B(\widehat{\mathcal{H}}) \to \mathbb{C}$ defined by $\sigma(N) = \frac{\tau(N)}{\tau(\Pi)}$, for every $N \in B(\widehat{\mathcal{H}})$, is a tracial state on $\widehat{\mathscr{A}}$.

Proof. For a proof that $\widehat{\mathscr{A}}$ is a von Neumann algebra see the section on “Elementary properties of von Neumann algebras” in the notes by Vaughan Jones [46]. The functional σ is a positive linear functional because τ is a positive linear functional. It is unital because $\sigma(1_{\widehat{\mathcal{H}}}) = \sigma(\Pi) = \tau(\Pi)/\tau(\Pi) = 1$. It is cyclic on $\widehat{\mathscr{A}}$ because τ is cyclic on $\mathscr{A}$ and $\widehat{\mathscr{A}} \subset \mathscr{A}$. □

1.4 Question Reduction

In this section we present the Question Reduction transformation, whose properties are given by the following Theorem.

Theorem 1.27 (Question Reduction)**.** *For all $\alpha \in \mathbb{N}$, there exists a polynomial-time algorithm $\mathcal{A}QuestionReduction_\alpha$ that takes as input a pair of Turing machines (D, C) and outputs a pair of Turing machines $(D^{\text{intro}}, C^{\text{intro}})$ such that the following holds. If $\mathscr{V} = (D, C)$ is a verifier for a sequence of games $\mathscr{G}_{\mathscr{V}} = (G_n)_{n\in\mathbb{N}}$ and $n_0 \in \mathbb{N}$ is an integer such that for all $n \geq n_0$,*

$$\max\left\{\mathsf{TIME}_C(n), \mathsf{TIME}_D(n)\right\} \leq n^\alpha ,$$

then $\mathscr{V}^{\text{intro}} = (D^{\text{intro}}, C^{\text{intro}})$ is a verifier corresponding to a sequence of games $\mathscr{G}_{\mathscr{V}^{\text{intro}}} = (G_n^{\text{intro}})_{n\in\mathbb{N}}$ with the following properties. There exists $\beta = \text{poly}(\alpha) \in \mathbb{N}$ and $n_0^{\text{intro}} = \text{poly}(\beta, n_0) \in \mathbb{N}$ such that for all $n \geq n_0^{\text{intro}}$,

1. *(Complexity bounds)*

   The questions of G_n^{intro} have length at most $\log^\beta n$,

   $\mathsf{TIME}_{C^{\text{intro}}}(n) \leq \log^\beta n$, *and*

   $\mathsf{TIME}_{D^{\text{intro}}}(n) \leq n^\beta$

2. *(Completeness) For all oracularizable synchronous strategies $\mathscr{S}$ for G_n, there exists an oracularizable synchronous strategy $\mathscr{S}^{\text{intro}}$ for G_n^{intro} such that*

   $$\omega(G_n^{\text{intro}}, \mathscr{S}^{\text{intro}}) \geq \omega(G_n, \mathscr{S}).$$

   Furthermore, if $\mathscr{S}$ is finite-dimensional, then so is $\mathscr{S}^{\text{intro}}$.

3. *(Soundness) For all $t \in \{q, co\}$ we have*

$$\omega_t^s(G_n) < 1 \Longrightarrow \omega_t^s(G_n^{\text{intro}}) < 1 \ .$$

4. *(Entanglement bound)*

$$\mathcal{E}(G_n^{\text{intro}}, 1) \geq \max\left\{\mathcal{E}(G_n, 1), 2^{2n}\right\} \ .$$

Intuitively, the Question Reduction transformation transforms a sequence of games $(G_1, G_2, \ldots)$ to a sequence $(G_1^{\text{intro}}, G_2^{\text{intro}}, \ldots)$ of "Introspection games" such that the question lengths of the Introspection game G_n^{intro} is *polylogarithmic* in the time complexity of the "original game" G_n while the value of G_n^{intro} approximates the value of G_n. In particular, the value of G_n^{intro} is 1 if and only if the value of G_n is 1. Furthermore, the time complexity of the Introspection game G_n^{intro} is polynomial in the time complexity of the original game G_n. The reason this is called "Question Reduction" is because the question lengths of the original game G_n can be as large as n^α (because that's the time complexity of the decision procedure D_n) and the question lengths of the Introspection games are at most $\log^\beta n$. The core of the Question Reduction transformation is the *Introspection protocol*, which is a simplification of the one developed by [19, 4]. Aside from the fact that we work in the setting of synchronous games, the two other major simplifications are that

- we only need to introspect games with uniform question distributions, and
- the transformation does not need to be gap preserving.

The bulk of this section will be spent on analyzing the Introspection protocol, and then in Section 1.4.5 we prove Theorem 1.27.

1.4.1 Overview

Let $G = (\mathcal{X}, \mathcal{A}, D)$ be a synchronous game with $\mathcal{X} = \{0,1\}^\ell, \mathcal{A} = \{0,1\}^m$. We present a transformation $G \mapsto G^{\text{intro}}$ where G^{intro} is called the *Introspection game* corresponding to G. The question lengths of G^{intro} will be much smaller than those of G, but the values of the two games will still be tightly related.

At an intuitive level, the question lengths are reduced in G^{intro} by asking the players to "ask themselves" – i.e., to introspect – their own questions from $\mathcal{X}$. The players in G^{intro} are each asked to sample a question $x \in \mathcal{X}$ and answer with $a \in \mathcal{A}$ as they would have answered in the original game G if they have received question x. The players then each respond with a tuple (x, a). If the players' responses are (x, a) and (y, b), the decision procedure in G^{intro} will check that $D(x, y, a, b) = 1$.

In order for the values of G and G^{intro} to be meaningfully related, we need to ensure that the players sample their introspected questions x and y from the uniform distribution (instead of, say, always picking a fixed (x^*, y^*) for which they have prepared winning answers). We ensure this by introducing a small number of special questions in the game G^{intro}. The cross-checks between these special questions force the players to behave "honestly" (i.e., to sample (x, y) from the uniform distribution), or risk losing the game with some nonzero probability.

The Introspection game G^{intro} is an extension of the Question Sampling game QS_ℓ from Section 1.3.3, where ℓ is the bit length of questions in the original game G. Recall that the Question Sampling game certifies that the players have measurements for questions S_A, S_B, E_A, E_B satisfying the rigidity properties detailed in Theorem 1.24.

In addition to these questions, the Introspection game has an additional question I, which stands for "introspect". When a player receives question I, they are expected to answer with a tuple $(x, a, y, b) \in (\mathcal{X} \times \mathcal{A})^2$, and the players win if $D(x, y, a, b) = 1$. The Introspection game certifies the measurement corresponding to I is consistent with the following measurement process: performing both S_A, S_B measurements (which commute with each other) to produce $(x, y) \in \mathcal{X}^2$, and then performing measurements N^x and N^y (which commute with each other when (x, y) is a nontrivial question pair in the original game) to produce $(a, b) \in \mathcal{A}^2$. Furthermore, N^x commutes with the E_B measurement and N^y commutes with the E_A measurement.

The fact that the I measurement is consistent with S_A, S_B ensures that the distribution of the pair (x, y) is uniform over $\mathcal{X}^2$. The fact that the the measurements N^x, N^y commute with the E_B and E_A measurements, respectively, ensures that the output a of N^x does not depend on y and similarly the output b of N^y does not depend on x. Thus the measurements $\{N^x\}$ give rise to a strategy for the original game G, and thus the value of G^{intro} is related to that of G.

There are several other questions that are used in the Introspection game G^{intro} to ensure these consistency properties. Overall, the number of questions in G^{intro} is $|\mathrm{QS}_\ell|+7$, and thus the question lengths represented in binary is $\lceil \log(|\mathrm{QS}_\ell| + 7) \rceil = O(\log(\ell))$.

We formally define the Introspection game next.

1.4.2 Definition of Introspection game

Throughout this section, we write W to denote a value from the set $\{A, B\}$, and we write

$$\overline{W} = \begin{cases} B & \text{if } W = A, \\ A & \text{if } W = B. \end{cases} .$$

The Introspection game G^{intro} corresponding to G is a synchronous game $(\mathcal{Q}^{\text{intro}}, \mathcal{A}^{\text{intro}}, D^{\text{intro}})$ with

$$\mathcal{Q}^{\text{intro}} = \mathcal{Q}_{\mathrm{QS}_\ell} \cup \{\ I\ \} \cup \{\ I_W,\ \ I_W S_{\overline{W}}\ \ ,\ \ I_W E_{\overline{W}}\ \}_{W \in \{A,B\}},$$
$$\mathcal{A}^{\text{intro}} = \mathcal{A}_{\mathrm{QS}_\ell} \cup \mathcal{X} \cup (\mathcal{X} \times \mathcal{A}) \cup (\mathcal{X} \times \mathcal{A} \times \mathcal{X}) \cup (\mathcal{X} \times \mathcal{A} \times \mathcal{X} \times \mathcal{A})\ .$$

The symbol I stands for *introspect*, and S and E stand for *sample* and *erase* as in the Question Sampling game. We emphasize that the symbols $I_W S_{\overline{W}}$ and $I_W E_{\overline{W}}$ respectively are each individual questions; for example $I_A S_B$ is distinct from the questions I_A and S_B, and is also distinct from the question $I_B S_A$.

The decision procedure D^{intro} is specified by Table 1.4. On question pair (q, r) and answer pair $(\widehat{a}, \widehat{b})$, the decision procedure checks if (q, r) is nontrivial according to the table, and if so, checks the corresponding winning condition. For the sake of clarity, we omit the symmetric case where the question pair is (r, q) and the answer pair is $(\widehat{b}, \widehat{a})$.

Nontrivial Question Pair (q, r)	**Winning Condition on Answers** $(\widehat{a}, \widehat{b})$
$q = r$	$\widehat{a} = \widehat{b}$
(q, r) is nontrivial for QS_ℓ	$D_{\mathrm{QS}_\ell}(q, r, \widehat{a}, \widehat{b}) = 1$
$q = I$ $r = I_W$	$\Big((x_A, x_B)$ is trivial for $G\Big)$ or $\Big(z = x_W \wedge c = a_W \wedge D(x_A, x_B, a_A, a_B) = 1\Big)$ where $\widehat{a} = (x_A, a_A, x_B, a_B) \in (\mathcal{X} \times \mathcal{A})^2$ and $\widehat{b} = (z, c) \in \mathcal{X} \times \mathcal{A}$
$q = I_W$ $r = I_W S_{\overline{W}}$	$z = x_W \wedge c = a_W$ where $\widehat{a} = (x_W, a_W) \in \mathcal{X} \times \mathcal{A}$ and $\widehat{b} = (z, c, x_{\overline{W}}) \in \mathcal{X} \times \mathcal{A} \times \mathcal{X}$
$q = I_W$ $r = S_W$	$z = x_W$ where $\widehat{a} = (x_W, a_W) \in \mathcal{X} \times \mathcal{A}$ and $\widehat{b} = z \in \mathcal{X}$
$q = I_W$ $r = I_W E_{\overline{W}}$	$z = x_W \wedge c = a_W$ where $\widehat{a} = (x_W, a_W) \in \mathcal{X} \times \mathcal{A}$ and $\widehat{b} = (z, c, x_{\overline{W}}) \in \mathcal{X} \times \mathcal{A} \times \mathcal{X}$
$q = I_W E_{\overline{W}}$ $r = E_{\overline{W}}$	$z = x_{\overline{W}}$ where $\widehat{a} = (x_W, a_W, x_{\overline{W}}) \in \mathcal{X} \times \mathcal{A} \times \mathcal{X}$ and $\widehat{b} = z \in \mathcal{X}$
$q = I_W S_{\overline{W}}$ $r = S_{\overline{W}}$	$z = x_{\overline{W}}$ where $\widehat{a} = (x_W, a_W, x_{\overline{W}}) \in \mathcal{X} \times \mathcal{A} \times \mathcal{X}$ and $\widehat{b} = z \in \mathcal{X}$

Table 1.4: The nontrivial question pairs and winning conditions for the Introspection game G^{intro}.

The nontrivial question pairs of the Introspection game G^{intro}, apart from those in the Question Sampling game QS_ℓ, are also depicted as a graph in Figure 1.3. The questions are connected via an edge if they form a nontrivial question pair (and self-loops are not drawn for clarity).

The rationale behind the questions $I_W S_{\overline{W}}$ and $I_W E_{\overline{W}}$ is the following. A player receiving the composite question $I_W S_{\overline{W}}$, for example, is expected to answer both questions I_W and $S_{\overline{W}}$. By cross-checking this player's answers against the other player (who may have received either I_W or $S_{\overline{W}}$ alone), the game ensures that the measurements corresponding to I_W and $S_{\overline{W}}$ *commute*, and this in

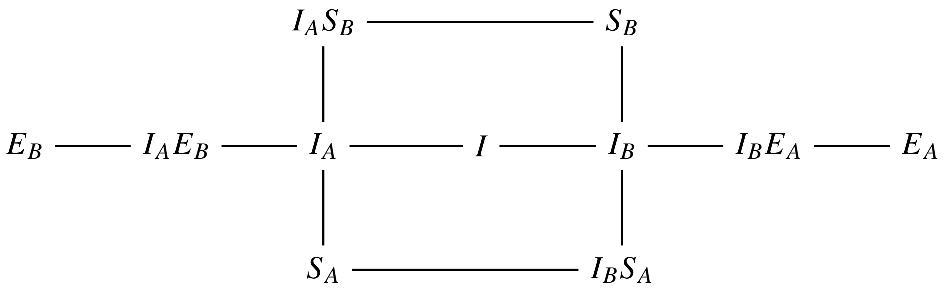

Figure 1.3: A node indicates a special question in G^{intro}. A pair of questions are connected with an edge if the pair is a nontrivial question pair as defined in Section 1.2.4. There should also be loops on every node (which we omitted here for clarity).

turn enables the "honest" strategy in the completeness case to be oracularizable. This and more will become clear in the next subsection.

1.4.3 Completeness of Introspection

As mentioned earlier, we need to show that the value of the original game and the introspected game are tightly related. This has two directions. First we need to show that if G has a perfect strategy so does G^{intro}; this is called the *completeness* property. In fact we prove the following stronger statement.

Proposition 1.28 (Completeness of Introspection)**.** *For all oracularizable synchronous strategies $\mathscr{S}$ for G, there exists an oracularizable synchronous strategy $\mathscr{S}^{\text{intro}}$ for G^{intro} such that*

$$\omega(G^{\text{intro}}, \mathscr{S}^{\text{intro}}) \geq \omega(G, \mathscr{S}) \ .$$

Furthermore, if $\mathscr{S}$ is finite-dimensional then so is $\mathscr{S}^{\text{intro}}$.

Recall that a synchronous strategy $\mathscr{S}$ for a synchronous game G is oracularizable if for every nontrivial question pair (q, r), the corresponding measurement operators commute (see Theorem 1.19).

Proof. Let $\mathscr{S} = (\sigma, \{N^x\}_{x \in \mathcal{X}})$ be an oracularizable synchronous strategy for G and let $\mathscr{S}_{\mathrm{QS}_\ell} = (\tau, \{M^q\}_{q \in Q_{\mathrm{QS}_\ell}})$ be the "honest" perfect oracularizable strategy for the Question Sampling game

QS_ℓ as defined in Section 1.3.3. Let $\mathcal{H}_{\mathrm{QS}_\ell}$, $\mathcal{H}_{\mathscr{S}}$ and $\mathscr{A}_{\mathrm{QS}_\ell} \subseteq \mathrm{B}(\mathcal{H}_{\mathrm{QS}_\ell}), \mathscr{A}_{\mathscr{S}} \subseteq \mathrm{B}(\mathcal{H}_{\mathscr{S}})$ denote the Hilbert spaces and algebras of the two strategies, respectively. We define a synchronous strategy $\mathscr{S}^{\mathrm{intro}} = (\rho, \{P^q\}_{q \in Q^{\mathrm{intro}}})$, which we call the *honest Introspection strategy*, for G^{intro} over the algebra $\mathscr{A}_{\mathrm{QS}_\ell} \otimes \mathscr{A}_{\mathscr{S}}$ with the tracial state $\rho = \tau \otimes \sigma$. In this proof we use the shorthand notation S_x^W, E_x^W to denote the operators $M_x^{S_W}$, $M_x^{E_W}$ from the strategy $\mathscr{S}_{\mathrm{QS}_\ell}$, respectively.

The measurement operators are defined as follows. For all $q \in Q_{\mathrm{QS}_\ell}$ and $x \in \mathcal{A}_{\mathrm{QS}_\ell}$, let $P_x^q = M_x^q \otimes 1$ where the 1 denotes the identity on the Hilbert space $\mathcal{H}_{\mathscr{S}}$. Since M_x^q is a projection on $\mathcal{H}_{\mathrm{QS}_\ell}$, the operators $\{P_x^q\}$ are also projections and furthermore form a measurement.

For all other questions $q \in Q^{\mathrm{intro}} \setminus Q_{\mathrm{QS}_\ell}$, we define

$$P_{x,a}^{I_W} := S_x^W \otimes N_a^x\,, \qquad P_{x,a,y}^{I_W S_{\overline{W}}} := S_x^W S_y^{\overline{W}} \otimes N_a^x\,, \qquad P_{x,a,y}^{I_W E_{\overline{W}}} := S_x^W E_y^{\overline{W}} \otimes N_a^x$$

for all $W \in \{A, B\}$, $x, y \in \mathcal{X}$, and $a \in \mathcal{A}$. The operator $P_{x,a}^{I_W}$ is clearly a projection (because S_x^W, N_a^x are projections), and forms a projective measurement. In the honest Question Sampling strategy the operators S_x^W and $S_y^{\overline{W}}$ commute (by Theorem 1.24), therefore $P_{x,a,y}^{I_W S_{\overline{W}}}$ forms a projective measurement. Similarly S_x^W and $E_y^{\overline{W}}$ commute, therefore $P_{x,a,y}^{I_W S_{\overline{W}}}$ forms a projective measurement.

It should be clear now why we choose the notation $I_W S_{\overline{W}}$ and $I_W E_{\overline{W}}$: in the honest Introspection strategy, we have that

$$P_{x,a,y}^{I_W S_{\overline{W}}} = P_{x,a}^{I_W}\ S_y^{\overline{W}} = S_y^{\overline{W}}\ P_{x,a}^{I_W} \qquad \text{and} \qquad P_{x,a,y}^{I_W E_{\overline{W}}} = P_{x,a}^{I_W}\ E_y^{\overline{W}} = E_y^{\overline{W}}\ P_{x,a}^{I_W}\,. \tag{1.4.1}$$

It remains to define the projective measurement $\{P_{x,a,y,b}^I\}$ for the Introspection question I. If $(x, y) \in \mathcal{X} \times \mathcal{X}$ is a nontrivial question in G, we define

$$P_{x,a,y,b}^I := S_x^A\ S_y^B \otimes N_a^x\ N_b^y.$$

Since N_a^x and N_b^y commute when (x, y) is nontrivial for G (because $\mathscr{S}$ is oracularizable), we see that $P^{I}_{x,a,y,b}$ is a projection. If on the other hand (x, y) is a trivial question in G, we define

$$P^{I}_{x,a,y,b} := \begin{cases} S^A_x \ S^B_y \otimes 1 & \text{if } (a,b) = (0^m, 0^m), \\ 0 & \text{otherwise.} \end{cases}$$

This is clearly a projective measurement as well. Intuitively, when a player receives the question I, they first perform the sampling measurements S^A and S^B (which can be performed simultaneously since they commute) to obtain a pair of questions $(x, y) \in \mathcal{X} \times \mathcal{X}$ for the original game G. If (x, y) is trivial for G, then the player outputs $(x, 0^m, y, 0^m)$. Otherwise, the player then simultaneously measures N^x and N^y (which commute since (x, y) is nontrivial for G) to obtain answers $(a, b) \in \mathcal{A} \times \mathcal{A}$. The player then returns (x, a, y, b) as its answer.

Clearly $\mathcal{S}^{\text{intro}}$ is finite-dimensional when $\mathcal{S}$ is finite-dimensional. Next we show that $\mathcal{S}^{\text{intro}}$ is oracularizable and has success probability 1 in the Introspection game G^{intro}.

First, if (q, r) is a trivial pair of questions for G^{intro} then by definition the players win with probability 1 on those questions. Assume that (q, r) is a nontrivial question pair.

Suppose that $(q, r) \in \mathcal{Q}_{\text{QS}_\ell}$. Since $\mathcal{S}_{\text{QS}_\ell}$ is oracularizable and (q, r) must also be nontrivial for QS_ℓ, the measurement operators $\{P^q_x\}$ and $\{P^r_x\}$ commute. Furthermore, by design the strategy $\mathcal{S}_{\text{QS}_\ell}$ succeeds with probability 1 in the game QS_ℓ and thus succeeds with probability 1 in G^{intro} conditioned on questions from $\mathcal{Q}_{\text{QS}_\ell}$.

It remains to check the commutativity property and success probability for all question pairs that are connected via an edge in Figure 1.3. For self-loops (i.e, question pairs (q, q)), commutativity and success probability 1 are trivially satisfied because the operators $P^q_{\hat{a}}$ are projections. We now check the other nontrivial question pairs.

$\underline{(I_W, S_W)}$: Commutativity follows because

$$P^{I_W}_{x,a} \ P^{S_W}_z = S^W_x \, S^W_z \otimes N^x_a = S^W_z \, S^W_x \otimes N^x_a = P^{S_W}_z \ P^{I_W}_{x,a} \ .$$

Here we used the fact that S^W_x, S^W_z are elements of the same projective measurement and thus commute. The probability of winning conditioned on this question pair is

$$\sum_{x,a} \rho(P^{I_W}_{x,a}\ P^{S_W}_{x}) = \sum_{x,a} \tau(S^W_x\ S^W_x)\ \sigma(N^x_a) = \sum_{x} \tau(S^W_x) = 1\ .$$

$\underline{(I_W, I_W S_{\overline{W}})}$: Commutativity follows because

$$P^{I_W}_{x,a}\ P^{I_W S_{\overline{W}}}_{z,c,y} = S^W_x\ S^W_z\ S^{\overline{W}}_y \otimes N^x_a\ N^z_c = S^W_z\ S^{\overline{W}}_y\ S^W_x \otimes N^z_c\ N^x_a = P^{I_W S_{\overline{W}}}_{z,c,y}\ P^{I_W}_{x,a}.$$

The second equality holds because if $x \neq z$, then $S^W_x\ S^W_z = 0$ and the equality holds trivially. If on the other hand $x = z$, the equality holds because $S^W_x, S^{\overline{W}}_y$ commute with each other and N^x_a, N^x_c commute with each other.

The probability of winning conditioned on this question pair is

$$\sum_{x,a,y} \rho(P^{I_W}_{x,a}\ P^{I_W S_{\overline{W}}}_{x,a,y}) = \sum_{x,a,y} \rho(P^{I_W}_{x,a}\ P^{I_W}_{x,a}\ S^{\overline{W}}_y) = \sum_{x,a} \rho(P^{I_W}_{x,a}) = 1$$

where in the first equality we used (1.4.1).

$\underline{(I_W, I_W E_{\overline{W}})}$: The argument for this is nearly identical to that for the previous question pair, except we replace the sampling measurement $S^{\overline{W}}$ with the erasure measurement $E^{\overline{W}}$.

$\underline{(I_W S_{\overline{W}}, S_{\overline{W}})}$: Commutativity follows because

$$P^{I_W S_{\overline{W}}}_{x,a,y}\ S^{\overline{W}}_z = P^{I_W}_{x,a}\ S^{\overline{W}}_y\ S^{\overline{W}}_z = S^{\overline{W}}_z\ P^{I_W}_{x,a}\ S^{\overline{W}}_y = S^{\overline{W}}_z\ P^{I_W S_{\overline{W}}}_{x,a,y}$$

where in the first equality we used (1.4.1), and then we used the fact that $S^{\overline{W}}_z$ commute with $P^{I_W}_{x,a}$.

The probability of winning conditioned on this question pair is

$$\sum_{x,a,y} \rho(P^{I_W S_{\overline{W}}}_{x,a,y}\ S^{\overline{W}}_y) = \sum_{x,a,y} \rho(P^{I_W}_{x,a}\ S^{\overline{W}}_y\ S^{\overline{W}}_y) = \sum_{x,a} \rho(P^{I_W}_{x,a}) = 1$$

where in the first equality we used (1.4.1) and in the second equality we used the fact that $S^{\overline{W}}_y$ is a projection and forms a measurement.

$\underline{(I_W E_{\overline{W}}, E_{\overline{W}})}$: The argument for this is identical to that for the previous question pair, except we replace the sampling measurement $S^{\overline{W}}$ with $E^{\overline{W}}$.

$\underline{(I, I_W)}$: Assume without loss of generality that $W = A$. Commutativity is due to the following. Suppose (x, y) is a trivial question pair for G. Then

$$P^{I}_{x,0,y,0}\ P^{I_A}_{z,c} = S^A_x\ S^B_y\ S^A_z \otimes N^z_c = S^A_z\ S^A_x\ S^B_y \otimes N^z_c = P^{I_A}_{z,c}\ P^{I}_{x,0,y,0}$$

where 0 is shorthand for 0^m, and for all $(a, b) \neq (0^m, 0^m)$ we have

$$P^{I}_{x,a,y,b}\ P^{I_A}_{z,c} = 0 = P^{I_A}_{z,c}\ P^{I}_{x,a,y,b}\ .$$

If (x, y) is a nontrivial question pair for G then

$$P^{I}_{x,a,y,b}\ P^{I_A}_{z,c} = S^A_x\ S^B_y\ S^A_z \otimes N^x_a\ N^y_b\ N^z_c = S^A_z\ S^A_x\ S^B_y \otimes N^z_c\ N^x_a\ N^y_b = P^{I_A}_{z,c}\ P^{I}_{x,a,y,b}$$

where the second equality holds because if $x \neq z$, then $S^A_x\ S^B_y\ S^A_z = 0$ and the equality holds trivially. If on the other hand $x = z$, the equality holds because N^x_a, N^y_b, N^x_c all commute (because (x, y) is a nontrivial question pair and N^x_a, N^x_c are elements of the same projective measurement).

We calculate the probability of success as follows. If (x, y) is a nontrivial question pair in the original game G we have

$$\rho(P^{I}_{x,a,y,b}\ P^{I_A}_{z,c}) = \tau(S^A_x\ S^B_y\ S^A_z)\ \sigma(N^x_a\ N^y_b\ N^z_c) = 2^{-2\ell}\ \sigma(N^x_a\ N^y_b)\ \mathbf{1}_{z=x,c=a}$$

where we used the fact that in the honest strategy $\mathscr{S}_{\mathrm{QS}_\ell}$ we have $\tau(S^A_x\ S^B_y) = 2^{-2\ell}$. Notation $\mathbf{1}_{z=x,c=a}$ denotes the indicator variable for the equalities $z = x, c = a$. If (x, y) is trivial we have

$$\rho(P^{I}_{x,a,y,b}\ P^{I_A}_{z,c}) = 2^{-2\ell}\ \sigma(N^z_c)\ \mathbf{1}_{z=x,a=b=0^m}\ .$$

So the probability of winning using $\mathscr{S}^{\text{intro}}$ conditioned on players receiving question pair (I, I_A) is

$$\begin{aligned}
\sum_{x,a,y,b,z,c} & \rho(P^I_{x,a,y,b}\ P^{I_A}_{z,c})\ D^{\text{intro}}(I, I_A, (x,a,y,b), (z,c)) \\
&= \frac{1}{2^{2\ell}} \sum_{\substack{(x,y) \\ \text{nontrivial for } G}} \sum_{a,b} \sigma(N^x_a\ N^y_b)\ D(x,y,a,b) + \frac{1}{2^{2\ell}} \sum_{\substack{(x,y) \\ \text{trivial for } G}} \sum_{c} \sigma(N^x_c) \\
&= \frac{1}{2^{2\ell}} \sum_{\substack{(x,y) \\ \text{nontrivial for } G}} \sum_{a,b} \sigma(N^x_a\ N^y_b)\ D(x,y,a,b) + \frac{1}{2^{2\ell}} \sum_{\substack{(x,y) \\ \text{trivial for } G}} 1 \\
&= \frac{1}{2^{2\ell}} \sum_{\substack{(x,y) \\ \text{nontrivial for } G}} \sum_{a,b} \sigma(N^x_a\ N^y_b)\ D(x,y,a,b) + \frac{1}{2^{2\ell}} \sum_{\substack{(x,y) \\ \text{trivial for } G}} \sum_{a,b} \sigma(N^x_a\ N^y_b)\ D(x,y,a,b) \\
&= \omega(G, \mathscr{S})
\end{aligned}$$

where in the third line we used that $\{N^x_c\}$ is a measurement, and in the fourth line we used that $D(x,y,a,b) = 1$ for all trivial (x,y).

So conditioned on any pair of questions the players win with probability 1 using strategy $\mathscr{S}^{\text{intro}}$, except when they receive question pair (I, I_A) or (I, I_B) in which case they win with probability $\omega(G, \mathscr{S})$. From this we conclude that $\omega(G^{\text{intro}}, \mathscr{S}^{\text{intro}}) \geq \omega(G, \mathscr{S})$. □

1.4.4 Soundness of Introspection

The second part of showing that the value of the original game and the introspected game are tightly related is called *soundness*. Informally speaking the soundness property states that if the original game has no perfect strategy, then neither does the introspected game.

In the soundness proposition below, we also prove a lower bound on the dimension of the Hilbert space for any perfect strategy of G^{intro}. We show this dimension is at least as big as the maximum of $2^{2\ell}$ and the smallest dimension of a Hilbert space among all perfect strategies of G. Recall that ℓ is the bit length of questions in G. This dimension lower bound will be used later in the section on compression.

Proposition 1.29 (Soundness of Introspection)**.** *For all $t \in \{q, co\}$*

$$\omega_t^s(G^{\text{intro}}) = 1 \implies \omega_t^s(G) = 1.$$

Furthermore it holds that

$$\mathcal{E}(G^{\text{intro}}, 1) \geq \max\left\{\mathcal{E}(G, 1), 2^{2\ell}\right\}.$$

At a high level, the proof of Theorem 1.29 proceeds by taking a synchronous strategy $\mathscr{S}^{\text{intro}} = (\rho, \{P^q\}_{q\in Q^{\text{intro}}})$ for G^{intro} that succeeds with probability $1 - \varepsilon$, with ε sufficiently small, and "extracting" from it a strategy $\mathscr{S} = (\sigma, \{N^x\}_{x\in\mathcal{X}})$ for the original game G that has value $1-\delta(\varepsilon)$ where δ is a proper error function (see Section 1.2.5 for definition of proper error function). The error function δ also has a dependence on ℓ, but since we do not need to carry that around, we hide it in our notation $\delta(\varepsilon)$.

Note that $\omega_q^s(G^{\text{intro}}) = 1$ does not imply the existence of a finite-dimensional synchronous strategy with value 1. All we can guarantee is that for every $\varepsilon > 0$ there exists a finite-dimensional synchronous strategy with value at least $1 - \varepsilon$. On the other hand $\omega_{co}^s(G^{\text{intro}}) = 1$ means that there exists a perfect synchronous strategy for G^{intro}.

To make the notation easier to read, we use the following abbreviations for the measurements P^q corresponding to the questions $q \in \{\ I,\ I_W,\ I_W S_{\overline{W}},\ I_W E_{\overline{W}},\ S_W,\ E_W\ \}_{W\in\{A,B\}} \subseteq Q^{\text{intro}}$. For all $W \in \{A, B\}$, $x, y \in \mathcal{X}$ and $a, b \in \mathcal{A}$,

$$I_{x,a,y,b} = P^I_{x,a,y,b}\,, \qquad I^W_{x,a} = P^{I_W}_{x,a}\,, \qquad (I^W S^{\overline{W}})_{x,a,y} = P^{I_W S_{\overline{W}}}_{x,a,y}$$
$$(I^W E^{\overline{W}})_{x,a,y} = P^{I_W E_{\overline{W}}}_{x,a,y}\,, \qquad S^W_x = P^{S_W}_x\,, \qquad E^W_x = P^{E_W}_x\,.$$

Furthermore, we define the *erasure observables*

$$O^W_x = \sum_{y\in\mathcal{X}} (-1)^{x\cdot y}\, E^W_y$$

for $W \in \{A, B\}$. Unlike the section on Question Sampling, we do not need to define sampling observables for the purpose of proving the current proposition. We use $\cdot$ in the subscript to indicate the data-processed measurement that ignores part of the measurement outcome, so for example

$$
\begin{aligned}
I_{\cdot,a,y,b} &= \sum_{x \in \mathcal{X}} I_{x,a,y,b}, \\
I_{x,\cdot,y,b} &= \sum_{a \in \mathcal{A}} I_{x,a,y,b}, \\
I_{x,a,\cdot,\cdot} &= \sum_{y \in \mathcal{X}, b \in \mathcal{A}} I_{x,a,y,b},
\end{aligned}
$$

etc. We may sometime drop $\cdot$ when there is no risk of ambiguity, for example we may write I_x^W instead of $I_{x,\cdot}^W$.

We first prove two key lemmas establishing that in any strategy with large value certain commutation relations are approximately satisfied and that introspected questions are almost uniformly sampled. Throughout this section, we let $\mathcal{S}^{\text{intro}} = (\rho, \{P^q\}_{q \in Q^{\text{intro}}})$ be a fixed synchronous strategy for G^{intro} with value $1 - \varepsilon$.

Lemma 1.30. *The following approximate relations hold*

$$
\begin{aligned}
I_x^W &\approx S_x^W \\
I_{x,a}^W \, S_y^W &\approx S_y^W \, I_{x,a}^W \\
I_{x,a}^W \, S_y^{\overline{W}} &\approx S_y^{\overline{W}} \, I_{x,a}^W \\
I_{x,a}^W \, E_y^{\overline{W}} &\approx E_y^{\overline{W}} \, I_{x,a}^W \\
I_{x,a}^W \, O_u^{\overline{W}} &\approx O_u^{\overline{W}} \, I_{x,a}^W .
\end{aligned}
$$

Proof. As mentioned in Section 1.2.5, when we write $I_x^W \approx S_x^W$ we mean $I_x^W \approx_{\delta(\varepsilon)} S_x^W$ for some function δ such that $\delta(\varepsilon) \to 0$ as $\varepsilon \to 0$.

Since the strategy is winning with probability $1 - \varepsilon$, the winning probability conditioned on receiving question (I_W, S_W) is at least $1 - |Q^{\text{intro}}|^2 \varepsilon$. The expression for the probability of winning conditioned on players receiving question pair (I_W, S_W) is

$$\begin{aligned}\sum_{x,a,y} \rho(I^W_{x,a}\, S^W_y) D^{\text{intro}}(I_W, S_W, (x,a), y) &= \sum_{x,a} \rho(I^W_{x,a}\, S^W_x) \\ &= \sum_x \rho(I^W_x\, S^W_x).\end{aligned}$$

Therefore we have

$$\sum_x \rho(I^W_x\, S^W_x) \approx 1,$$

or equivalently that $I^W_x \simeq S^W_x$. By Lemma 1.13, we get that $I^W_x \approx S^W_x$. By Proposition 1.8, we obtain that $I^W_{x,a}\, S^W_y \approx I^W_{x,a}\, I^W_y$ from which we arrive at our first approximate commutation relation

$$I^W_{x,a}\, S^W_y \approx I^W_{x,a}\, I^W_y = I^W_y\, I^W_{x,a} \approx S^W_y\, I^W_{x,a}$$

where the equality in the middle follows because operators belonging to the same projective measurement commute. This is the basic idea behind the proof of the remaining approximate relations.

Next we prove the approximate commutation relation $I^W_{x,a}\, E^{\overline{W}}_y \approx E^{\overline{W}}_y\, I^W_{x,a}$ (the relation $I^W_{x,a}\, S^{\overline{W}}_y \approx S^{\overline{W}}_y\, I^W_{x,a}$ is proved nearly identically). Similar to our argument above for (I_W, S_W), the players winning probability conditioned on receiving question pair $(E_{\overline{W}}, I_W E_{\overline{W}})$ is $1 - \delta(\varepsilon)$, that is

$$\sum_y \tau(E^{\overline{W}}_y (I^W E^{\overline{W}})_y) \approx 1$$

from which, similar to the argument above, we arrive at $E^{\overline{W}}_y \approx (I^W E^{\overline{W}})_y$. With a similar argument, this time starting from the winning probability conditioned on question pair $(I_W, I_W E_{\overline{W}})$, we get that $I^W_{x,a} \approx (I^W E^{\overline{W}})_{x,a}$. Putting these together we obtain

$$\begin{aligned} I^W_{x,a} E^{\overline{W}}_y &\approx (I^W E^{\overline{W}})_{x,a} (I^W E^{\overline{W}})_y \\ &= (I^W E^{\overline{W}})_y (I^W E^{\overline{W}})_{x,a} \\ &\approx E^{\overline{W}}_y I^W_{x,a}. \end{aligned}$$

Finally the last approximate commutation relation follows

$$\begin{aligned} I^W_{x,a} O^{\overline{W}}_u &= \sum_{y \in \mathcal{X}} (-1)^{y.u} I^W_{x,a} E^{\overline{W}}_y \\ &\approx \sum_{y \in \mathcal{X}} (-1)^{y.u} E^{\overline{W}}_y I^W_{x,a} \\ &= O^{\overline{W}}_u I^W_{x,a}. \end{aligned}$$

Switching the order of multiplication in $I^W_{x,a} E^{\overline{W}}_y$ incurs an error of $\delta(\varepsilon)$ for each x, a, y. So over all the norm of $\sum_{y \in \mathcal{X}} (-1)^{y.u} I^W_{x,a} E^{\overline{W}}_y - \sum_{y \in \mathcal{X}} (-1)^{y.u} E^{\overline{W}}_y I^W_{x,a}$ is bounded above by $|\mathcal{X} \times \mathcal{A} \times \mathcal{X}| \delta(\varepsilon)$ which is another error function $\delta(\varepsilon)$. □

Next lemma establishes that the introspected questions are sampled almost uniformly from the question set of the original game. We then use this to justify that $I_{x,a,y,b}$ is approximately $I^A_{x,a} I^B_{y,b}$ when x, y is a nontrivial question pair in the original game.

Lemma 1.31. *Let $I_{x,y} = I_{x,\cdot,y,\cdot}$. Then the following hold*

$$\begin{aligned} I_{x,y} &\approx S^A_x S^B_y, \\ \rho(I_{x,y}) &\approx \frac{1}{2^{2\ell}}. \end{aligned}$$

Furthermore, if x, y is a nontrivial question pair in the original game, then for every $a, b \in \mathcal{A}$

$$I_{x,a,y,b} \approx I^A_{x,a} I^B_{y,b}.$$

Proof. The players winning probability conditioned on receiving question pair (I, I_A) is $1 - \delta(\varepsilon)$. So $\sum_x \rho(I_{x,\cdot,\cdot,\cdot}\, I^A_x) = 1 - \delta(\varepsilon)$ where $I^A_x = \sum_a I^A_{x,a}$. Therefore $I_{x,\cdot,\cdot,\cdot} \approx I^A_x$ and consequently $I_{x,\cdot,\cdot,\cdot} \approx S^A_x$ by Theorem 1.13. Similarly $I_{\cdot,y,\cdot,\cdot} \approx I^B_y \approx S^B_y$. Thus we have $I_{x,y} = I_{x,\cdot,\cdot,\cdot}\, I_{\cdot,y,\cdot,\cdot} \approx S^A_x\, S^B_y$. By Theorem 1.24 and Theorem 1.8, we conclude that $\rho(I_{x,y}) \approx \frac{1}{2^{2\ell}}$.

So far we established that any question pair (x, y) in the answer to the Introspection question I occurs almost uniformly, that is with probability approximately $1/2^{2\ell}$. Fix a nontrivial question pair x, y in the original game. The probability of the event that players receive question pair (I, I^A) and respond with (x, a, y, b) and (z, c), respectively, for some $a, b, c \in \mathcal{A}$ and $z \in \mathcal{X}$ is at least $(1-\delta(\varepsilon))2^{-2\ell}/|\boldsymbol{Q}^{\text{intro}}|^2$. Since the overall strategy looses with probability at most ε, the probability of loosing conditioned on this event is bonded above by

$$2^{2\ell}|\boldsymbol{Q}^{\text{intro}}|^2\varepsilon/(1 - \delta(\varepsilon)) \leq 2^{2\ell}|\boldsymbol{Q}^{\text{intro}}|^2(1 + \delta(\varepsilon))\varepsilon = \delta(\varepsilon)$$

or in other words the probability of winning conditioned on this event is $1-\delta(\varepsilon)$. It is now a simple exercise in probability theory to see that conditioned on receiving question (I, I_A), the probability that player receiving I answers with introspected questions (x, y) and the players win is $\approx 2^{-2\ell}$.

By the construction of the Introspection game, if the players win, then it must be that $(z, c) = (x, a)$. Therefore we have

$$\sum_a \rho(I_{x,a,y,\cdot}\, I^A_{x,a}) = \sum_{a,b} \rho(I_{x,a,y,b}\, I^A_{x,a}) \approx 2^{-2\ell}.$$

Using the relation $I_y \approx S^B_y$ that we proved earlier together with the approximate commutations in Theorem 1.30, we obtain

$$\sum_a \rho(I_{x,a,y,\cdot}(S^B_y\ I^A_{x,a}\ S^B_y)) \approx \sum_a \rho(I_{x,a,y,\cdot}(I_y\ I^A_{x,a}\ I_y)) = \sum_a \rho(I_{x,a,y,\cdot}\ I^A_{x,a}) \approx 2^{-2\ell}. \tag{1.4.2}$$

Define positive semidefinite operators $R_a = I_{x,a,y,\cdot}$ and $S_a = S^B_y I^A_{x,a} S^B_y$, and write

$$\begin{aligned}
\sum_a \|R_a - S_a\|^2_\rho &= \sum_a \rho(R_a^2 + S_a^2 - 2R_a\, S_a) \\
&\leq \sum_a \rho(R_a + S_a - 2R_a S_a) \\
&= \sum_a \rho(R_a) + \rho(S_a) - 2\rho(R_a\, S_a) \\
&\leq 2(1+\delta(\varepsilon))2^{-2\ell} - 2(1-\delta(\varepsilon))2^{-2\ell} \\
&= \delta(\varepsilon).
\end{aligned}$$

The first inequality follows from the fact that R_a, S_a are positive semidefinite with operator norm ≤ 1. The last inequality follows from $\rho(\sum_a R_a S_a) \approx 2^{-2\ell}$ which we proved in (1.4.2) and the following two calculations

$$\begin{aligned}
&\rho(\sum_a R_a) = \rho(I_{x,y}) \approx 2^{-2\ell}, \\
&\rho(\sum_a S_a) = \rho(S^B_y I^A_x\ S^B_y) = \rho(I^A_x\ S^B_y) \approx \rho(S^A_x\ S^B_y) \approx 2^{-2\ell}.
\end{aligned}$$

We conclude that $I_{x,a,y,\cdot} \approx S^B_y\ I^A_{x,a}\ \ S^B_y \approx I^A_{x,a}\ S^B_y$. By a similar argument we get that

$$I_{x,\cdot,y,b} \approx I^B_{y,b}\ S^A_x.$$

Putting these two together

$$I_{x,a,y,b} = I_{x,a,y,\cdot}\ I_{x,\cdot,y,b} \approx I^A_{x,a}\ S^B_y\ I^B_{y,b}\ S^A_x \approx I^A_{x,a}\ S^A_x\ I^B_{y,b}\ S^B_y = I^A_{x,a}\ I^A_x\ I^B_{y,b}\ I^B_y = I^A_{x,a}\ I^B_{y,b}.$$

□

We first sketch a proof of Theorem 1.29. The key step is to establish that, in any strategy that wins with high probability in G^{intro}, when players A and B receive questions I_A and I_B, respectively, their answers (x_A, a_A) and (x_B, a_B) are such that (x_A, x_B) is uniformly distributed in $\mathcal{X} \times \mathcal{X}$ and a_A has no dependence on x_B and similarly a_B has no dependence on x_A. In other words players introspectively asked themselves a uniformly random question (x_A, x_B) and produced answers (a_A, a_B) as they would have answered if they received question (x_A, x_B) in the original game.

In Theorem 1.30, we proved that $I^W_x \approx S^W_x$. This relation implies that on question I_W the player effectively obtains x_W part of the answer by measuring $\{S^W_x\}$. So, by the rigidity properties of the Question Sampling game, we get that (x_a, x_b) is sampled (almost) uniformly at random from $\mathcal{X}\times\mathcal{X}$. We also showed in Theorem 1.31 that (x_a, x_b) in answer to question I are also distributed (almost) uniformly. From the rigidity properties of the Question Sampling game, measurements S^W and E^W (approximately) anticommute while they both (approximately) commute with measurements $S^{\overline{W}}$ and $E^{\overline{W}}$. Additionally we saw in Theorem 1.30 that I^W commutes with both $S^{\overline{W}}$ and $E^{\overline{W}}$. These relationships intuitively imply that the Hilbert space $\mathcal{H}$ can be (approximately) divided into a tensor product $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_G$ of three Hilbert spaces such that the players measurements for special questions S_W and E_W are forced to act as identity on $\mathcal{H}_{\overline{W}}$. Furthermore, the commutation of I^W with $S^{\overline{W}}$ and $E^{\overline{W}}$ implies that operators I^W act trivially on the register $\mathcal{H}_{\overline{W}}$. Now since $x_{\overline{W}}$ is obtained by a measurement on $\mathcal{H}_{\overline{W}}$ we conclude that a_W has no dependence on $x_{\overline{W}}$.

Putting these together, we get that the player with question I_W produces x_W via a measurement on $\mathcal{H}_W$, then produces a_W with a measurement that depends on x_W and has a nontrivial support only on the game register $\mathcal{H}_G$. In other words $I^W_{x,a} = S^W_x \otimes N^x_a$ for some N^x_a that acts as identity on $\mathcal{H}_{\overline{W}}$. We can now let $\{N^x_a\}$ be the measurements in a strategy in the original game G and show that its value is large. In what follows we make this argument precise.

Proof of Theorem 1.29. Let $\mathscr{S}^{\text{intro}} = (\rho, \{P^q\}_{q\in Q^{\text{intro}}})$ be a synchronous strategy for G^{intro} that has value at least $1-\varepsilon$. Let $\widehat{\mathcal{H}}, \Pi, \widehat{\mathscr{A}}, \sigma$ be as defined in Theorem 1.26.

For every $W \in \{A, B\}$, $x \in \mathcal{X}$ and $a \in \mathcal{A}$ define the operator

$$\widetilde{W}^x_a := O^W_x \; I^W_{x,a} \; O^W_x \; .$$

Note that for every $W \in \{A, B\}$ and $x \in \mathcal{X}$ the operators $\{\widetilde{W}^x_a\}_{a\in\mathscr{A}}$ are pairwise orthogonal projections. For every $x \in \mathcal{X}$ define the *leftover* operator

$$\widetilde{W}^x_\perp := 1 - \sum_{a\in\mathscr{A}} \widetilde{W}^x_a \; .$$

Let $\widetilde{\mathscr{A}} = \mathscr{A} \cup \{\perp\}$ denote the expanded answer set. Then $\{\widetilde{W}^x_a\}_{a\in\widetilde{\mathscr{A}}}$ is a projective measurement for every $W \in \{A, B\}, x \in \mathcal{X}$.

Now for every $x \in \mathcal{X}, a \in \widetilde{\mathscr{A}}$ define

$$\widehat{W}^x_a := \Pi \; \widetilde{W}^x_a \; \Pi \; .$$

These are clearly positive semidefinite operators and

$$\sum_{a\in\widetilde{A}} \widehat{W}^x_a = \Pi \left(\sum_{a\in\widetilde{A}} \widetilde{W}^x_a \right) \Pi = \Pi^2 = \Pi \; .$$

Since Π is projection onto $\widehat{\mathcal{H}}$, the set of operators $\{\widehat{W}^x_a\}_{a\in\widetilde{A}}$ are POVMs on $\widehat{\mathcal{H}}$ for every x.

Our first goal is to show that for every $x, y \in \mathcal{X}, a, b \in \mathscr{A}$ it holds that

$$\rho(\widehat{A}^x_a \; \widehat{B}^y_b) \approx \rho(I^A_{x,a} \; I^B_{y,b}). \tag{1.4.3}$$

We achieve this by repeatedly applying Theorem 1.8. First recall from Theorem 1.25 that $\Pi \approx S^A_0 S^B_0$. Here we use 0 as a shorthand notation for 0^ℓ. So we have

$$\begin{aligned} \rho(\widehat{A}^x_a \; \widehat{B}^y_b) &= \rho(\Pi \; \widetilde{A}^x_a \; \Pi \; \widetilde{B}^y_b \; \Pi) \\ &\approx \rho(S^A_0 \; \widetilde{A}^x_a \; S^A_0 \; S^B_0 \; \widetilde{B}^y_b \; S^B_0), \end{aligned}$$

where we used Theorem 1.24 which states that S^A_0 and S^B_0 approximately commute. We continue by expanding $\widetilde{A}_a^x$ and $\widetilde{B}_a^x$ to obtain

$$\begin{aligned}\rho(S_0^A\ \widetilde{A}_a^x\ S_0^A\ S_0^B\ \widetilde{B}_b^y\ S_0^B) &= \rho(S_0^A\ (O_x^A\ I_{x,a}^A\ O_x^A)\ S_0^A\ S_0^B\ (O_y^B\ I_{y,b}^B\ O_y^B)\ S_0^B) \\ &\approx \rho((O_x^A\ S_x^A\ I_{x,a}^A\ S_x^A\ O_x^A)\ (O_y^B\ S_y^B\ I_{y,b}^B\ S_y^B\ O_y^B))\end{aligned}$$

where in the last line, we used Theorem 1.24 which states that $S_0^W\ O_x^W \approx O_x^W\ S_x^W$. By Theorem 1.30 we have $I_x^W \approx S_x^W$ so

$$\begin{aligned}\rho((O_x^A\ S_x^A\ I_{x,a}^A\ S_x^A\ O_x^A)\ (O_y^B\ S_y^B\ I_{y,b}^B\ S_y^B\ O_y^B)) &\approx \rho((O_x^A\ I_x^A\ I_{x,a}^A\ I_x^A O_x^A)(O_y^B\ I_y^B\ I_{y,b}^B\ I_y^B\ O_y^B)) \\ &\approx \rho((O_x^A\ I_{x,a}^A\ O_x^A)(O_y^B\ I_{y,b}^B\ O_y^B))\end{aligned}$$

where in the last line we used that $I_x^W = \sum_a I_{x,a}^W$ and that $I_{x,a}^W$ are projections. Now using Theorem 1.30 again, we know that erasure observables O^W approximately commute with $I^{\overline{W}}$ projections. We also know that erasure observables O^A and O^B approximately commute. So we continue as follows

$$\begin{aligned}\rho((O_x^A\ I_{x,a}^A\ O_x^A)(O_y^B\ I_{y,b}^B\ O_y^B)) &\approx \rho(O_y^B\ O_x^A\ I_{x,a}^A I_{y,b}^B\ O_x^A\ O_y^B) \\ &\approx \rho((O_y^B)^2\ (O_x^A)^2\ I_{x,a}^A\ I_{y,b}^B) \\ &= \rho(I_{x,a}^A\ I_{y,b}^B).\end{aligned}$$

This completes the proof of Equation (1.4.3).

Our next goal is to show that POVMs $\{\widehat{W}_a^x\}_a$ are close to being projective measurements. To this end, we first show that for any $x \in \mathcal{X}$ and $a, b \in \mathcal{A}$

$$\widehat{W}_a^x \widehat{W}_b^x \approx \widehat{W}_a^x \mathbf{1}_{a=b} \tag{1.4.4}$$

where $\mathbf{1}_{a=b}$ is the indicator variable for the equality $a = b$. First expanding according to the definitions

$$\begin{aligned}\widehat{W}^x_a\widehat{W}^x_b &= \Pi\ O^W_x\ I^W_{x,a}\ O^W_x\ \Pi\ O^W_x\ I^W_{x,b}\ O^W_x\ \Pi \\ &\approx \Pi\ O^W_x\ I^W_{x,a}\ O^W_x(S^{\overline{W}}_0\ S^W_0\ S^{\overline{W}}_0)O^W_x\ I^W_{x,b}\ O^W_x\ \Pi\end{aligned}$$

where in the last line we used the fact that $\Pi \approx S^{\overline{W}}_0\ S^W_0\ S^{\overline{W}}_0$ by Theorem 1.25. Now sampling projections $S^{\overline{W}}$ commute with erasure observables O^W and Introspection projections I^W so

$$\begin{aligned}\Pi\ O^W_x\ I^W_{x,a}\ O^W_x(S^{\overline{W}}_0\ S^W_0\ S^{\overline{W}}_0)O^W_x\ I^W_{x,b}\ O^W_x\ \Pi &\approx \Pi\ S^{\overline{W}}_0\ O^W_x\ I^W_{x,a}\ O^W_x\ S^W_0\ O^W_x\ I^W_{x,b}\ O^W_x\ S^{\overline{W}}_0\ \Pi \\ &\approx \Pi\ O^W_x\ I^W_{x,a}\ O^W_x\ S^W_0\ O^W_x\ I^W_{x,b}\ O^W_x\ \Pi\end{aligned}$$

where in the last line we use the fact that $\Pi \approx S^{\overline{W}}_0\ S^W_0\ S^{\overline{W}}_0$, and hence $\Pi\ S^{\overline{W}}_0 \approx \Pi \approx S^{\overline{W}}_0\ \Pi$. Now moving S^W_0 passed O^W_x using the relation $O^W_x\ S^W_0 \approx S^W_x\ O^W_x$, and then using the fact that $(O^W_x)^2 = I$ (as O^W_x is an observable), we get

$$\begin{aligned}\Pi\ O^W_x\ I^W_{x,a}\ O^W_x\ S^W_0\ O^W_x\ I^W_{x,b}\ O^W_x\ \Pi &\approx \Pi\ O^W_x\ I^W_{x,a}\ S^W_x\ (O^W_x)^2\ I^W_{x,b}\ O^W_x\ \Pi \\ &= \Pi\ O^W_x\ I^W_{x,a}\ S^W_x\ I^W_{x,b}\ O^W_x\ \Pi\end{aligned}$$

Now substituting I^W_x in place of S^W_x we get

$$\begin{aligned}\Pi\ O^W_x\ I^W_{x,a}\ S^W_x\ I^W_{x,b}\ O^W_x\ \Pi &\approx \Pi\ O^W_x\ I^W_{x,a}\ I^W_x\ I^W_{x,b}\ O^W_x\ \Pi \\ &\approx\ \Pi\ O^W_x\ I^W_{x,a}\ I^W_{x,b}\ O^W_x\ \Pi \\ &= \widehat{W}^x_a\ \delta_{a,b},\end{aligned}$$

where in the last line we used the fact that $I^W_{x,a}$ and $I^W_{x,b}$ are orthogonal projections when $a \neq b$. This completes the proof of Equation (1.4.4). From this, we immediately obtain that $(\widehat{W}^x_\perp)^2 \approx \widehat{W}^x_\perp$ also. So we established that

$$(\widehat{W}^x_a)^2 \approx \widehat{W}^x_a$$

for all $x \in \mathcal{X}$ and $a \in \widetilde{\mathcal{A}}$. Using Theorem 1.8, this in turn implies that

$$\rho((\widehat{W}_a^x)^2) \approx \rho(\widehat{W}_a^x)$$

for all $a \in \widetilde{\mathcal{A}}$. By definition of σ it is also true that

$$\sigma((\widehat{W}_a^x)^2) \approx \sigma(\widehat{W}_a^x).$$

So far we established that $\widehat{W}_a^x$, as operators in $\widehat{\mathscr{A}}$ acting on $\widehat{\mathcal{H}}$, are close to projections. So applying Theorem 1.17, for every $W \in \{A, B\}$ and $x \in \mathcal{X}$, there exists a projective measurement $\{W_a^x\}_a \subset \widehat{\mathscr{A}}$ that is close to $\{\widehat{W}_a^x\}_a$.

Our final goal is to build a strategy for G using these hard-earned projective measurements $\{A^x\}$ and $\{B^y\}$. On our way, we first need to relate $\{A_a^x\}_a$ and $\{B_b^y\}_b$ to the original measurements $I_{x,a}^A$ and $I_{y,b}^B$. For every $x, y \in \mathcal{X}$, $a, b \in \mathcal{A}$, we can write

$$\sigma(A_a^x B_b^y) \approx \sigma(\widehat{A}_a^x \widehat{B}_b^y) = \frac{\rho(\widehat{A}_a^x \widehat{B}_b^y)}{\rho(\Pi)} \approx \frac{\rho(\widehat{A}_a^x \widehat{B}_b^y)}{2^{-2\ell}} \approx \frac{\rho(I_{x,a}^A I_{y,b}^B)}{2^{-2\ell}}.$$

From this and Theorem 1.31, if x, y is nontrivial in G, it holds that

$$\frac{1}{2^{2\ell}} \sigma(A_a^x B_b^y) \approx \rho(I_{x,a,y,b}).$$

Therefore summing over all nontrivial question pairs, we have

$$\sum_{\substack{x,y \\ \text{nontrivial}}} \frac{1}{2^{2\ell}} \sum_{a,b \in \mathcal{A}} D(x,y,a,b) \sigma(A_a^x B_b^y) \approx \sum_{\substack{x,y \\ \text{nontrivial}}} \sum_{a,b \in \mathcal{A}} D(x,y,a,b) \rho(I_{x,a,y,b}).$$

A similar approximate identity holds when summing over trivial question pairs, that is

$$\sum_{\substack{x,y \\ \text{trivial}}} \frac{1}{2^{2\ell}} \sum_{a,b \in \mathcal{A}} D(x,y,a,b) \sigma(A_a^x \ B_b^y) \approx \sum_{\substack{x,y \\ \text{trivial}}} \sum_{a,b \in \mathcal{A}} D(x,y,a,b) \rho(I_{x,a,y,b}).$$

Let us see why this is true. First using the fact that $D(x,y,a,b) = 1$ for all a, b and trivial question pair x, y, we can write

$$\sum_{\substack{x,y\\ \text{trivial}}} \frac{1}{2^{2\ell}} \sum_{a,b\in\mathcal{A}} D(x,y,a,b)\sigma(A_a^x\ B_b^y) = \sum_{\substack{x,y\\ \text{trivial}}} \frac{1}{2^{2\ell}} \sum_{a,b\in\mathcal{A}} \sigma(A_a^x\ B_b^y) = \sum_{\substack{x,y\\ \text{trivial}}} \frac{1}{2^{2\ell}}$$

where in the last equality we used the fact that $\sum_{a,b} A_a^x\ B_b^y = I_{\widehat{\mathcal{H}}}$. Luckily, we also know that $\rho(I_{x,y}) \approx \frac{1}{2^{2\ell}}$ by Theorem 1.31, and thus

$$\begin{aligned}\sum_{\substack{x,y\\ \text{trivial}}} \frac{1}{2^{2\ell}} &\approx \sum_{\substack{x,y\\ \text{trivial}}} \rho(I_{x,y})\\ &= \sum_{\substack{x,y\\ \text{trivial}}} \sum_{a,b\in\mathcal{A}} \rho(I_{x,a,y,b})\\ &= \sum_{\substack{x,y\\ \text{trivial}}} \sum_{a,b\in\mathcal{A}} D(x,y,a,b)\rho(I_{x,a,y,b})\end{aligned}$$

where in the last line we again used the fact that $D(x,y,a,b) = 1$ for all a, b and trivial question pair x, y.

So overall we established that

$$\sum_{x,y} \frac{1}{2^{2\ell}} \sum_{a,b\in\mathcal{A}} D(x,y,a,b)\sigma(A_a^x\ B_b^y) \approx \sum_{x,y} \sum_{a,b\in\mathcal{A}} D(x,y,a,b)\rho(I_{x,a,y,b}).$$

The right-hand-side is an upper bound on the probability of winning of $\mathcal{S}^{\text{intro}}$ conditioned on the event that one of the players received the Introspection question I. This probability must be at least $1 - \delta(\varepsilon)$ by a simple averaging argument. So we have

$$\sum_{x,y} \frac{1}{2^{2\ell}} \sum_{a,b\in\mathcal{A}} D(x,y,a,b)\sigma(A_a^x\ B_b^y) = 1 - \delta(\varepsilon). \tag{1.4.5}$$

To summarize, at a high level, we constructed a set of operators A_a^x and B_b^y that together resemble a strategy for G albeit with two sets of measurement operators instead of one. It remains to show that we can turn this into a synchronous strategy. From Equation (1.4.5), for every $x \in \mathcal{X}$ it must be that

$$\sum_{a,b\in\mathcal{A}} D(x,x,a,b)\sigma(A_a^x\ B_b^x) = 1 - \delta(\varepsilon).$$

Since G is synchronous, we have $D(x,x,a,b) = 0$ whenever $a \neq b$. Therefore

$$\sum_{a\in\mathcal{A}} \sigma(A_a^x\ B_a^x) = 1 - \delta(\varepsilon)$$

or equivalently that $A_a^x \simeq B_a^x$ for every $x \in \mathcal{X}$. Therefore by Theorem 1.13, it holds that $A_a^x \approx B_a^x$ for every $x \in \mathcal{X}$. Therefore $\sigma(A_a^x\ B_b^y) \approx \sigma(A_a^x\ A_b^y)$. Using this approximation in (1.4.5) we conclude that

$$\sum_{x,y\in\mathcal{X}} \frac{1}{2^{2\ell}} \sum_{a,b\in\mathcal{A}} D(x,y,a,b)\sigma(A_a^x\ A_b^y) = 1 - \delta(\varepsilon). \tag{1.4.6}$$

Now we reduced to one set of measurement operators A_a^x that more closely resemble a synchronous strategy for G. Unfortunately we are not quite there as the set of operators $\{A_a^x\}_{a\in\mathcal{A}}$ is not a projective measurement if $A_\perp^x \neq 0$. We can resolve this issue by defining projective measurements $\{N_a^x\}_{a\in\mathcal{A}}$ for every x such that $N_{a^*}^x = A_{a^*}^x + A_\perp^x$ for some special element $a^* \in \mathcal{A}$ and $N_a^x = A_a^x$ for all $a \neq a^*$. Now $\mathcal{S} = (\sigma, \{N^x\}_{x\in\mathcal{X}})$ is a synchronous strategy and is such that $\sigma(N_a^x N_b^y) \geq \sigma(A_a^x A_b^y)$. So by (1.4.6), we have

$$\omega(G,\mathcal{S}) = \sum_{x,y\in\mathcal{X}} \frac{1}{2^{2\ell}} \sum_{a,b\in\mathcal{A}} D(x,y,a,b)\sigma(N_a^x N_b^y) = 1 - \delta(\varepsilon).$$

So for all sufficiently small ε, if there exists a strategy $\mathcal{S}^{\text{intro}}$ with value at least $1-\varepsilon$, we showed the existence of a strategy for G with value $1-\delta(\varepsilon)$. This in turn implies that for all $t \in \{q, co\}$

$$\omega_t^s(G^{\text{intro}}) = 1 \implies \omega_t^s(G) = 1.$$

Next we prove the inequality

$$\mathcal{E}(G^{\text{intro}}, 1) \geq \max\left\{\mathcal{E}(G, 1), 2^{2\ell}\right\}.$$

Suppose the finite dimensional strategy $\mathscr{S}^{\text{intro}} = (\rho, \{P^q\}_{q \in Q^{\text{intro}}})$ defined over a Hilbert space $\mathcal{H}$ has value 1. Then since the strategy restricted to the Question Sampling game also wins with probability 1, from Theorem 1.25, we get that the dimension of $\mathcal{H}$ is at least $2^{2\ell}$.

It remains to show that $\mathcal{E}(G^{\text{intro}}, 1) \geq \mathcal{E}(G, 1)$. Consider the finite-dimensional strategy $\mathscr{S} = (\sigma, \{N_a^x\})$ constructed above for the original game G. The inequality now follows from the fact that the strategy $\mathscr{S}$ is over the Hilbert space $\widehat{\mathcal{H}}$ defined in Theorem 1.26 which is a subspace of $\mathcal{H}$.

□

1.4.5 Proof of Theorem 1.27

From Theorem 1.20, we can let $G_n = (\mathcal{X}_n, \mathcal{A}_n, D_n)$ where $\mathcal{X}_n = \{0,1\}^{\ell_n}$ for some polynomial-time computable function ℓ_n of n. As we indicated in Theorem 1.20, the decider and checker Turing machines discard any string that comes after the ℓ_nth bit in their second and third input tapes. By assumption, for all sufficiently large n, we have $\ell_n \leq n^\alpha$, so from our previous statement, we can simply assume that $\ell_n = n^\alpha$. We design the algorithm $\mathcal{A}QuestionReduction_\alpha$ so that G_n^{intro} is the Introspection game $(G_n)^{\text{intro}}$ as defined in Section 1.4.2. From the definition of Introspection, it is straightforward to see that a polynomial-time algorithm exists that computes a description of $\mathscr{V}^{\text{intro}} = (D^{\text{intro}}, C^{\text{intro}})$ from a description of $\mathscr{V} = (D, C)$. The question length of G_n^{intro} is $\text{poly}(\alpha, \log n)$ by the definition of the Introspection game and the assumption that $\ell_n = n^\alpha$.

Given a pair of questions in G_n^{intro}, if they are both Question Sampling questions, then they are a nontrivial question pair in the Introspection game if and only if they are a nontrivial question pair in the Question Sampling game. If questions are both among special questions

$$S_A, E_A, I_A, I_AS_B, I_AE_B, S_B, E_B, I_B, I_BS_A, I_BE_A,$$

then the pair is nontrivial if they are connected by an edge or a self-loop in Figure 1.3. Since this graph has constant size, this can be decided in $O(1)$. If one question is a Question Sampling question that is not any of S_A, S_B, E_A, E_B and the other is a special Introspection game question

$$I_A, I_A S_B, I_A E_B, I_B, I_B S_A, I_B E_A,$$

then the pair is trivial. Therefore the complexity of deciding if a pair is trivial in G_n^{intro} is asymptotically the same as the complexity of deciding if a pair is trivial in QS_{n^α} which is $\mathrm{poly}(\alpha, \log n)$ (see Table 1.3).

Next we bound the complexity of $D^{\text{intro}}(n)$. The bit length of questions in the Introspection game G_n^{intro} is $\mathrm{poly}(\alpha, \log n)$. The answer length of G_n^{intro} is n^α (as the answer length of G_n is bounded by $\mathsf{TIME}_D(n)$). So the decider can compute in time $\mathrm{poly}(n^\alpha)$ whether the answer format of G_n^{intro} is respected. The decider, by simulating $D(n)$ and $C(n)$, can compute in time $\mathrm{poly}(|D|, |C|, \alpha, n^\alpha)$ whether a give quadruple $(q, r, \widehat{a}, \widehat{b})$ is an accepting quadruple in G_n^{intro} according to Table 1.4.

The completeness, soundness, and the dimension bound follow immediately from Propositions 1.28 and 1.29.

1.5 Answer Reduction

In this section we present the answer reduction transformation, whose properties are given by the following Theorem.

Theorem 1.32 (Answer Reduction)**.** *For all $\beta \in \mathbb{N}$ there exists a polynomial-time algorithm $\mathcal{A}AnswerReduction_\beta$ that takes as input a pair of Turing machines (D, C) and outputs a pair of Turing machines $(D^{\text{ans}}, C^{\text{ans}})$ such that the following holds. If $\mathscr{V} = (D, C)$ is a verifier for a* *sequence of games $\mathscr{G}_{\mathscr{V}} = (G_n)_{n\in\mathbb{N}}$ and $n_0 \in \mathbb{N}$ is an integer such that for all $n \geq n_0$,*

$$\begin{aligned}&\textit{The questions of } G_n \textit{ have length at most } \log^{\beta}(n),\\ &\mathsf{TIME}_C(n) = \log^{\beta} n\ , \ \textit{and}\\ &\mathsf{TIME}_D(n) \leq n^{\beta}\end{aligned}$$

then the output $\mathscr{V}^{\text{ans}} = (D^{\text{ans}}, C^{\text{ans}})$ is a verifier for a sequence of games $\mathscr{G}_{\mathscr{V}^{\text{ans}}} = (G_n^{\text{ans}})_{n\in\mathbb{N}}$ with the following properties. There exists $\gamma = \text{poly}(\beta)$ and $n_0^{\text{ans}} = \text{poly}(\gamma^{\gamma}, n_0)$ such that for all $n \geq n_0^{\text{ans}}$,

1. *(Complexity bounds)*

$$\mathsf{TIME}_{D^{\text{ans}}}(n) = \log^{\gamma} n$$
$$\mathsf{TIME}_{C^{\text{ans}}}(n) = \log^{\gamma} n\ .$$

2. *(Completeness) For all oracularizable synchronous strategies $\mathscr{S}$ for G_n, there exists an oracularizable synchronous strategy $\mathscr{S}^{\text{ans}}$ for G_n^{ans} such that*

$$\omega(G_n^{\text{ans}}, \mathscr{S}^{\text{ans}}) \geq \frac{1}{2} + \frac{1}{2}\omega(G_n, \mathscr{S}).$$

Furthermore, if $\mathscr{S}$ is finite-dimensional, then so is $\mathscr{S}^{\text{ans}}$.

3. *(Soundness) For all $t \in \{q, co\}$ we have*

$$\omega_t^s(G_n) < 1 \Longrightarrow \omega_t^s(G_n^{\text{ans}}) < 1\ .$$

4. *(Entanglement bound)*

$$\mathcal{E}(G_n^{\text{ans}}, 1) \geq \mathcal{E}(G_n, 1)\ .$$

Intuitively, the answer reduction transformation transforms a sequence of games $(G_1, G_2, \ldots)$ to a sequence $(G_1^{\text{ans}}, G_2^{\text{ans}}, \ldots)$ such that the time complexity of the "answer reduced" game G_n^{ans}

(in terms of computing its decision predicate) is *polylogarithmic* in the time complexity $T(n)$ of the "original game" G_n, and *polynomial* in the question length $Q(n)$ of G_n. The reason this transformation is called "answer reduction" is as follows. Suppose the original game G_n already has polylogarithmic-length questions (i.e. $Q(n) \leq \mathrm{poly}(\log T(n))$), but the answer lengths are, say, $\Omega(T(n))$; this will be the case when we apply answer reduction to the introspection games from the previous section. The resulting game G_n^{ans} then has time complexity $\mathrm{poly}(\log T(n))$ and in particular both the question and answer lengths of G_n^{ans} are at most $\mathrm{poly}(\log T(n))$.

We describe and analyze the answer reduction transformation $G \mapsto G^{\mathrm{ans}}$ for a single game (rather than a sequence), and then prove Theorem 1.32 in Section 1.5.5.

1.5.1 Overview

Let $Q, T \in \mathbb{N}$ be integers and let $G = (\mathcal{X}, \mathcal{A}, D)$ be a synchronous game where $\mathcal{X} = \{0,1\}^Q$ and $\mathcal{A} = \{0,1\}^T$, and $\mathsf{TIME}_D \leq T$ (meaning that on all inputs D halts within T timesteps). We can assume via padding that all questions have the same length, and all the answers have the same length.

Oracularization. We first give an overview of a transformation on G called *oracularization*. This produces the following game G^{orac}. The verifier may send a player either a question $x \in \mathcal{X}$ or a pair of questions $(x, y) \in \mathcal{X}^2$; thus the question alphabet is $\mathcal{X} \cup \mathcal{X}^2$. When a player receives a single question x we call them an *isolated player* and its question an *isolated question*. When a player receives a pair (x, y) we call them an *oracle player* and its question an *oracle question*.

If both players receive the same question (either isolated or oracle), then they must return the same answer. If one player receives an oracle question $(x, y) \in \mathcal{X}^2$ that is nontrivial for the original game G and the other receives an isolated question x (resp. receives y), then the players win if the oracle player responds with an answer pair $(a, b) \in \mathcal{A}^2$ such that $D(x, y, a, b) = 1$ and the isolated player responds with answer a (resp. responds with answer b). All other question combinations are considered trivial for G^{orac}, and the players automatically win in those cases.

Intuitively, in the oracularization of G an oracle player must "simulate" the behavior of the two players in G, and the isolated player (who only receives half of the oracle question) is used to check that the oracle player's answers (a, b) are produced in a way that a only depends on x and b only depends on y.

Answer Reduction. We now give a high-level overview of the *answer-reduced* game $G^{\text{ans}} = (\mathcal{X}^{\text{ans}}, \mathcal{A}^{\text{ans}}, D^{\text{ans}})$. The questions of G^{ans} are of the form (g, p), where g is a *game question* and p is a *proof question*. The game question g, intuitively, is meant to indicate a question from the original game G. However, in the answer reduction transformation, the game questions g come from the oracularization G^{orac} of G.

In the oracularized game G^{orac}, the players are supposed to respond with either an answer from $\mathcal{A}$ or from $\mathcal{A}^2$, depending on whether they received an isolated or oracle question. In the answer reduced game G^{ans}, however, the players do not respond with a "full-sized" answer in $\mathcal{A} \cup \mathcal{A}^2$. Instead, the verifier expects that the oracle players will generate a *proof* π that they can produce answers $(a, b) \in \mathcal{A}^2$ that satisfies the decision predicate of the game G, and furthermore these answers can be produced in a way such that a only depends on x and b only depends on y. The verifier does not examine this purported proof π in its entirety but instead uses the proof question p to query it in a constant number of locations.

The main point is this: now the players only have to respond with a constant number of bits corresponding to the proof locations queried, rather than with a symbol from the set $\mathcal{A} \cup \mathcal{A}^2$ (whose size we think of as growing to infinity). To ensure that the players' answers to the local queries are consistent with a global proof string π, and that the purported answers (a, b) (which are included in π) was generated "honestly" (e.g., a does not depend on x), the verifier performs cross-checks between the two players. Before describing the format of the proof questions, we first explain in detail what a proof is supposed to look like.

The starting point is the well-known *Cook-Levin reduction* from classical computer science: this is an efficient transformation that maps Turing machines M to 3SAT formulas φ_M such that there is an input w (called the *witness*) where $M(w) = 1$ if and only if φ_M is satisfiable. Furthermore, it is well-known [48, Chapter 20] that the clauses of the SAT formula φ_M can be computed extremely efficiently – in fact, in time that is *logarithmic* in the size of the entire SAT formula (if we treat the description length of M as a constant):

Theorem 1.33 (Cook-Levin Theorem)**.** *For all* 1*-input Turing machines M and integers $R, T \in \mathbb{N}$, there exists a 3SAT formula $\varphi(M, T, R)$ (called a* Cook-Levin SAT formula*) with $L = \mathrm{poly}(|M|, T, R)$ variables, such that*

- *For all $w \in \{0,1\}^R$ such that $M(w)$ accepts within T time steps, there exists a unique satisfying assignment π for the formula $\varphi(M, T, R)$, and furthermore $\pi_{\leq R}$ (the first R bits of π) is w, and*
- *For all satisfying assignments π for the formula $\varphi(M, T, R)$, the Turing machine M accepts $\pi_{\leq R}$ within T time steps.*

Furthermore, there exists a polynomial-time algorithm $\mathcal{A}CookLevin$ that takes as input a tuple (M, T, R, i, j, k) where R, T, i, j, k are integers written in binary, and outputs the literals of the clause(s) of $\varphi(M, T, R)$ that contains the i-th, j-th, and k-th variables (or outputs a null symbol if no such clause exists).

We note that while the algorithm $\mathcal{A}CookLevin$ runs in polynomial time in the length of its input, it runs in *logarithmic* time in the number of variables of the Cook-Levin SAT formula $\varphi(M, T, R)$. This is because the length of the input tuple (M, T, R, i, j, k) is $O(|M| + \log T + \log R + \log i + \log j + \log k)$, and since the variable indices i, j, k are at most $\mathrm{poly}(|M|, T, R)$, the time complexity of the algorithm $\mathcal{A}CookLevin$ is at most $\mathrm{poly}(|M|, \log T, \log R)$.

The verifier in the answer-reduced game G^{ans} expects an oracle player who received game question pair $g = (x, y)$ to compute a string π satisfying the following:

1. π is a satisfying assignment for the Cook-Levin SAT formula $\varphi(D_{x,y}, T, 2T)$ where $D_{x,y}$ is the 1-input Turing machine that on input $(a, b) \in \{0,1\}^{2T}$ executes the Turing machine D on input (x, y, a, b), and

2. π is composed of three strings $(a, b, \pi') \in \{0,1\}^T \times \{0,1\}^T \times \{0,1\}^L$ where $L = \mathrm{poly}(|D_{x,y}|, T) = \mathrm{poly}(|D|, Q, T)$. Here we used that the description length $|D_{x,y}| = O(|D| + |x| + |y|) = \mathrm{poly}(|D|, Q)$.

Henceforth we shall abbreviate the Cook-Levin formula $\varphi(D_{x,y}, T, 2T)$ as $\varphi_{x,y}$.

The verifier asks proof questions p in order to ascertain whether it is possible for an oracle player to generate a proof π satisfying these conditions. This requires the verifier to ask proof questions to both oracle players *and* isolated players. Oracle players (who get game question pair $g = (x, y)$) can get asked to provide:

- A single bit π_i of the proof π, or
- A triple of bits (π_i, π_j, π_k) from the proof π (which may not necessarily correspond to a clause in $\varphi_{x,y}$).

An isolated player (who gets a single question x or y) is asked to provide a pair of bits (a_i, a_j) of their purported answer $a \in \{0,1\}^T$.

Thus the proof questions are sampled from the set $[L] \cup [L]^2 \cup [L]^3$. Thus the question and answer sets for G^{ans} are

$$\mathcal{X}^{\mathrm{ans}} = \mathcal{X}^{\mathrm{orac}} \times ([L] \cup [L]^2 \cup [L]^3) \qquad \mathcal{A}^{\mathrm{ans}} = \{0,1\} \cup \{0,1\}^2 \cup \{0,1\}^3$$

where $\mathcal{X}^{\mathrm{orac}} = \mathcal{X} \cup \mathcal{X}^2$ is the question alphabet for the oracularized game G^{orac}.

Since the player answers (a, b) are supposed to be embedded into a proof π, we use the following mapping to translate between indexing into answer a or b versus indexing into the proof π: given an index $i \in [T]$, the i-th bit of the *first* answer a (corresponding to the *first* question x) is mapped to index $\eta(i) = i$ of the proof π, and the i-th bit of the *second* answer b (corresponding to the *second* question y) is mapped to index $\lambda(i) = T + i$ of π.

1.5.2 The answer-reduced decision procedure

We now formally specify the decision procedure D^{ans}. On input $(\widehat{x}, \widehat{y}, \widehat{a}, \widehat{b})$, it checks if $(\widehat{x}, \widehat{y})$ (resp. $(\widehat{y}, \widehat{x})$) is one of the nontrivial question pairs of G^{ans}, which are presented in Table 1.5. If so, then it accepts if and only if the answers $(\widehat{a}, \widehat{b})$ (resp. $(\widehat{b}, \widehat{a})$) satisfy the corresponding winning condition. Otherwise, if $(\widehat{x}, \widehat{y})$ is a trivial question, the verifier automatically accepts.

Nontrivial Question Pair $(\widehat{x}, \widehat{y})$	**Winning Condition on Answers** $(\widehat{a}, \widehat{b})$
$\widehat{x} = \widehat{y}$	$\widehat{a} = \widehat{b}$
$\widehat{x} = ((x,y),i)$ where (x,y) is nontrivial for G $\widehat{y} = ((x,y),(j,k,\ell))$ where $i \in \{j,k,\ell\}$ $\widehat{a} = r_i \in \{0,1\}$, $\widehat{b} = (s_j, s_k, s_\ell) \in \{0,1\}^3$	(s_j, s_k, s_ℓ) satisfies clause(s) specified by $\mathcal{A}CookLevin(D_{x,y}, T, 2T, j, k, \ell)$ and $r_i = s_i$, where
$\widehat{x} = ((x,y),i)$ where (x,y) is nontrivial for G $\widehat{y} = (x,(j,k))$ where $i \in \{\eta(j), \eta(k)\}$	$r_i = a_{\eta^{-1}(i)}$ where $\widehat{a} = r_i \in \{0,1\}$, $\widehat{b} = (a_j, a_k) \in \{0,1\}^2$
$\widehat{x} = ((x,y),i)$ where (x,y) is nontrivial for G $\widehat{y} = (y,(j,k))$ where $i \in \{\lambda(j), \lambda(k)\}$	$r_i = b_{\lambda^{-1}(i)}$ where $\widehat{a} = r_i \in \{0,1\}$, $\widehat{b} = (b_j, b_k) \in \{0,1\}^2$

Table 1.5: The nontrivial question pairs and winning conditions for the game G^{ans}.

Table 1.5 should be read as follows. In the second row, for example, the nontrivial question pair is where $\widehat{x} = (g_1, p_1)$ where $g_1 = g_2 = (x,y) \in \mathcal{X}^2$ where (x,y) is nontrivial for G, $p_1 = i$ for some $i \in [L]$, and $p_2 = (j,k,\ell) \in [L]^3$ such that $i \in \{j,k,\ell\}$. The answer $\widehat{a}$ is expected to be a single bit r_i and $\widehat{b}$ is expected to be a triple of bits (s_j, s_k, s_ℓ); otherwise the verifier rejects. The verifier then checks that $r_i = s_i$ (i.e. the first player's assignment to the i-th variable of the proof is the same as the second player's assignment to the i-th variable), and the second player's assignment (s_j, s_k, s_ℓ) satisfies the clause of $\varphi_{x,y}$ that involves the triple of variables (j,k,ℓ). If there is no clause, then the verifier accepts any assignment to those variables.

1.5.3 Completeness of answer reduction

We now prove the completeness property of the answer reduction transformation. Similarly to Section 1.4, the completeness property implies that the value of G^{ans} is lower bounded by the value of G.

Proposition 1.34. *For all oracularizable synchronous strategies $\mathscr{S}$ for G, there exists an oracularizable synchronous strategy $\mathscr{S}^{\text{ans}}$ for G^{ans} such that*

$$\omega(G_n^{\text{ans}}, \mathscr{S}^{\text{ans}}) \geq \frac{1}{2} + \frac{1}{2}\omega(G_n, \mathscr{S}) \ .$$

Furthermore, if $\mathscr{S}$ is finite-dimensional then so is $\mathscr{S}^{\text{ans}}$.

Proof. Let $\mathscr{S} = (\tau, \{M^x\})$ be a tracial synchronous strategy for G that commutes on the set of nontrivial questions of G. We now define a tracial strategy $\mathscr{S}^{\text{ans}} = (\tau, \{N^x\})$ for G^{ans}. Before doing so, we define some intermediate measurements. Let $\mathcal{X}$ and $\mathcal{A}$ denote the question and answer sets of G, respectively. For all $x, y \in \mathcal{X}, a, b \in \mathcal{A}$:

- $N^{x,y}_{a,b} = \begin{cases} M^x_a \ M^y_b & \text{if } (x,y) \text{ is a nontrivial question for } G \\ 1 & \text{if } (x,y) \text{ is a trivial question for } G \text{ and } a = b = 0 \\ 0 & \text{otherwise} \end{cases}$
- $N^x_a = M^x_a$.

The POVM N^x is projective because M^x is projective. Note that whenever (x, y) is a nontrivial question of G, the projectors M^x_a and M^y_b commute, so $N^{x,y}$ is always projective.

Now we define the measurements for $\mathscr{S}^{\text{ans}}$:

1. $N^{x,j,k} = N^x_{[a \mapsto (a_j, a_k)]}$
2. $N^{x,y,i} = N^{x,y}_{[(a,b) \mapsto \pi_i]}$
3. $N^{x,y,i,j,k} = N^{x,y}_{[(a,b) \mapsto (\pi_i, \pi_j, \pi_k)]}$

where here π denotes the unique satisfying assignment to the Cook-Levin SAT formula $\varphi_{x,y}$ such that $\pi = (a, b, w)$ for some string w.

We now verify that the strategy $\mathscr{S}^{\text{ans}}$ satisfies the desired properties: it is synchronous because the measurements are all projective. It commutes on the nontrivial questions of G^{ans}, as seen by the following case analysis: letting $\widehat{x} = (g_1, p_1)$ and $\widehat{y} = (g_2, p_2)$,

1. If $\widehat{x} = \widehat{y}$, then clearly the measurements $N^{\widehat{x}}$ and $N^{\widehat{y}}$ commute with each other because they are the same measurement.

2. If $g_1 = g_2 = (x, y)$, $p_1 = i$, and $p_2 = (j, k, \ell)$, then $N^{\widehat{x}}$ and $N^{\widehat{y}}$ are marginalizations of the same projective measurement $\{N^{x,y}\}$, and thus $N^{\widehat{x}}$, $N^{\widehat{y}}$ commute with each other.

3. If $g_1 = (x, y)$, $p_1 = i$, $g_2 = x$ (or $g_2 = y$) and $p_2 = (j, k)$, then either (x, y) is a trivial question for G (in which case $N^{\widehat{x}}$ is the identity measurement, which commutes with everything), or (x, y) is a nontrivial question, in which case $N^{\widehat{x}}$ is a marginalization of the product $M^x_a M^y_b$, whereas $N^{\widehat{y}}$ is a marginalization of M^x_a (resp. M^y_b), which commutes with M^y_b (resp. M^x_a).

Clearly, the dimensionality of $\mathscr{S}^{\text{ans}}$ is the same as the dimension of $\mathscr{S}$.

Finally, we can evaluate the winning probability of $\mathscr{S}^{\text{ans}}$ as follows: let γ denote the probability that at least one of the players that receives a question (g, p) where $g = (x, y)$ with (x, y) nontrivial for G. If neither player receives such a game question, then either their question pair $(\widehat{x}, \widehat{y})$ is trivial for G^{ans} (in which case the players win automatically), or $\widehat{x} = \widehat{y}$ (in which case the players win because their strategy is synchronous).

Suppose one of the players (say, the first player) receiving such question pair $\widehat{x} = (g, p)$. Intuitively, this oracle player will simultaneously measure M^x and M^y to obtain answers (a, b). Since x an y are drawn uniformly at random, the probability that $D(x, y, a, b) = 1$ is exactly $\omega(G, \mathscr{S})$. Suppose (a, b) are winning answers. Then the oracle player can compute a satisfying assignment $\pi = (a, b, w)$ for the Cook-Levin formula $\varphi_{x,y}$ – this uses the assumption that $\mathsf{TIME}_D \leq T$. Furthermore, the second player, no matter what question $\widehat{y}$ they receive, they will be able to obtain perfectly consistent answers (if they receive game question (x, y), then they can obtain the same proof $\pi = (a, b, w)$; if they receive game questions x or y, they will obtain the same answers a or b, respectively). Thus the success probability of the strategy $\mathscr{S}^{\text{ans}}$ overall is at least

$$\omega(G^{\text{ans}}, \mathscr{S}^{\text{ans}}) \geq (1-\gamma) + \gamma\ \omega(G, \mathscr{S})\ .$$

Since $\gamma \leq 1/2$, the Proposition follows. $\square$

1.5.4 Soundness of answer reduction

Proposition 1.35. *For all $t \in \{q, co\}$, $\omega_t^s(G) < 1 \implies \omega_t^s(G^{\text{ans}}) < 1$.*

Proof. Let $\mathscr{S}^{\text{ans}} = (\tau, \{N^{\widehat{x}}\})$ be a tracial synchronous strategy for G^{ans} that has value $1-\varepsilon$. Our goal will be to construct measurements $\{M_a^x\}$ and $\{M_\pi^{x,y}\}$ that produce entire answer strings and entire proof strings, respectively. They will be constructed from the $N^{x,y,i}$ and $N^{x,j,k}$ measurements which only provide "local" views of purported answer and purported proof strings. In order to "paste" these "local" views together into consistent "global" views, we will need to establish pairwise consistency conditions between the measurement operators of the strategy $\mathscr{S}^{\text{ans}}$.

From the condition that the strategy $\mathscr{S}^{\text{ans}}$ has value $1-\varepsilon$, we obtain the following consistency conditions pointwise over all $x, y \in \mathcal{X}$ and $i, j, k, \ell \in [L]$:

- $N_r^{x,y,i} \simeq N^{x,y,j,k,\ell}_{[(s_j,s_k,s_\ell)\mapsto s_i|r]}$ whenever $i \in \{j, k, \ell\}$,
- $N_r^{x,y,\eta(j)} \simeq N^{x,j,k}_{[(a_j,a_k)\mapsto a_j|r]}$ and $N_r^{x,y,\eta(k)} \simeq N^{x,j,k}_{[(a_j,a_k)\mapsto a_k|r]}$
- $N_r^{x,y,\lambda(j)} \simeq N^{y,j,k}_{[(a_j,a_k)\mapsto a_j|r]}$ and $N_r^{x,y,\lambda(k)} \simeq N^{y,j,k}_{[(a_j,a_k)\mapsto a_k|r]}$

In other words, the assignments to variables that are in common to both players' questions are approximately consistent. Here and throughout this proof, all approximations "$\simeq$" and "$\approx$" implicitly hide some error function $\delta(\varepsilon)$ that goes to 0 as $\varepsilon \to 0$. Furthermore, the error function will generally be different each time the "$\simeq$" or "$\approx$" notation is used. (See Section 1.2.5 for a more in-depth discussion of approximations and asymptotics).

We first prove a utility lemma, which will be used repeatedly throughout the analysis of soundness:

Lemma 1.36. *Let $t \in \mathbb{N}$ and let $A = \{A_r\}$ denote a projective measurement with outcomes in $\mathcal{R}^t$. For $i \in [t]$, let $B^i = \{B^i_r\}$ be a POVM with outcomes in $\mathcal{R}$. Suppose that for all $i \in [t]$,*

$$A_{[r \mapsto r_i | c]} \simeq_\delta B^i_c$$

where the answer summation is over $c \in \mathcal{R}$. Then for all permutations $\sigma \in S_t$, we have that

$$A_r \approx_{t\sqrt{2\delta}} B^{\sigma(1)}_{r_{\sigma(1)}} \cdot B^{\sigma(2)}_{r_{\sigma(2)}} \cdots B^{\sigma(t)}_{r_{\sigma(t)}} \; .$$

In other words, the measurement $\{A_r\}$ is $t\sqrt{2\delta}$-close to the product of the $\{B^i_{r_i}\}$, in any order. Furthermore,

$$B^{\sigma(1)}_{r_{\sigma(1)}} \cdot B^{\sigma(2)}_{r_{\sigma(2)}} \cdots B^{\sigma(t)}_{r_{\sigma(t)}} \approx_{2t\sqrt{2\delta}} B^{\rho(1)}_{r_{\rho(1)}} \cdot B^{\rho(2)}_{r_{\rho(2)}} \cdots B^{\rho(t)}_{r_{\rho(t)}}$$

for all permutations $\rho, \sigma \in S_t$.

Proof. We first argue that

$$A_r \approx_{t\sqrt{2\delta}} B^1_{r_1} \cdot B^2_{r_2} \cdots B^t_{r_t} \; .$$

Using Theorem 1.13 we get that for all $i \in [t]$,

$$A_{[r \mapsto r_i | c]} \approx_{\sqrt{2\delta}} B^i_r \; . \tag{1.5.1}$$

Using Theorem 1.16 we can right-multiply Equation (1.5.1) for $i = 1$ by the measurement $A_{[r \mapsto r_2 : d]}$ to deduce

$$A_{[r \mapsto r_1]} \cdot A_{[r \mapsto r_2]} \approx_{\sqrt{2\delta}} B^1_{r_1} \cdot A_{[r \mapsto r_2]} \tag{1.5.2}$$

Using using Theorem 1.16 again we get that the right hand side of Equation (1.5.2) is $\sqrt{2\delta}$-close to $B^1_{r_1} \cdot B^2_{r_2}$, and therefore via the triangle inequality we get

$$A_{[r \mapsto r_1]} \cdot A_{[r \mapsto r_2]} \approx_{2\sqrt{2\delta}} B^1_{r_1} \cdot B^2_{r_2}.$$

Notice that since A is projective, we have

$$A_{[r \mapsto r_1]} \cdot A_{[r \mapsto r_2]} = A_{[r \mapsto (r_1, r_2)]}$$

Thus $A_{[r \mapsto (r_1, r_2)]} \approx_{2\sqrt{2\delta}} B^1_{r_1} \cdot B^2_{r_2}$. By repeatedly using Theorem 1.16, we deduce that

$$A_r \approx_{t\sqrt{2\delta}} B^1_{r_1} \cdot B^2_{r_2} \cdots B^t_{r_t}$$

as desired. The same argument holds with any other ordering of the B^i's.

The "Furthermore" part of the lemma then follows from the triangle inequality. □

Constructing the M^x_a measurements. The first step is to show that, for fixed x, y, the $\{N^{x,y,i}\}$ measurements approximately commute.

Fix $i, j \in [T]$. Using Theorem 1.36 with $A = N^{x,i,j}$, $B^1 = N^{x,y,\eta(i)}$ and $B^2 = N^{x,y,\eta(j)}$, we get

$$N^{x,y,\eta(j)}_s \cdot N^{x,y,\eta(i)}_r \approx N^{x,y,\eta(i)}_r \cdot N^{x,y,\eta(j)}_s \ . \tag{1.5.3}$$

The next step is to deduce that the marginalizations of the $N^{x,i,j}$ measurements commute. Since $N^{x,y,\eta(i)}_r \approx N^{x,i,k}_{[(a_i,a_k) \mapsto a_i | r]}$ and $N^{x,y,\eta(j)}_s \approx N^{x,j,k}_{[(a_j,a_k) \mapsto a_j | s]}$ for all $k \in [T]$. Thus, using Theorem 1.16 twice we get

$$N^{x,y,\eta(j)}_s \cdot N^{x,y,\eta(i)}_r \approx N^{x,y,\eta(j)}_s \cdot N^{x,i,k}_{[(a_i,a_k) \mapsto a_i | r]} \approx N^{x,j,k}_{[(a_j,a_k) \mapsto a_j | s]} \cdot N^{x,i,k}_{[(a_i,a_k) \mapsto a_i | r]}$$

and similarly we get

$$N_r^{x,y,\eta(i)} \cdot N_s^{x,y,\eta(j)} \approx N^{x,i,k}_{[(a_i,a_k)\mapsto a_i|r]} \cdot N^{x,j,k}_{[(a_j,a_k)\mapsto a_j|s]} \ .$$

Using the triangle inequality and Equation (1.5.3), we get for all $x \in \mathcal{X}$ and $i, j, k \in [T]$,

$$N^{x,j,k}_{[(a_j,a_k)\mapsto a_j|s]} \cdot N^{x,i,k}_{[(a_i,a_k)\mapsto a_i|r]} \approx N^{x,i,k}_{[(a_i,a_k)\mapsto a_i|r]} \cdot N^{x,j,k}_{[(a_j,a_k)\mapsto a_j|s]}$$

Fix an arbitrary $k \in [T]$ and define

$$N_r^{x,i} = N^{x,i,k}_{[(a_i,a_k)\mapsto a_i|r]} \ .$$

Fix an $x \in \mathcal{X}$. We invoke the Pasting Lemma (Theorem 1.18) on the set of measurements $\{N^{x,i}\}_{i\in[T]}$, and obtain a projective measurement $M^x = \{M_a^x\}$ with outcomes in $\{0,1\}^T$ such that for all $i \in [T]$,

$$M^x_{[a\mapsto a_i|r]} \approx N_r^{x,i} \ .$$

Furthermore, by the triangle inequality, for all $y \in \mathcal{X}$ we have that

$$M^x_{[a\mapsto a_i|r]} \approx N_r^{x,y,\eta(i)} \ . \tag{1.5.4}$$

Via the same arguments as above we have that $N_r^{x,i} \approx N_r^{y,x,\lambda(i)}$, which means that

$$M^x_{[a\mapsto a_i|r]} \approx N_r^{y,x,\lambda(i)} \ .$$

Constructing the $M_\pi^{x,y}$ measurements. Fix $x, y \in \mathcal{X}$ and $i, j, k \in [L]$. Using Theorem 1.36 with $A = N^{x,y,i,j,k}$, $B^1 = N^{x,y,i}$, $B^2 = N^{x,y,j}$, and $B^3 = N^{x,y,k}$ we get that the product of $N_r^{x,y,i}$, $N_s^{x,y,j}$, and $N_t^{x,y,k}$ (using any ordering) is close to $N^{x,y,i,j,k}$.

In particular, we have

$$N_r^{x,y,i} \cdot N_s^{x,y,j} \approx N_s^{x,y,j} \cdot N_r^{x,y,i} \ .$$

Using the Pasting Lemma on the set of measurements $\{N^{x,y,i}\}$, we obtain a projective measurement $M^{x,y} = \{M_\pi^{x,y}\}$ with outcomes in $\{0,1\}^R$ (i.e. proof strings) such that

$$M^{x,y}_{[\pi\mapsto\pi_i|r]} \approx N_r^{x,y,i} \ .$$

Using Theorem 1.16 repeatedly, we get that for all $i, j, k \in [L]$,

$$\begin{aligned} M^{x,y}_{[\pi\mapsto\pi_i|r]} \cdot M^{x,y}_{[\pi\mapsto\pi_j|s]} \cdot M^{x,y}_{[\pi\mapsto\pi_k|t]} &\approx N_r^{x,y,i} \cdot M^{x,y}_{[\pi\mapsto\pi_j|s]} \cdot M^{x,y}_{[\pi\mapsto\pi_k|t]} \\ &\approx N_r^{x,y,i} \cdot N_s^{x,y,j} \cdot M^{x,y}_{[\pi\mapsto\pi_k|t]} \\ &\approx N_r^{x,y,i} \cdot N_s^{x,y,j} \cdot N_t^{x,y,k} \\ &\approx N_{r,s,t}^{x,y,i,j,k} \end{aligned}$$

where the last approximation follows from our earlier application of Theorem 1.36. Since $M_\pi^{x,y}$ is projective, we have that

$$M^{x,y}_{[\pi\mapsto(\pi_i,\pi_j,\pi_k)|(r,s,t)]} \approx N_{r,s,t}^{x,y,i,j,k} \ . \tag{1.5.5}$$

We now relate the $M^{x,y}$ measurements to the M^x measurements constructed previously. Using the triangle inequality with Equation (1.5.4) we get for all $x, y \in \mathcal{X}$ and $j \in [T]$,

$$M^{x,y}_{[\pi\mapsto\pi_{\eta(j)}|r]} \approx M^x_{[a\mapsto a_j|r]} \tag{1.5.6}$$

and similarly

$$M^{x,y}_{[\pi\mapsto\pi_{\lambda(j)}|r]} \approx M^y_{[a\mapsto a_j|r]} \ . \tag{1.5.7}$$

Before proceeding we prove a utility lemma that allows us to argue that if all the marginalizations of projective measurements are close, then the original measurements must be close.

Lemma 1.37. *Let A and B be projective measurements with outcomes in $\{0,1\}^K$ such that for all $i \in [K]$, we have $A_{[r\mapsto r_i]} \approx_\kappa B_{[r\mapsto r_i]}$. Then*

$$A_r \approx_{K\kappa} B_r \ .$$

Proof. We prove this inductively on the prefix length of r. For the base case $t = 1$, we have that $A_{[r\mapsto r_1]} \approx_\kappa B_{[r\mapsto r_1]}$ by assumption. Let the inductive hypothesis be that for some $t \geq 1$, $A_{[r\mapsto r_{\leq t}]} \approx_{t\kappa} B_{[r\mapsto r_{\leq t}]}$ where $r_{\leq t}$ denotes the first t bits of r. Then using Theorem 1.16 twice, we get that

$$A_{[r\mapsto r_{\leq t}]} \cdot A_{[r\mapsto r_{t+1}]} \approx_{t\kappa} B_{[r\mapsto r_{\leq t}]} \cdot A_{[r\mapsto r_{t+1}]} \approx_\kappa B_{[r\mapsto r_{\leq t}]} \cdot B_{[r\mapsto r_{t+1}]}$$

which, via the triangle inequality, implies that

$$A_{[r\mapsto r_{\leq t+1}]} \approx_{t\kappa} B_{[r\mapsto r_{\leq t+1}]}$$

where we used the fact that the A and B measurements are projective. By induction, this statement is true for all t, and since $A_{[r\mapsto r_{\leq K}]} = A_r$ and $B_{[r\mapsto r_{\leq K}]} = B_r$, we conclude the proof. □

Applying Theorem 1.37 to Equations (1.5.6) and (1.5.7) and interpreting the outcome of the $M^{x,y}$ measurement as a triple $(a,b,w) \in \{0,1\}^T \times \{0,1\}^T \times \{0,1\}^L$, we get

$$M^{x,y}_{[(a,b,w)\mapsto a]} \approx M^x_a \tag{1.5.8}$$

$$M^{x,y}_{[(a,b,w)\mapsto b]} \approx M^y_b \ . \tag{1.5.9}$$

Using Theorem 1.16 several times with Equations (1.5.8) and (1.5.9) we get

$$\begin{aligned} M^{x,y}_{[(a,b,w)\mapsto a]} \cdot M^{x,y}_{[(a,b,w)\mapsto b]} \cdot M^{x,y}_{[(a,b,w)\mapsto a]} &\approx M^x_a \cdot M^{x,y}_{[(a,b,w)\mapsto b]} \cdot M^{x,y}_{[(a,b,w)\mapsto a]} \\ &\approx M^x_a \cdot M^y_b \cdot M^{x,y}_{[(a,b,w)\mapsto a]} \\ &\approx M^x_a \cdot M^y_b \cdot M^x_a \end{aligned}$$

and thus

$$M^{x,y}_{[(a,b,w)\mapsto(a,b)]} \approx M^x_a \cdot M^y_b \cdot M^x_a \ . \tag{1.5.10}$$

Evaluating the probability of success of the M^x measurements. Define the tracial synchronous strategy $\mathscr{S} = (\tau, \{M^x\})$ for game G. Its success probability can be lower-bounded as follows:

$$\begin{aligned}
\omega(G,\mathscr{S}) &= \mathop{\mathbf{E}}_{x,y} \sum_{a,b} D(x,y,a,b) \cdot \tau(M^x_a \ M^y_b) \\
&= \mathop{\mathbf{E}}_{x,y} \sum_{a,b} D(x,y,a,b) \cdot \tau(M^x_a \cdot M^y_b \cdot M^x_a) \\
&= \mathop{\mathbf{E}}_{x,y} \sum_{a,b} D(x,y,a,b) \cdot \Big(\tau\Big(M^{x,y}_{[(a,b,w)\mapsto(a,b)]}\Big) + \tau\Big(M^{x,y}_{[(a,b,w)\mapsto(a,b)]} - M^x_a \ M^y_b \ M^x_a\Big)\Big) \\
&\geq \mathop{\mathbf{E}}_{x,y} \sum_{a,b} D(x,y,a,b) \cdot \tau\Big(M^{x,y}_{[(a,b,w)\mapsto(a,b)]}\Big) - \mathop{\mathbf{E}}_{x,y} \sum_{a,b} \Big|\tau\Big(M^{x,y}_{[(a,b,w)\mapsto(a,b)]} - M^x_a \ M^y_b \ M^x_a\Big)\Big|
\end{aligned}$$

We bound the second term first. From Theorem 1.13 applied to Equation (1.5.10) we get that $M^{x,y}_{[(a,b,w)\mapsto(a,b)]} \simeq_\delta M^x_a \cdot M^y_b \cdot M^x_a$ for some proper error function $\delta = \delta(\varepsilon)$. We then apply Theorem 1.15 to get that

$$\mathop{\mathbf{E}}_{x,y} \sum_{a,b} \Big|\tau\Big(M^{x,y}_{[(a,b,w)\mapsto(a,b)]} - M^x_a \ M^y_b \ M^x_a\Big)\Big| \leq 2\delta \ .$$

Next, we evaluate

$$\begin{aligned}
&\mathop{\mathbf{E}}_{x,y} \sum_{a,b} D(x,y,a,b) \cdot \tau\Big(M^{x,y}_{[(a,b,w)\mapsto(a,b)]}\Big) \\
&= \mathop{\mathbf{E}}_{x,y} \sum_{a,b,w} D(x,y,a,b) \cdot \tau\Big(M^{x,y}_{a,b,w}\Big) \\
&= \mathop{\mathbf{E}}_{x,y} \sum_{a,b,w} \mathbf{1}[\exists w' : (a,b,w') \text{ satisfies } \varphi_{x,y}] \cdot \tau\Big(M^{x,y}_{a,b,w}\Big) \\
&\geq \mathop{\mathbf{E}}_{x,y} \sum_{a,b,w} \mathbf{1}[(a,b,w) \text{ satisfies } \varphi_{x,y}] \cdot \tau\Big(M^{x,y}_{a,b,w}\Big) \\
&= 1 - \mathop{\mathbf{E}}_{x,y} \sum_{a,b,w} \mathbf{1}[(a,b,w) \text{ does not satisfy } \varphi_{x,y}] \cdot \tau\Big(M^{x,y}_{a,b,w}\Big)
\end{aligned}$$

where in the second line we use the conclusion of Theorem 1.33 that since $\mathsf{TIME}_D \leq T$, we have $D(x, y, a, b) = 1$ if and only if there exists a satisfying assignment (a, b, w') for the Cook-Levin formula $\varphi_{x,y}$.

Via the union bound, the probability that $\pi = (a, b, w)$ does not satisfy $\varphi_{x,y}$ is at most the sum, over all $i, j, k \in [L]$, that (π_i, π_j, π_k) does not satisfy a clause in $\varphi_{x,y}$ (if there exists such a clause). Thus we have

$$\mathop{\mathbf{E}}_{x,y} \sum_{a,b,w} \mathbf{1}[(a, b, w) \text{ unsat. } \varphi_{x,y}] \cdot \tau\Big(M^{x,y}_{a,b,w}\Big) \leq \mathop{\mathbf{E}}_{x,y} \sum_{i,j,k} \sum_{\pi} \mathbf{1}[(\pi_i, \pi_j, \pi_k) \text{ unsat. } \varphi_{x,y}] \cdot \tau\Big(M^{x,y}_{\pi}\Big)$$

We can now relate this quantity to the success probability of $\mathscr{S}^{\text{ans}}$ in the answer-reduced game G^{ans}. Let θ denote the probability that one of the players receives a question $\widehat{x} = (g, p)$ of the form $g = (x, y)$ and $p = (i, j, k)$, and the other player receives a question $\widehat{y} = (g', p')$ of the form $g' = x$ and $p \in \{i, j, k\}$. In this situation, by the design of the decider (see Section 1.5.2), the verifier checks whether the player who got question $\widehat{x}$ responds with proof bits (π_i, π_j, π_k) that satisfy a corresponding clause in $\varphi_{x,y}$. Thus, since the overall success probability of the strategy $\mathscr{S}^{\text{ans}}$ in the game G^{ans} is at least $1 - \varepsilon$, it must be that conditioned on a player receiving question of the form $\widehat{x} = (x, y, i, j, k)$, their answer does not satisfies a corresponding clause in the formula $\varphi_{x,y}$ (if one exists) with probability at most ε/θ. In other words:

$$\mathop{\mathbf{E}}_{x,y,i,j,k} \sum_{\pi_i,\pi_j,\pi_k} \mathbf{1}[(\pi_i, \pi_j, \pi_k) \text{ unsat. } \varphi_{x,y}] \cdot \tau(N^{x,y,i,j,k}_{\pi_i,\pi_j,\pi_k}) \leq \varepsilon/\theta.$$

Multiplying both sides by L^3, we get that

$$\mathop{\mathbf{E}}_{x,y} \sum_{i,j,k} \sum_{\pi_i,\pi_j,\pi_k} \mathbf{1}[(\pi_i, \pi_j, \pi_k) \text{ unsat. } \varphi_{x,y}] \cdot \tau(N^{x,y,i,j,k}_{\pi_i,\pi_j,\pi_k}) \leq L^3\varepsilon/\theta\ .$$

Using Theorem 1.13 with Equation (1.5.5), we get that for every $i, j, k \in [L]$ and on average over x, y,

$$M^{x,y}_{[\pi\mapsto(\pi_i,\pi_j,\pi_k)|r,s,t]} \simeq_{\nu} N^{x,y,i,j,k}_{r,s,t}$$

for some proper error function $\nu = \nu(\varepsilon)$. Then using Theorem 1.15 we get that

$$\mathop{\mathbf{E}}_{x,y} \sum_{r,s,t} \left| \tau\left(M^{x,y}_{[\pi \mapsto (\pi_i, \pi_j, \pi_k) | r,s,t]} - N^{x,y,i,j,k}_{r,s,t} \right) \right| \leq 2\nu$$

for every $i, j, k \in [L]$. Putting everything together, we find that

$$\begin{aligned} & \mathop{\mathbf{E}}_{x,y} \sum_{i,j,k} \sum_{\pi} \mathbf{1}[(\pi_i, \pi_j, \pi_k) \text{ unsat. } \varphi_{x,y}] \cdot \tau\left(M^{x,y}_{\pi}\right) \\ & \leq \mathop{\mathbf{E}}_{x,y} \sum_{i,j,k} \sum_{\pi_i, \pi_j, \pi_k} \mathbf{1}[(\pi_i, \pi_j, \pi_k) \text{ unsat. } \varphi_{x,y}] \cdot \tau(N^{x,y,i,j,k}_{\pi_i,\pi_j,\pi_k}) + 2\nu \\ & \leq L^3 \left(\frac{\varepsilon}{\theta} + 2\nu \right) . \end{aligned}$$

Let $\zeta = L^3\left(\frac{\varepsilon}{\theta} + 2\nu\right) + 2\delta$. Then we deduce that

$$\omega(G, \mathscr{S}) \geq 1 - \zeta.$$

Since δ, ν are proper error functions of ε, so is ζ. Thus $\zeta \longrightarrow 0$ as $\varepsilon \longrightarrow 0$. Furthermore, the strategy $\mathscr{S}$ is finite-dimensional if and only if $\mathscr{S}^{\text{ans}}$ is finite-dimensional. Thus, suppose that $\omega^s_t(G^{\text{ans}}) = 1$ for $t = q$ (resp. for $t = co$). This implies that there is a sequence of finite-dimensional (resp. commuting operator) strategies $\mathscr{S}^{\text{ans}}$ such that $\omega(G^{\text{ans}}, \mathscr{S}^{\text{ans}})$ approaches 1. This in turn implies the existence of a sequence of finite-dimensional (resp. commuting operator) strategies $\mathscr{S}$ such that $\omega(G, \mathscr{S})$ approaches 1, and thus $\omega^s_t(G) = 1$. Taking the contrapositive, we conclude that

$$\omega^s_t(G) < 1 \Longrightarrow \omega^s_t(G^{\text{ans}}) < 1 .$$

This finishes the proof of the Proposition. □

1.5.5 Proof of Theorem 1.32

We now prove the main result of this section, Theorem 1.32. Fix $\beta \in \mathbb{N}$. The algorithm $\mathcal{A}AnswerReduction_\beta$, on input (D, C) where D is a 5-input Turing machine and C is a 3-input Turing machine, computes the descriptions of 5-input and 3-input Turing machines $D^{\text{ans}}, C^{\text{ans}}$ respectively as follows. Let $Q(n) = \log^\beta n$ and $T(n) = n^\beta$.

Question checker C^{ans}. At a high level, the Turing machine C^{ans}, on input $(n, \widehat{x}, \widehat{y})$ checks whether the question pair $(\widehat{x}, \widehat{y})$ is nontrivial according to Table 1.5, where "G" in the table is supposed to be the n-th game G_n of the sequence specified by the verifier $\mathscr{V} = (D, C)$, "$D_{x,y}$" in the table is supposed to be the Turing machine $D_{n,x,y}$ which on input (a, b) outputs $D(n, x, y, a, b)$, and "T" in the table is supposed to be $T(n)$.

In order to compute whether $(\widehat{x}, \widehat{y})$ (or $(\widehat{y}, \widehat{x})$) is one of the question pairs specified by Table 1.5, the Turing machine C^{ans} has to compute the question lengths of the n-th answer-reduced game G^{ans}: it computes L_n, the number of variables of a Cook-Levin formula corresponding to a Turing machine with description length $|D| + O(\log n) + 2Q(n)$. (This is the description length of a Turing machine $D_{n,x,y}$, which is D with (n, x, y) "hardwired" into it.) It then checks whether $\widehat{x}, \widehat{y}$ are (binary encodings of) elements of $(\{0,1\}^{Q(n)} \cup \{0,1\}^{2Q(n)}) \times ([L_n] \cup [L_n]^2 \cup [L_n]^3)$, which is the question alphabet of G_n^{ans}. It not, then it outputs 0. At this point, the Turing machine C^{ans} has ensured that $(\widehat{x}, \widehat{y})$ is a properly-formatted question pair in the n-th answer-reduced game G_n^{ans}.

The Turing machine C^{ans} then attempts to parse $(\widehat{x}, \widehat{y})$ or $(\widehat{y}, \widehat{x})$ as one of the combinations specified in Table 1.5 and outputs 1 if there is a match; otherwise it outputs 0. To determine whether $(x, y) \in (\{0,1\}^{Q(n)})^2$ is nontrivial for G_n, it computes whether $C(n, x, y) = 1$. This concludes the description of C^{ans}.

Decider D^{ans}. The Turing machine D^{ans} on input $(n, \widehat{x}, \widehat{y}, \widehat{a}, \widehat{b})$ first computes $C^{\text{ans}}(n, \widehat{x}, \widehat{y})$. If the output is 0 (i.e. the question pair $(\widehat{x}, \widehat{y})$ is trivial), then the Turing machine D^{ans} accepts (i.e. outputs 1). Otherwise, it continues. It computes L_n just like with C^{ans}, and then matches $(\widehat{x}, \widehat{y})$ (resp. $(\widehat{y}, \widehat{x})$) to one of the entries of the table. Since $C^{\text{ans}}(n, \widehat{x}, \widehat{y}) = 1$, there must be a match.

The Turing machine D^{ans} then evaluates whether the winning conditions $(\widehat{a}, \widehat{b})$ (resp. $(\widehat{b}, \widehat{a})$) are satisfied according to Table 1.5. If the winning conditions are satisfied, then D^{ans} outputs 1 (accepts), otherwise it outputs 0 (rejects).

Now assume the conditions of Theorem 1.32; i.e., that $\mathscr{V} = (D, C)$ is a verifier for a sequence of games $\mathscr{G}_{\mathscr{V}} = (G_n)_{n \in \mathbb{N}}$ and

1. The questions of G_n have length at most $Q(n)$,
2. $\mathsf{TIME}_C(n) \leq Q(n)$, and
3. $\mathsf{TIME}_D(n) \leq T(n)$.

Now we argue that the output $\mathscr{V}^{\text{ans}} = (D^{\text{ans}}, C^{\text{ans}})$ is a verifier for a sequence of games $\mathscr{G}_{\mathscr{V}^{\text{ans}}} = (G_n^{\text{ans}})_{n \in \mathbb{N}}$ satisfying the conclusions of Theorem 1.32.

Complexity of the question checker C^{ans}. The question checker C^{ans} for the answer-reduced game first has to compute L_n, the number of variables in the Cook-Levin formula corresponding to $D_{n,x,y}$. This requires computing the description length of $D_{n,x,y}$, where x, y are questions in the original game G_n, which by assumption has length at most $Q(n)$. It then has to check that the questions $(\widehat{x}, \widehat{y})$ are properly formatted questions from the question alphabet of G_n^{ans}, which takes time $\text{poly}(Q(n), \log L_n)$. Then, it has to determine whether $(\widehat{x}, \widehat{y})$ matches one of the question pairs in Table 1.5, which includes running the question checker C for the original verifier $\mathscr{V}$. Thus overall we have $\mathsf{TIME}_{C^{\text{ans}}}(n) \leq \text{poly}(|D|, |C|, Q(n), \log T(n), \log n) = \text{poly}(|D|, |C|, \beta, \log^{\beta} n)$.

Complexity of the decider D^{ans}. The time complexity of the answer-reduced verifier D^{ans} includes the complexity of computing the question checker $C^{\text{ans}}(n, x, y)$ and computing the number of variables L_n. It also includes the complexity of computing a clause of the Cook-Levin formula $\varphi_{n,x,y}$, which involves invoking the algorithm $\mathscr{A}CookLevin$ on the input $(D_{n,x,y}, T(n), 2T(n), i, j, k)$ for some variable indices $i, j, k \in [L_n]$, where (x, y) are questions for the original game G_n (which have length $Q(n)$ by assumption). Computing the description of $D_{n,x,y}$ takes time $\text{poly}(|D|, |x|, |y|, \log n)$

because it involves "hard-wiring" the integer n and strings x, y into the description of D. Thus it takes at most $\mathrm{poly}(|D|, Q(n), \log T(n), \log n)$ to compute a clause. Computing the $\eta(\cdot)$ and $\lambda(\cdot)$ maps also take time at most $\mathrm{poly}(\log T(n))$ (because it requires computing $T(n)$). Thus, in total, the complexity of the answer-reduced verifier is $\mathrm{poly}(|D|, |C|, Q(n), \log T(n), \log n) = \mathrm{poly}(|D|, |C|, \beta, \log^{\beta} n)$.

Completeness and Soundness. Completeness follows from Theorem 1.34. Soundness follows from Theorem 1.35.

This completes the proof of Theorem 1.32.

1.6 Compressions of nonlocal games and their applications

In this section we describe the compression theorems and some of their applications.

1.6.1 Gapless compression

First we present the main technical result of this paper, which is a gapless compression theorem for both the quantum and commuting operator value of nonlocal games. This theorem statement is a formalization of Theorem 1.3 from the introduction.

Theorem 1.38 (Gapless compression of nonlocal games)**.** *For all $\alpha \in \mathbb{N}$ there is a polynomial time algorithm $\mathcal{A}GaplessCompress_{\alpha}$ that takes as input a pair of Turing machines (D, C) and outputs a pair of Turing machines (D', C') such that the following holds. If $\mathscr{V} = (D, C)$ is a verifier for a sequence of games $\mathscr{G}_{\mathscr{V}} = (G_n)_{n\in\mathbb{N}}$ and $n_0 \in \mathbb{N}$ is an integer such that for all $n \geq n_0$,*

$$\max\left\{\mathsf{TIME}_C(n), \mathsf{TIME}_D(n)\right\} \leq n^{\alpha}\ , \tag{1.6.1}$$

then $\mathscr{V}' = (D', C')$ is a verifier for a sequence of games $\mathscr{G}_{\mathscr{V}'} = (G'_n)_{n\in\mathbb{N}}$ with the following properties. There exist an integer $\gamma = \mathrm{poly}(\alpha)$ and $n'_0 = \mathrm{poly}(\gamma^{\gamma}, n_0)$ such that for all $n \geq n'_0$,

1. *(Complexity bounds)*

$$\max\{\mathsf{TIME}_{C'}(n), \mathsf{TIME}_{D'}(n)\} \leq \log^{\gamma} n \ .$$

2. *(Completeness) For all oracularizable synchronous strategies $\mathscr{S}$ for G_n, there exists an oracularizable synchronous strategy $\mathscr{S}'$ for G'_n such that*

$$\omega(G'_n, \mathscr{S}') \geq \frac{1}{2} + \frac{1}{2}\omega(G_n, \mathscr{S}) \ .$$

Furthermore, if $\mathscr{S}$ is finite dimensional, so is $\mathscr{S}'$.

3. *(Soundness) For all $t \in \{q, co\}$ we have*

$$\omega^s_t(G_n) < 1 \Longrightarrow \omega^s_t(G'_n) < 1 \ .$$

4. *(Entanglement bound)*

$$\mathcal{E}(G'_n, 1) \geq \max\left\{\mathcal{E}(G_n, 1), 2^{2n}\right\} \ .$$

We prove this by combining the question reduction and answer reduction transformations of Sections 1.4 and 1.5. The algorithm $\mathcal{A}GaplessCompress_\alpha$ is presented below. The parameter β in Algorithm 5 is defined to be the same $\beta = \mathrm{poly}(\alpha)$ from Theorem 1.27.

```
Input: $D, C$.
Compute $(D^{\text{intro}}, C^{\text{intro}}) = \mathcal{A}QuestionReduction_\alpha(D, C)$.
Compute $(D', C') = \mathcal{A}AnswerReduction_\beta(D^{\text{intro}}, C^{\text{intro}})$.
Return $(D', C')$.
```

Pseudocode 5: $\mathcal{A}GaplessCompress_\alpha$

Proof. First, it is clear that $\mathcal{A}GaplessCompress_\alpha$ runs in polynomial time in the description length of the input (D, C), because the algorithm $\mathcal{A}QuestionReduction_\alpha$ runs in time $\mathrm{poly}(|D|, |C|)$

and the algorithm $\mathcal{A}AnswerReduction_\beta$ runs in time $\mathrm{poly}(|D^{\mathrm{intro}}|, |C^{\mathrm{intro}}|) = \mathrm{poly}(|D|, |C|)$. This last equality uses that $\max\{|D^{\mathrm{intro}}|, |C^{\mathrm{intro}}|\} \leq \mathrm{poly}(|D|, |C|)$ because the running time of $\mathcal{A}QuestionReduction_\alpha$ is an upper bound on the length of the descriptions of D^{intro} and C^{intro}.

Next, suppose that $\mathscr{V} = (D, C)$ is such that the time bound of (1.6.1) is satisfied. Then, the complexity bounds on $(D^{\mathrm{intro}}, C^{\mathrm{intro}})$ given by the conclusion of Theorem 1.27 are exactly those that satisfy the conditions of Theorem 1.32. Thus, the output (D', C') of $\mathcal{A}AnswerReduction_\beta(D^{\mathrm{intro}}, C^{\mathrm{intro}})$ satisfy the conclusions of Theorem 1.32 (with $\gamma = \mathrm{poly}(\beta) = \mathrm{poly}(\alpha)$) and thus this establishes the desired complexity bounds on the output verifier $\mathscr{V}'$.

Define the integers $\beta = \mathrm{poly}(\alpha)$,$n_0^{\mathrm{intro}} = \mathrm{poly}(\beta, n_0)$ as given by Theorem 1.27. Then, define the integers $\gamma = \mathrm{poly}(\beta)$, $n_0^{\mathrm{ans}} = \mathrm{poly}(\gamma^\gamma, n_0^{\mathrm{intro}}) = \mathrm{poly}(\gamma^\gamma, n_0)$ as given by Theorem 1.32. Define $n_0' = \max\{n_0, n_0^{\mathrm{intro}}, n_0^{\mathrm{ans}}\}$.

We now establish the completeness property of $\mathscr{V}'$. Fix an integer n not less than n_0'. Let $\mathscr{S}$ be an oracularizable synchronous strategy for G_n. By the completeness of Question Reduction, this implies there is an oracularizable synchronous strategy $\mathscr{S}^{intro}$ for G_n^{intro} such that

$$\omega(G_n^{\mathrm{intro}}, \mathscr{S}^{intro}) \geq \omega(G_n, \mathscr{S}) .$$

Then, by the completeness of Answer Reduction, there is an oracularizable synchronous strategy $\mathscr{S}'$ for G_n' such that

$$\omega(G_n', \mathscr{S}') \geq \frac{1}{2} + \frac{1}{2}\omega(G_n^{\mathrm{intro}}, \mathscr{S}^{intro}) \geq \frac{1}{2} + \frac{1}{2}\omega(G_n, \mathscr{S}) .$$

Furthermore, if $\mathscr{S}$ is finite-dimensional, then so are $\mathscr{S}^{\mathrm{intro}}$ and $\mathscr{S}'$.

We establish the soundness property of $\mathscr{V}'$ by combining the soundness guarantees of Question Reduction and Answer Reduction:

$$\omega_t^s(G_n) < 1 \Longrightarrow \omega_t^s(G_n^{\mathrm{intro}}) < 1 \Longrightarrow \omega_t^s(G_n') < 1.$$

Finally, we establish the entanglement bound property by combining the entanglement bounds from Question Reduction and Answer Reduction

$$\mathcal{E}(G'_n, 1) \geq \mathcal{E}(G_n^{intro}, 1) \geq \max\left\{\mathcal{E}(G_n, 1), 2^{2n}\right\} \; .$$

□

1.6.2 Super compression

The gapless compression procedure of Theorem 1.38 transforms uniform sequences of games $(G_1, G_2, \ldots)$ to another uniform sequence $(G'_1, G'_2, \ldots)$ that is, in a sense, exponentially more efficient. Using this we prove a *super compression* procedure, which transforms a sequence of games $(G_1, G_2, \ldots)$ into a *single* game G' such that $\omega_t^s(G') = 1$ if and only if $\omega_t^s(G_n) = 1$ for all sufficiently large n and $t \in \{q, co\}$.

Theorem 1.39 (Super compression of nonlocal games)**.** *For all $\alpha \in \mathbb{N}$ there is a polynomial time algorithm $\mathcal{A}SuperCompress_\alpha$ that takes as input a pair of Turing machines (D, C) and outputs a pair of Turing machines $(D^{\text{super}}, C^{\text{super}})$ such that the following holds. If $\mathscr{V} = (D, C)$ is a verifier for a sequence of games $\mathscr{G}_{\mathscr{V}} = (G_n)_{n\in\mathbb{N}}$ and $n_0 \in \mathbb{N}$ is an integer such that for all $n \geq n_0$,*

$$\max\left\{\mathsf{TIME}_C(n), \mathsf{TIME}_D(n)\right\} \leq n^\alpha \; , \tag{1.6.2}$$

then $\mathscr{V}^{\text{super}} = (D^{\text{super}}, C^{\text{super}})$ is a verifier for a sequence of games $\mathscr{G}_{\mathscr{V}^{\text{super}}} = (G_n^{\text{super}})_{n\in\mathbb{N}}$ such that there exist integers $\lambda = O(\alpha)$ and $\kappa = \text{poly}(|D|, |C|, \alpha, n_0, \lambda^{\text{poly}(\lambda)})$ and the κ-th game in the sequence, G_κ^{super}, satisfies the following properties:

1. *(Complexity bounds)*

$$\max\left\{\mathsf{TIME}_{C^{\text{super}}}(\kappa), \mathsf{TIME}_{D^{\text{super}}}(\kappa)\right\} \leq \kappa^\lambda \; .$$

2. *(Completeness for $t = q$) If for all $n \geq \kappa$ we have*

$$\sup_{\textit{finite-dim osync } \mathscr{S}_n} \omega(G_n, \mathscr{S}_n) = 1$$

   where the supremum is over finite-dimensional oracularizable synchronous strategies $\mathscr{S}_n$, then $\omega_q^s(G_\kappa^{\text{super}}) = 1$.

3. *(Completeness for $t = co$) If for all $n \geq \kappa$, there exists an oracularizable synchronous strategy $\mathscr{S}_n$ for G_n such that $\omega(G_n, \mathscr{S}_n) = 1$, then $\omega_{co}^s(G_\kappa^{\text{super}}) = 1$.*

4. *(Soundness) For all $t \in \{q, co\}$, if there exists an $n \geq \kappa$ such that $\omega_t^s(G_n) < 1$, then $\omega_t^s(G_\kappa^{\text{super}}) < 1$.*

5. *(Entanglement lower bound) There is no finite-dimensional strategy $\mathscr{S}_\kappa^{\text{super}}$ such that $\omega(G_\kappa^{\text{super}}, \mathscr{S}_\kappa^{\text{super}}) = 1$.*

Note that, unlike Theorem 1.38, the conclusions of Theorem 1.39 pertain to a *single* game in the output sequence $\mathscr{G}_{\mathscr{V}^{\text{super}}} = (G_n^{\text{super}})_n$ of games, namely, G_κ^{super}.

At a high level, the games $(G_n^{\text{super}})_n$ has the following structure: with probability $\frac{1}{2}$, the verifier in the game G_n^{super} plays the game G_n. With the remaining probability the verifier plays the game G'_{n+1} where $(G'_n)_n$ is the compression of $(G_n^{\text{super}})_n$ using $\mathscr{A}GaplessCompress$ from Theorem 1.38. Note the self-referentiality! We now proceed with the proof.

Proof. Let (D, C) be a pair of Turing machines and let α be such that eq. (1.6.1) is satisfied. We first define, for every integer $\lambda \in \mathbb{N}$, a pair of Turing machines $(D_\lambda^{\text{super}}, C_\lambda^{\text{super}})$ whose descriptions are given below in Algorithms **??**. We will then identify a special λ^* and define the algorithm $\mathscr{A}SuperCompress_\alpha$ to output the descriptions of $(D_{\lambda^*}^{\text{super}}, C_{\lambda^*}^{\text{super}})$.

Note that the descriptions of $D_\lambda^{\text{super}}, C_\lambda^{\text{super}}$ are self-referential: they perform computations on *their own descriptions*. It is possible to define Turing machines in this manner; one can appeal to either Kleene's Recursion Theorem/Roger's Fixed Point Theorem to argue that these descriptions are well-defined (see, e.g. [49, Chapter 14] for a modern explanation). The description lengths of these Turing machines satisfy

$$\max\{|D_\lambda^{\text{super}}|, |C_\lambda^{\text{super}}|\} \leq \text{poly}(\lambda, |D|, |C|) \ .$$

```
**Input**: $n, x, y, a, b$
If the following takes more than $n^\lambda$ steps, then automatically reject.
Parse $x = (t_x, \widehat{x})$ and $y = (t_y, \widehat{y})$, where $t_x, t_y \in \{0, 1\}$.
**if** $t_x = t_y = 0$ **then**
    If $D(n, \widehat{x}, \widehat{y}, a, b)$ accepts, then accept. Otherwise, reject.
**end**
**else if** $t_x = t_y = 1$ **then**
    Compute $(D', C') = \mathcal{A}GaplessCompress_\lambda(D_\lambda^{\text{super}}, C_\lambda^{\text{super}})$.
    If $D'(n + 1, \widehat{x}, \widehat{y}, a, b)$ accepts, then accept. Otherwise, reject.
**end**
On all other inputs, accept.
```

Pseudocode 6: Specification of Turing machine D_λ^{super}.

```
**Input**: $n, x, y$
If the following takes more than $n^\lambda$ steps, then automatically reject.
Parse $x = (t_x, \widehat{x})$ and $y = (t_y, \widehat{y})$, where $t_x, t_y \in \{0, 1\}$.
**if** $t_x = t_y = 0$ **then**
    Output $C(n, \widehat{x}, \widehat{y})$.
**end**
**else if** $t_x = t_y = 1$ **then**
    Compute $(D', C') = \mathcal{A}GaplessCompress_\lambda(D_\lambda^{\text{super}}, C_\lambda^{\text{super}})$.
    Output $C'(n + 1, \widehat{x}, \widehat{y})$.
**end**
On all other inputs, output 1.
```

Pseudocode 7: Specification of Turing machine C_λ^{super}.

First, observe that by construction both D_λ^{super} and C_λ^{super}, when given index n, run in time at most n^λ. Thus, $(D_\lambda^{\text{super}}, C_\lambda^{\text{super}})$ satisfy the complexity conditions of Theorem 1.38 for the algorithm $\mathcal{A}GaplessCompress_\lambda$, and thus the output Turing machines (D', C') satisfy the complexity bounds in the conclusion of $\mathcal{A}GaplessCompress_\lambda$, namely, that there exists $\gamma = \text{poly}(\lambda)$ such that for all $n \in \mathbb{N}$,

$$\max\{\mathsf{TIME}_{D'}(n), \mathsf{TIME}_{C'}(n)\} \le \log^\gamma n\ .$$

The next claim shows that we can find an integer λ^* such that for sufficiently large n, the Turing machines $D_{\lambda^*}^{\text{super}}, C_{\lambda^*}^{\text{super}}$ never encounter the time-out.

Claim 1. *There exist integers $\lambda^* = O(\alpha), \kappa = \text{poly}(|D|, |C|, \alpha, n_0, \lambda^{\text{poly}(\lambda)})$ such that for all $n \ge \kappa$, the Turing machines $D_{\lambda^*}^{\text{super}}, C_{\lambda^*}^{\text{super}}$ when given index n never reject due to exceeding the n^{λ^*} time-out.*

Proof. Next, the time complexity of D_λ^{super} (resp. C_λ^{super}) *without* the automatic n^λ timeout is polynomial in the complexity of running the decider D/checker C, computing $\mathcal{A}GaplessCompress_\lambda$, and running the decider D' (resp. checker C'). By our assumptions on (D, C), when $n \geq n_0$ we have the bounds from eq. (1.6.1). The algorithm $\mathcal{A}GaplessCompress_\lambda$ runs in time $\mathrm{poly}(|D_\lambda^{\mathrm{super}}|, |C_\lambda^{\mathrm{super}}|, \lambda) = \mathrm{poly}(|D|, |C|, \lambda)$. Putting this together with the complexity bounds on D' (resp. C'), we have that the complexity of $D_\lambda^{\mathrm{super}}$ (resp. $C_\lambda^{\mathrm{super}}$), without the automatic timeout, is at most

$$\sigma(n^\alpha \cdot |D| \cdot |C| \cdot \lambda \cdot \log^\gamma n)^\sigma \tag{1.6.3}$$

for all $n \geq n_0$, where $\sigma \in \mathbb{N}$ is some universal constant.

We can find integers $\lambda^*, \kappa \in \mathbb{N}$ such that each component of the expression in (1.6.3) is at most n^{λ^*} for all $n \geq \kappa$. Namely:

- By taking $\lambda^* \geq \sigma \cdot \alpha$ and $\kappa \geq \sigma$, we have that $\sigma n^{\alpha \cdot \sigma} \leq n^{\lambda^*}$ for all $n \geq \kappa$.
- By taking $\lambda^* \geq \sigma$ and $\kappa \geq |D| \cdot |C| \cdot \lambda^*$, we have that $(|D| \cdot |C| \cdot \lambda^*)^\sigma \leq n^{\lambda^*}$ for all $n \geq \kappa$.
- By taking $\lambda^* \geq 2$ and $\kappa \geq (\gamma \cdot \sigma)^{\gamma \cdot \sigma}$ where $\gamma = \mathrm{poly}(\lambda^*)$, we have that $\log^{\gamma \cdot \sigma}(n) \leq n^{\lambda^*}$ for all $n \geq \kappa$.

Putting everything together, by setting $\lambda^* = 2\sigma\alpha$ and $\kappa = \sigma \cdot \alpha \cdot |D| \cdot |C| \cdot \lambda^* \cdot (\gamma \cdot \sigma)^{\gamma \cdot \sigma} \cdot n_0$, we get that the Turing machines $D_{\lambda^*}^{\mathrm{super}}$ and $C_{\lambda^*}^{\mathrm{super}}$ run in time that is less than n^{λ^*} for all $n \geq \kappa$.

□

We define the algorithm $\mathcal{A}SuperCompress_\alpha$, on input (D, C), to compute $\lambda^* = O(\alpha)$ and output the descriptions of $(D_{\lambda^*}^{\mathrm{super}}, C_{\lambda^*}^{\mathrm{super}})$. The algorithm clearly runs in polynomial time.

By construction the Turing machines $(D_{\lambda^*}^{\mathrm{super}}, C_{\lambda^*}^{\mathrm{super}})$ satisfy the desired time complexity bound on index $n = \kappa$. What remains is to argue completeness and soundness. For notational simplicity we fix λ^* and let $(D^{\mathrm{super}}, C^{\mathrm{super}}) = (D_{\lambda^*}^{\mathrm{super}}, C_{\lambda^*}^{\mathrm{super}})$.

Fix $t \in \{q, co\}$. Since the Turing machines $D^{\mathrm{super}}, C^{\mathrm{super}}$ never reject due to the time-out, we have that the verifier in the game G_n^{super} automatically accepts with probability $\frac{1}{2}$ (when $t_x \neq t_y$), plays the game G_n with probability $\frac{1}{4}$ (when $t_x = t_y = 0$), and plays the game G'_{n+1} with probability

$\frac{1}{4}$ (when $t_x = t_y = 1$) where G'_{n+1} is the $(n+1)$-st game in the sequence of games output by $\mathcal{A}GaplessCompress$ on input $(D^{\text{super}}, C^{\text{super}})$.

We first prove completeness for $t = q$. Suppose for all $n \geq \kappa$ we have

$$\sup_{\text{finite-dim osync } \mathscr{S}_n} \omega(G_n, \mathscr{S}_n) = 1. \tag{1.6.4}$$

Define

$$c_n = \sup_{\text{finite-dim osync } \mathscr{S}_n^{\text{super}}} \omega(G_n^{\text{super}}, \mathscr{S}_n^{\text{super}})$$

and define $c = \inf_{n \geq \kappa} c_n$. We aim to prove that $c = 1$; this would imply that $\omega_q^s(G_n^{\text{super}}) = 1$ for all $n \geq \kappa$. Suppose this were not true, so that $0 \leq c < 1$. We now show that $c_n \geq \frac{7+c}{8} > c$ for all $n \geq \kappa$, which would contradict the fact that c is the infimum of the sequence $(c_n)_{n \geq \kappa}$.

For all $m \geq \kappa$, let: (a) $\mathscr{S}_m$ be a finite-dimensional oracularizable synchronous ("finite-dim osync") strategy for G_m, (b) let $\mathscr{S}_m^{\text{super}}$ denote a finite-dim osync strategy for G_m^{super} whose value is at least c, and (c) let $\mathscr{S}'_m$ denote the finite-dim osync strategy for G'_m, given by the completeness property of Theorem 1.38, whose value satisfies

$$\omega(G'_m, \mathscr{S}'_m) \geq \frac{1}{2} + \frac{1}{2}\omega(G_m^{\text{super}}, \mathscr{S}_m^{\text{super}}) \geq \frac{1+c}{2}\ . \tag{1.6.5}$$

We now construct, for all $n \geq \kappa$, a finite-dim osync strategy $\mathscr{T}_n$ for G_n^{super} that has value at least

$$\omega(G_n^{\text{super}}, \mathscr{T}_n) \geq \frac{1}{2} + \frac{1}{4}\omega(G_n, \mathscr{S}_n) + \frac{1}{4}\omega(G'_{n+1}, \mathscr{S}'_{n+1}) \geq \frac{5+c}{8} + \frac{1}{4}\omega(G_n, \mathscr{S}_n) \tag{1.6.6}$$

where the second inequality follows from eq. (1.6.5). The strategy $\mathscr{T}_n$ is constructed as follows. Its tracial state is the tensor product of the tracial states from $\mathscr{S}_n$ and $\mathscr{S}'_{n+1}$; since both of these strategies are finite-dimensional so is the strategy $\mathscr{T}_n$. When a player gets question $x = (0, \widehat{x})$, they perform the measurement corresponding to question $\widehat{x}$ from the strategy $\mathscr{S}_n$. When a player gets question $x = (1, \widehat{x})$, they perform the measurement corresponding to question $\widehat{x}$ from the strategy $\mathscr{S}'_n$. Thus when both players get questions whose first bit is 0, they are essentially playing the game

G_n, and when they both get questions whose first bit is 1, they are essentially playing the game G'_{n+1}. Taking the supremum of the right-hand side of eq. (1.6.6) over finite-dim osync strategies $\mathscr{S}_n$ for G_n and using eq. (1.6.4), we get that $c_n \geq \frac{7+c}{8}$, which yields a contradiction as desired.

The proof of completeness for $t = co$ is virutally identical, except we consider all oracularizable synchronous strategies, not just finite-dimensional ones.

We now prove the soundness property. Let $t \in \{q, co\}$. Let $n^* \geq \kappa$ be such that $\omega_t^s(G_{n^*}) < 1$. For all $m \geq \kappa$, by construction of the game G_m^{super} we have

$$\omega_t^s(G_m^{\text{super}}) = \frac{1}{2} + \frac{1}{4}\omega_t^s(G_m) + \frac{1}{4}\omega_t^s(G'_{m+1}) \ ,$$

so therefore $\omega_t^s(G_{n^*}^{\text{super}}) < 1$. By the soundness property of Theorem 1.38, this means that $\omega_t^s(G'_{n^*}) < 1$, and therefore $\omega_t^s(G_{n^*-1}^{\text{super}}) < 1$. This in turn implies that $\omega_t^s(G_{n^*-2}^{\text{super}}) < 1$, and so on, until we obtain $\omega_t^s(G_\kappa^{\text{super}}) < 1$, the desired conclusion.

Finally, we prove that there is no finite-dimensional perfect strategy for G_κ^{super}. Suppose for contradiction that there a d-dimensional strategy $\mathscr{S}_\kappa^{\text{super}}$ such that $\omega(G_\kappa^{\text{super}}, \mathscr{S}_\kappa^{\text{super}}) = 1$. Then in particular it must give rise to a d-dimensional strategy $\mathscr{S}'_{\kappa+1}$ such that $\omega(G'_{\kappa+1}, \mathscr{S}'_{\kappa+1}) = 1$ (simply by taking the measurement operators corresponding to questions $x = (1, \widehat{x})$). By the entanglement bound of Theorem 1.38, it must be that the dimension d is at least $\mathcal{E}(G_{\kappa+1}^{\text{super}}, 1)$. If this quantity is infinite, then we arrive at a contradiction and are done. Otherwise, there is a d-dimensional perfect strategy $\mathscr{S}_{\kappa+1}^{\text{super}}$ for $G_{\kappa+1}^{\text{super}}$. Again, this must imply a d-dimensional perfect strategy for $G'_{\kappa+2}$. Continuing in this fashion, we either obtain a contradiction or deduce the existence of a d-dimensional perfect strategy for G'_m for all $m \geq \kappa$. On the other hand, the entanglement bound of Theorem 1.38 also implies that $\mathcal{E}(G'_m, 1) \geq 2^{2m}$. Thus, $d \geq 2^{2m}$ for all $m \geq \kappa$, contradicting the assumption that d is finite. □

1.6.3 Π_1-completeness of the exact co-value problem

As a warmup, we present an application of the super compression procedure to show that the exact co-value problem (i.e. determining whether $\omega_{co}(G) = 1$) is complete for Π_1, also known as coRE. This was first shown by Slofstra [8] using very different techniques based on group theory.

Theorem 1.40. *The exact co-value problem is complete for* Π_1.

Proof. The easy direction is that the exact co-value problem is contained in Π_1 because one can express it as a Π_1 sentence: for all nonlocal games G, $\omega_{co}(G) = 1$ if and only if $\forall x\, \phi(x)$ where $\phi(x)$ is a computable predicate that is true when the x-th level of the semidefinite programming hierarchy of [14, 15] computes an upper bound of 1 on $\omega_{co}(G)$. In other words, the best upper bound on the commuting operator value of G computed by the x-th level of the hierarchy is 1. If this is true for all x, then this implies that $\omega_{co}(G) = 1$. On the other hand, if $\omega_{co}(G) < 1$, then there exists a level x such that $\phi(x)$ is false.

Now we turn to the other direction. To prove Π_1-hardness, we reduce an arbitrary Π_1 sentence $S = \forall x\, \phi(x)$ to a nonlocal game G such that S is true if and only if $\omega_{co}(G) = 1$.

Define the Turing machine T_ϕ that halts on the empty input if and only if the sentence S is false:

```
for $x \in \{0,1\}^*$ do
    If $\phi(x)$ is false then halt.
end
```

Pseudocode 8: Specification of T_ϕ.

Next, define the sequence of games $\mathscr{G}_\phi = (G_n)_{n\in\mathbb{N}}$ with verifier $\mathscr{V} = (D, C)$, where $C(x, y) = 1$ if and only if $x = y$, and where the decider D is defined as follows:

```
**Input**: $n, x, y, a, b$
If $T_\phi$ halts in $n$ steps, reject.
If any of $x, y, a, b$ exceed $n$ bits, reject.
If $x = y$ but $a \neq b$, reject.
Otherwise, accept.
```

Pseudocode 9: Specification of Turing machine D.

Notice that $\max\{\mathsf{TIME}_D(n), \mathsf{TIME}_c(n)\} \leq O(n)$, which is at most n^2 for sufficiently large n. Furthermore, $\omega_{co}(G_n) = 1$ if and only if the Turing machine T_ϕ does not halt in n steps. Furthermore, if T_ϕ does not halt in n steps, then there exists an oracularizable synchronous ("osync") strategy $\mathscr{S}_n$ such that $\omega(G_n, \mathscr{S}_n) = 1$: the strategy is to output a fixed answer no matter what the question is.

We apply super compression to the family of games $\mathscr{G}_\phi$: the output of $\mathscr{A}SuperCompress_\alpha(D, C)$ where $\alpha = 2$ is a verifier $(D^{\text{super}}, C^{\text{super}})$ for a sequence of games $\mathscr{G}^{\text{super}} = (G_n^{\text{super}})_{n\in\mathbb{N}}$ such that $\omega_{co}^s(G_\kappa^{\text{super}}) = 1$ if and only if there exists an osync value-1 strategy $\mathscr{S}_n$ for G_n, where κ is defined as in Theorem 1.39.

Thus if S is true, then T_ϕ never halts, and there exists an osync strategy $\mathscr{S}_n$ such that $\omega(G_n, \mathscr{S}_n) = 1$ for all $n \in \mathbb{N}$, and thus $\omega_{co}^s(G_\kappa^{\text{super}}) = 1$. On the other hand, if S is false and T_ϕ does halt in some time t, then $\omega_{co}^s(G_n) < 1$ for all $n \geq t$, which implies that $\omega_{co}^s(G_\kappa^{\text{super}}) < 1$.

By [34], since G_κ^{super} is a synchronous game, we have that $\omega_{co}^s(G_\kappa^{\text{super}}) = 1$ if and only if $\omega_{co}(G_\kappa^{\text{super}}) = 1$. This, combined with the fact that the mapping from the Π_1 sentence S to the game G_κ^{super} is computable, implies that the exact co-value problem is Π_1-hard.

□

Note that the exact same proof, considering q-type strategies rather than co-type strategies, shows that the exact q-value problem is hard for Π_1. While we improve this lower bound to Π_2 in the next section, we note that this directly implies that the set of quantum correlations is not closed, a result that was also established by Slofstra in [5].[13] Again, the proof approaches are quite different: his proof uses techniques from approximate representation theory as well as group theory.

Corollary 1.41 ([5]). *The set of quantum correlations is not closed.*

Proof. Let S be a true Π_1 sentence. The construction of the game G_κ^{super} from S in Theorem 1.40, by Theorem 1.39, has the property that $\omega_q(G_\kappa^{\text{super}}) = 1$ but there is no finite-dimensional strategy $\mathscr{S}$ that actually achieves value 1 in the game.

□

1.6.4 Π_2-completeness of the exact q-value problem

We now prove the main result of this paper, which is the Π_2-completeness of the exact q-value problem. As explained in Section 1.1.1, we combine our gapless compression theorem with a consequence of the $\mathsf{MIP}^* = \mathsf{RE}$ theorem from [4], which we state in the following theorem. In the theorem, nonlocal games G are represented via an integer $n \in \mathbb{N}$, and a pair of Turing machines (D, C) where D represents the decider for G (so is a 4-input Turing machine) and C represents the checker (so is a 2-input Turing machine). The game G is then defined to be $(\mathcal{X}, \mathcal{A}, D)$ where $\mathcal{X} = \mathcal{A} = \{0,1\}^n$. The checker C, on input $(x, y) \in \mathcal{X} \times \mathcal{X}$, indicates whether (x, y) is trivial for G.

Theorem 1.42 ([4]). *There is a universal constant $\lambda_{\texttt{Halt}} \in \mathbb{N}$ and algorithm $\mathcal{A}HaltingGame$ that takes as input the description of a Σ_1 sentence S and outputs a tuple (D, C) for a nonlocal game G such that*

1. *(Completeness) If S is true, then*

$$\sup_{\text{finite-dim osync } \mathscr{S}} \omega(G, \mathscr{S}) = 1.$$

[13] Briefly, the set of quantum correlations on n inputs and k outputs, denoted by $C_q(n, k)$, is the (convex) set of all vectors $p_{xyab} \in \mathbb{R}^{n \times n \times k \times k}$ such that

$$p_{xyab} = \langle \psi | A_a^x \otimes B_b^y | \psi \rangle$$

for some dimension d, some quantum state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$, and some POVMs $\{A_a^x\}, \{B_b^y\}$.

2. *(Soundness) If S is false, then*
$$\omega_q^s(G) < 1.$$

3. *(Complexity bounds) Letting $|S|$ denote the description length of the sentence S, we have*
$$\max\left\{\mathsf{TIME}_C, \mathsf{TIME}_D, \mathsf{TIME}_{\mathcal{A}HaltingGame(S)}\right\} \leq O(|S|^{\lambda_{\mathtt{Halt}}})$$
where $\mathsf{TIME}_C, \mathsf{TIME}_D$ denote the time complexities of C, D (on any input), and $\mathsf{TIME}_{\mathcal{A}HaltingGame(S)}$ denotes the time complexity of $\mathcal{A}HaltingGame$ on input S.

Proof. This is a corollary of [4, Theorem 12.7] which reduces the Halting problem to deciding whether the q-value of a nonlocal game is equal to 1 or at most $1/2$. To obtain the present theorem, we first observe that every Σ_1 sentence $S = \exists x\, \phi(x)$ can be expressed as an equivalent instance of the Halting problem: define the Turing machine M_S that on the empty input, starts looping over all x and evaluates $\phi(x)$. If it finds an x such that $\phi(x)$ is true, then it halts. Clearly S is true if and only if M_S halts.

The game H corresponding to M_S from [4, Theorem 12.7] is synchronous and the decider complexity is at most some polynomial in the description length of S. However, the question distribution μ of the game H is not uniform. Without loss of generality, assume that the question and answer sets of H are represented by n-bit strings. Because the reduction from M_S to H is efficient, we have that $n = \text{poly}(|S|)$.

The game G that we construct will be H but with a uniform distribution over all n-bit question pairs (x, y). Whenever a sampled question pair (x, y) is not in the support of μ, the decider D of G will automatically accept (and thus (x, y) is a trivial question). Otherwise, the decider from the game H is invoked. The key thing to note is that $\omega_q(H) = 1$ if and only if $\omega_q(G) = 1$. Furthermore, since G is a synchronous game (since H is a synchronous game), it holds that $\omega_q^s(G) = 1$ if and only if $\omega_q(G) = 1$.

Finally, since determining the support of the question distribution of H can be done in $\text{poly}(|S|)$ time, we obtain a checker C for the game G that runs in $\text{poly}(|S|)$ time. Thus, on input S, the algorithm $\mathscr{A}HaltingGame$ can output the tuple (D, C) which satisfies the conclusions of the theorem. □

We break up the proof of the Π_2 completeness of the exact q-value problem into two parts. First we show hardness.

Lemma 1.43. *The exact q-value problem is hard for Π_2.*

Proof. Fix a Π_2 sentence $S = \forall x \exists y \, \phi(x, y)$ where ϕ is a computable predicate. For every $n \in \mathbb{N}$ define the Σ_1 sentence

$$S_n = \exists y_1, \ldots, y_n \bigwedge_{i=1}^{n} \phi(i, y_i).$$

Thus the sentence S is true if and only if the sentences S_n are true for all $n \in \mathbb{N}$. Note that if S_n is true then S_i is true for all $i \leq n$.

Using $\mathscr{A}HaltingGame$ we construct the sequence of games $\mathscr{G}_\phi = (G_n)_{n \in \mathbb{N}}$ with verifier $\mathscr{V} = (D, C)$. Let

$$c_n = \sup_{\text{finite-dim osync } \mathscr{S}_n} \omega(G_n, \mathscr{S}_n),$$

then these games have the property that $c_n = 1$ if and only if the sentence S_n is true.

```
Input: $n, x, y, a, b$
Compute the game decider and checker $(D_n, C_n)$ for $\mathscr{A}HaltingGame(S_n)$.
If $D_n(x, y, a, b)$ accepts, then accept.
Otherwise, reject.
```

Pseudocode 10: Specification of Turing machine D.

```
Input: $n, x, y$
Compute the game decider and checker $(D_n, C_n)$ for $\mathscr{A}HaltingGame(S_n)$.
Output $C_n(x, y)$.
```

Pseudocode 11: Specification of Turing machine C.

For large enough n the verifier is bounded by

$$\max\left\{\mathsf{TIME}_C(n), \mathsf{TIME}_D(n)\right\} \leq n^{\lambda_{\texttt{Halt}}+1}$$

since

$$\max\left\{\mathsf{TIME}_{C_n}, \mathsf{TIME}_{D_n}, \mathsf{TIME}_{\mathcal{A}HaltingGame(S_n)}\right\} \leq (n|S|)^{\lambda_{\texttt{Halt}}}.$$

We apply super compression to the family of games $\mathscr{G}_\phi$: the output of $\mathcal{A}SuperCompress_\alpha(D, C)$ where $\alpha = \lambda_{\texttt{Halt}} + 1$ is a verifier $(D^{\text{super}}, C^{\text{super}})$ for a sequence of games $\mathscr{G}^{\text{super}} = (G_n^{\text{super}})_{n\in\mathbb{N}}$ such that $\omega_q^s(G_\kappa^{\text{super}}) = 1$ if and only if $c_n = 1$ for all $n \geq \kappa$, where κ is defined as in Theorem 1.39.

Therefore, $\omega_q^s(G_\kappa^{\text{super}}) = 1$ if and only if the sentences S_n are true for $n \geq \kappa$, which is equivalent to the Π_2 sentence S being true. We have therefore reduced the problem of deciding an arbitrary Π_2 sentence to deciding the exact q-value problem. □

Finally, we argue that the exact q-value problem is contained in Π_2.

Lemma 1.44. *The exact q-value problem is in* Π_2.

Proof. We will state the exact q-value problem as a Π_2 sentence. Fix a nonlocal game G then we would like to decide if

$$\sup_{\text{finite-dim } \mathscr{S}} \omega(G, \mathscr{S}) = 1.$$

Let $\mathcal{S}_\varepsilon^d$ be an ε-net for quantum strategies of dimension $d \in \mathbb{N}$. This is a finite set, since strategies of a fixed dimension form a compact set [50]. Let $\mathcal{S}_\varepsilon = \bigcup_{d\in\mathbb{N}} \mathcal{S}_\varepsilon^d$. Then we can equivalently formulate the decision problem as

$$\forall\varepsilon \in (0, 1]\ \exists\mathscr{S} \in \mathcal{S}_\varepsilon \text{ such that } \omega(G, \mathscr{S}) > 1 - 2\varepsilon.$$

This in turn is equivalent to the Π_2 sentence

$$\forall n \in \mathbb{N}\ \exists \mathscr{S} \in \mathcal{S}_{\frac{1}{n}} \text{ such that } \omega(G, \mathscr{S}) > 1 - \frac{2}{n}.$$

□

Putting the two together, we get:

Theorem 1.45. *The exact q-value problem is complete for* Π_2.

1.6.5 Necessity of compression

We will show how to compress nonlocal games given many-one reductions from arithmetical hierarchy classes to the corresponding t-value problems for $t \in \{q, co\}$. This shows that, in a certain sense, compression theorems are *necessary* for proving the complexity lower bounds indicated in Figure 1.1. In particular we construct *super compression* procedures (procedures that map families of games to a single equivalent game).

The following theorem was proved in [26]:

Theorem 1.46. *Assume that the approximate q-value problem is Σ_1-hard. Then there exists a computable map $\mathscr{A}GapCompress_q$ that takes in as input a description of a sequence of games $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$ and outputs the description of a single game G' such that*

1. $\omega_q(G') = 1$ *if* $\omega_q(G_n) = 1$ *for some game* $G_n \in \mathscr{G}$.

2. $\omega_q(G') < \frac{1}{2}$ *if* $\omega_q(G_n) < \frac{1}{2}$ *for every game* $G_n \in \mathscr{G}$.

Now we show that if the approximate co-value problem is Π_1-hard, then there exists a gap-preserving compression procedure for the commuting operator value of games.

Theorem 1.47. *Assume that the approximate co-value problem is Π_1-hard. Then there exists a computable map $\mathscr{A}GapCompress_{co}$ that takes in as input a description of a sequence of games $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$ and outputs the description of a single game G' such that*

1. *$\omega_{co}(G') = 1$ if $\omega_{co}(G_n) = 1$ for every game $G_n \in \mathscr{G}$,*

2. *$\omega_{co}(G') < \frac{1}{2}$, otherwise.*

Proof. Consider the following Turing machine $T^{co}_{\mathscr{G}}$: it interleaves running some number of levels of the NPA semidefinite programming hierarchy [14] on each game G_m in the sequence, trying to find a game m for which $\omega_{co}(G_m) < 1$. The completeness of the NPA hierarchy implies that if $\omega_{co}(G_m) < 1$ for some m, then eventually a certificate will be found. Thus the Turing machine halts only if there exists m such that $\omega_{co}(G_m) < 1$.

```
for $n \in \mathbb{N}$ do
    for $m \in \{1, ..., n\}$ do
        Run the first $n$ levels of the NPA hierarchy for the game $G_m \in \mathscr{G}$.
        If there is a certificate that $\omega_{co}(G_m) < 1$ then halt.
    end
end
```

Pseudocode 12: Specification of $T^{co}_{\mathscr{G}}$

Consider the sentence S defined as "$\forall n \in \mathbb{N}$, $T^{co}_{\mathscr{G}}$ does not halt in n steps". Note that S is a Π_1 sentence, and since the approximate co-value problem is Π_1-hard, this means there is a corresponding game G' computable from S such that such that $\omega_{co}(G') = 1$ if $T^{co}_{\mathscr{G}}$ never halts (i.e. $\omega_{co}(G_m) = 1$ for all m), otherwise $\omega_{co}(G') < \frac{1}{2}$. □

Next we show that Π_1-hardness of the *exact co*-value problem implies a *gapless* compression theorem for the commuting operator value of nonlocal games.

Theorem 1.48. *Assume that the exact co-value problem is Π_1-hard. Then there exists a computable map $\mathcal{A}GaplessCompress_{co}$ that takes in as input a description of a sequence of games $\mathscr{G} = (G_n)_{n \in \mathbb{N}}$ and outputs the description of a single game G' such that $\omega_{co}(G') = 1$ if and only if $\omega_{co}(G_n) = 1$ for all $n \in \mathbb{N}$.*

Proof. This follows exactly the same proof as above, except the reduction from the sentence S to the game G' is such that $\omega_{co}(G_m) = 1$ for all m if and only if S is true if and only if $\omega_{co}(G') = 1$. □

Finally we prove that Π_2-hardness of the exact q-value problem implies a gapless compression theorem for the quantum value of nonlocal games.

Theorem 1.49. *Assume that the exact q-value problem is Π_2-hard. Then there exists a computable map $\mathcal{A}GaplessCompress_q$ that takes in as input a description of a sequence of games $\mathcal{G} = (G_n)_{n \in \mathbb{N}}$ and outputs the description of a single game G' such that $\omega_q(G') = 1$ if and only if $\omega_q(G_n) = 1$ for all $n \in \mathbb{N}$.*

Proof. Consider the following Turing machine $T^q_{\mathcal{G}}$: it takes in as input a precision parameter ε and an integer m, and it searches for a finite-dimensional strategy $\mathcal{S}$ (specified with precision ε) such that the game G_m in the sequence $\mathcal{G}$ has $\omega(G_m, \mathcal{S}) \geq 1 - 2\varepsilon$. This can be done because given a dimension $d \in \mathbb{N}$ and a precision parameter ε, there is an algorithm to exhaustively search over an ε-net over d-dimensional quantum strategies.

```
Input: $\varepsilon, m$
for $d \in \mathbb{N}$ do
    If there exists a strategy $\mathcal{S}$ over an $\varepsilon$-net of quantum strategies of dimension $d$, such
      that $\omega(G_m, \mathcal{S}) > 1 - 2\varepsilon$, then halt.
end
```

Pseudocode 13: Specification of $T^q_{\mathcal{G}}$

Note that if $\omega_q(G_m) = 1$, then for all $\varepsilon > 0$ there exists a finite-dimensional strategy that achieves value at least $1 - 2\varepsilon$. On the other hand, if $\omega_q(G_m) < 1$, then there exists an ε for which *all* finite dimensional strategies have value at most $1 - 2\varepsilon$. Thus $\omega_q(G_m) = 1$ for all $m \in \mathbb{N}$ if and only if the following sentence S is true: "$\forall k, m\, \exists n\, T^q_{\mathcal{G}}$ halts on input $\left(\frac{1}{k}, m\right)$ in n steps". Note that S is a Π_2 sentence, and by our assumption there exists a nonlocal game G' that is computable from S such that $\omega_q(G') = 1$ if and only if $\omega_q(G_m) = 1$ for all $m \in \mathbb{N}$.

□

1.7 Appendix A: The pasting lemma

We now prove Theorem 1.18, which is reproduced below for convenience. Recall that $\mathscr{A}$ is a von Neumann algebra with a normal tracial state τ.

Lemma 1.50 (Pasting lemma)**.** *Let $\{M^{(1)}, M^{(2)}, \ldots, M^{(K)}\} \subset \mathscr{A}$ be a set of projective measurements with outcomes in a finite set $\mathcal{A}$. Suppose that for all $i \neq j$, we have that*

$$M_a^{(i)} M_b^{(j)} \approx_\varepsilon M_b^{(j)} M_a^{(i)}$$

where the answer summation is over $(a, b) \in \mathcal{A}^2$. Then there exists a projective measurement $R = \{R_{\vec{a}}\} \subset \mathscr{A}$ with outcomes in $\mathcal{A}^K$ such that for all $i \in [K]$,

$$R_{[\vec{a} \mapsto a_i | b]} \approx_{\delta_{pasting}} M_b^{(i)}$$

where $\delta_{pasting} = \delta_{pasting}(K, \varepsilon)$ is a function that goes to 0 as $\varepsilon \to 0$.

We introduce some notation. For every integer $k \geq 1$, vector $\vec{a} \in \mathcal{A}^k$, and operator index sequence $s \in [M]^k$, define the operator

$$P_{\vec{a}}^s = A_{\vec{a}_1}^{(s_1)} \cdot A_{\vec{a}_2}^{(s_2)} \cdots A_{\vec{a}_k}^{(s_k)}.$$

Note that $P^s = \{P_{\vec{a}}^s\}_{a \in \mathcal{A}^k}$ is a general set of operators (not necessarily a POVM, because the operators are not positive).

We first prove the following utility Lemma. We use the following notational convention: given two operator sets $C = \{C_a\}_{a \in \mathcal{A}}$ and $D = \{D_b\}_{b \in \mathcal{B}}$, we write $C \cdot D$ to denote the operator set $\{C_a \cdot D_b\}_{a \in \mathcal{A}, b \in \mathcal{B}}$.

Lemma 1.51. *For integers $k \geq 1$, for all all sequences $s \in [M]^k$, for all $i \in [M]$, we have*

$$\|P^s \cdot A^{(i)} - A^{(i)} \cdot P^s\|_\tau \leq k\varepsilon$$

Proof. We prove this via induction on k. The base case for $k = 1$ follows from the assumption of the approximate commutativity of the $A^{(i)}$ measurements. Assuming the inductive hypothesis holds for some $k \geq 1$, we now prove it for $k + 1$: let $s \in [M]^k, t \in [M]$. We can treat (s, t) as an operator index sequence of length $k + 1$. Then for all $i \in [M]$, we have

$$\begin{aligned} \|P^{s,t} \cdot A^{(i)} - A^{(i)} \cdot P^{s,t}\|_\tau &= \|P^s \cdot A^{(t)} \cdot A^{(i)} - A^{(i)} \cdot P^s \cdot A^{(t)}\|_\tau \\ &\leq \left\|P^s \cdot \left(A^{(t)} \cdot A^{(i)} - A^{(i)} \cdot A^{(t)}\right)\right\|_\tau + \left\|\left(P^s \cdot A^{(i)} - A^{(i)} \cdot P^s\right) \cdot A^{(t)}\right\|_\tau \end{aligned} \tag{1.7.1}$$

where the inequality follows from the triangle inequality of the τ-norm on operator sets (Theorem 1.10).

We can bound the first term as

$$\left\|P^s \cdot \left(A^{(t)} \cdot A^{(i)} - A^{(i)} \cdot A^{(t)}\right)\right\|_\tau = \left\|A^{(t)} \cdot A^{(i)} - A^{(i)} \cdot A^{(t)}\right\|_\tau \leq \varepsilon \; .$$

The inequality follows from the almost-commutativity of the A's, and the first equality is because

$$\begin{aligned} &= \sum_{\substack{\vec{a} \in \mathcal{A}^k \\ b,c \in \mathcal{A}}} \mathrm{TR}\left(\left(A^{(t)}_b \cdot A^{(i)}_c - A^{(i)}_c \cdot A^{(t)}_b\right)^* (P^s_{\vec{a}})^* P^s_{\vec{a}} \left(A^{(t)}_b \cdot A^{(i)}_c - A^{(i)}_c \cdot A^{(t)}_b\right)\right) \\ &= \sum_{b,c \in \mathcal{A}} \mathrm{TR}\left(\left(A^{(t)}_b \cdot A^{(i)}_c - A^{(i)}_c \cdot A^{(t)}_b\right)^* \left(A^{(t)}_b \cdot A^{(i)}_c - A^{(i)}_c \cdot A^{(t)}_b\right)\right) \end{aligned}$$

where we used the fact that $\sum_{\vec{a} \in \mathcal{A}^k} (P^s_{\vec{a}})^* P^s_{\vec{a}} = 1$.

The second term in (1.7.1) can be similarly bounded as

$$\left\|\left(P^s \cdot A^{(i)} - A^{(i)} \cdot P^s\right) \cdot A^{(t)}\right\|_\tau = \left\|P^s \cdot A^{(i)} - A^{(i)} \cdot P^s\right\|_\tau \leq k\varepsilon$$

by the inductive hypothesis. Thus we can bound (1.7.1) by $(k+1)\varepsilon$, completing the induction. □

For the remainder of the proof let $k = M$. Let $s = (1, 2, \ldots, M) \in [M]^k$ denote an operator index sequence. For all $\vec{a} \in \mathcal{A}^k$, define

$$Q_{\vec{a}} = P^s_{\vec{a}} (P^s_{\vec{a}})^* \ .$$

Note that $Q_{\vec{a}}$ is positive and furthermore $\{Q_{\vec{a}}\}$ forms a POVM with outcomes in $\mathcal{A}^k$ (this uses the fact that the $A^{(i)}_a$ operators are projections).

We now calculate the closeness of $Q_{[\vec{a} \mapsto \vec{a}_i | b]}$ to the individual $A^{(i)}_b$'s:

$$\begin{aligned}
\sum_{b \in \mathcal{A}} \| Q_{[\vec{a} \mapsto \vec{a}_i | b]} - A^{(i)}_b \|^2_\tau &= \sum_{b \in \mathcal{A}} \tau\left(\left(Q_{[\vec{a} \mapsto \vec{a}_i | b]} - A^{(i)}_b \right)^2 \right) \\
&\leq 2 - 2 \sum_{b \in \mathcal{A}} \tau\left(Q_{[\vec{a} \mapsto \vec{a}_i | b]} A^{(i)}_b \right) \\
&= 2 - 2 \sum_{\vec{a}} \tau\left(Q_{\vec{a}} A^{(i)}_{\vec{a}_i} \right)
\end{aligned}$$

We give a lower bound on the magnitude of the second term. Spliting the index sequence $s = (s_{<i}, i, s_{>i})$ and answer tuples $\vec{a} = (\vec{a}_{<i}, \vec{a}_i, \vec{a}_{>i})$, we get

$$\begin{aligned}
\sum_{\vec{a}} \tau\left(Q_{\vec{a}} A^{(i)}_{\vec{a}_i} \right) &= \sum_{\vec{a}} \tau\left(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot P^{s_{>i}}_{\vec{a}_{>i}} \cdot (P^{s_{>i}}_{\vec{a}_{>i}})^* \cdot A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^* \cdot A^{(i)}_{\vec{a}_i} \right) \\
&= \sum_{\vec{a}_{<i}, \vec{a}_i} \tau\left(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^* \cdot A^{(i)}_{\vec{a}_i} \right) \\
&= \sum_{\vec{a}_{<i}, \vec{a}_i} \tau\left(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^* \right) + \tau\left(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot \left((P^{s_{<i}}_{\vec{a}_{<i}})^* \cdot A^{(i)}_{\vec{a}_i} - A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^* \right) \right) \\
&= 1 + \sum_{\vec{a}_{<i}, \vec{a}_i} \tau\left(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot \left((P^{s_{<i}}_{\vec{a}_{<i}})^* \cdot A^{(i)}_{\vec{a}_i} - A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^* \right) \right)
\end{aligned}$$

We can bound the magnitude of the second term using Cauchy-Schwarz:

$$\begin{aligned}
&\left|\sum_{\vec{a}_{<i},\vec{a}_i} \tau\Big(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot \Big((P^{s_{<i}}_{\vec{a}_{<i}})^* \cdot A^{(i)}_{\vec{a}_i} - A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^*\Big)\Big)\right| \\
&\leq \sqrt{\sum_{\vec{a}_{<i},\vec{a}_i} \tau\Big(\Big(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} - A^{(i)}_{\vec{a}_i} \cdot P^{s_{<i}}_{\vec{a}_{<i}}\Big)^* \Big(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} - A^{(i)}_{\vec{a}_i} \cdot P^{s_{<i}}_{\vec{a}_{<i}}\Big)\Big)} \cdot \sqrt{\sum_{\vec{a}_{<i},\vec{a}_i} \tau\Big(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^*\Big)} \\
&\leq \sqrt{\sum_{\vec{a}_{<i},\vec{a}_i} \Big\|P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} - A^{(i)}_{\vec{a}_i} \cdot P^{s_{<i}}_{\vec{a}_{<i}}\Big\|^2_\tau} \\
&\leq M\varepsilon
\end{aligned}$$

where the last inequality follows from Theorem 1.51. Thus we deduce that

$$\sqrt{\sum_{b \in \mathcal{A}} \|Q_{[\vec{a} \mapsto \vec{a}_i | b]} - A^{(i)}_b\|^2_\tau} \leq \sqrt{2M\varepsilon}\ . \tag{1.7.2}$$

Next we argue that the $Q_{\vec{a}}$ is "almost projective". Using that $\sum_{\vec{a}} \tau(Q_{\vec{a}}) = \sum_{\vec{a}} \tau(P^s_{\vec{a}}) = 1$, we get

$$\begin{aligned}
\sum_{\vec{a}} \tau\Big(Q_{\vec{a}} - Q^2_{\vec{a}}\Big) &= \sum_{\vec{a}} \tau\Big(P^s_{\vec{a}} - Q^2_{\vec{a}}\Big) \\
&= \sum_{\vec{a}} \tau\Big(P^s_{\vec{a}} - P^s_{\vec{a}} \cdot Q_{\vec{a}}\Big) + \tau((P^s_{\vec{a}} - Q_{\vec{a}}) \cdot Q_{\vec{a}}) \\
&= \sum_{\vec{a}} \tau\Big(P^s_{\vec{a}} - P^s_{\vec{a}} \cdot (P^s_{\vec{a}})^*\Big) + \tau((P^s_{\vec{a}} - Q_{\vec{a}}) \cdot Q_{\vec{a}}) + \tau(((P^s_{\vec{a}})^* - Q_{\vec{a}}) \cdot P^s_{\vec{a}}) \\
&= \sum_{\vec{a}} \tau((P^s_{\vec{a}} - Q_{\vec{a}}) \cdot Q_{\vec{a}}) + \tau(((P^s_{\vec{a}})^* - Q_{\vec{a}}) \cdot P^s_{\vec{a}})
\end{aligned}$$

where in the last line we used that $P^s_{\vec{a}} \cdot (P^s_{\vec{a}})^* = Q_{\vec{a}}$ and $\sum_{\vec{a}} \tau(Q_{\vec{a}}) = \sum_{\vec{a}} \tau(P^s_{\vec{a}}) = 1$. Using Cauchy-Schwarz and the fact that $\sum_{\vec{a}} \|P^s_{\vec{a}}\|^2_\tau$ and $\sum_{\vec{a}} \|Q_{\vec{a}}\|^2_\tau$ are most 1, this last line is at most $2\sqrt{\sum_{\vec{a}} \|P^s_{\vec{a}} - Q_{\vec{a}}\|^2_\tau}$. To bound this, we note that we can express $P^s_{\vec{a}}$ and $Q_{\vec{a}}$ as longer products

$$P^t_{\vec{b}} = P^{(s_1)}_{\vec{a}_1} \cdot P^{(s_1)}_{\vec{a}_1} \cdots P^{(s_k)}_{\vec{a}_k} \cdot P^{(s_k)}_{\vec{a}_k}\ , \qquad\qquad P^u_{\vec{c}} = P^{(s_1)}_{\vec{a}_1} \cdots P^{(s_k)}_{\vec{a}_k} \cdot \cdots P^{(s_1)}_{\vec{a}_1}$$

where $t = (s_1, s_1, \ldots, s_k, s_k) \in [M]^{2k}$ and $u = (s_1, \ldots, s_k, s_k, \ldots, s_1)$, and $\vec{b} = (\vec{a}_1, \vec{a}_1, \ldots, \vec{a}_k, \vec{a}_k)$ and $\vec{c} = (\vec{a}_1, \ldots, \vec{a}_k, \vec{a}_k, \ldots, \vec{a}_1)$. In particular, let π denote a permutation on $2k$ elements such that $\pi(\vec{b}) = \vec{c}$. Thus

$$\sqrt{\sum_{\vec{a} \in \mathcal{A}^k} \|P^s_{\vec{a}} - Q_{\vec{a}}\|^2_\tau} = \sqrt{\sum_{\vec{a} \in \mathcal{A}^k} \left\|P^t_{\vec{b}} - P^u_{\vec{c}}\right\|^2_\tau} \leq \sqrt{\sum_{\vec{b} \in \mathcal{A}^{2k}} \left\|P^t_{\vec{b}} - P^u_{\pi(\vec{b})}\right\|^2_\tau}$$

Let π' be a permutation that differs from π by a swap of adjacent elements. Then

$$\sqrt{\sum_{\vec{b} \in \mathcal{A}^{2k}} \left\|P^t_{\vec{b}} - P^u_{\pi(\vec{b})}\right\|^2_\tau} \leq \varepsilon$$

by our assumption on the almost-commutativity of the A's. Since π can be formed from the identity permutation by swapping at most $(2k)^2$ adjacent elements, by the triangle inequality we have that

$$\sqrt{\sum_{\vec{b} \in \mathcal{A}^{2k}} \left\|P^t_{\vec{b}} - P^u_{\pi(\vec{b})}\right\|^2_\tau} \leq 4k^2 \varepsilon$$

and therefore $\sum_{\vec{a}} \tau\left(Q_{\vec{a}} - Q^2_{\vec{a}}\right) \leq 8M^2\varepsilon$.

Thus we can apply the Projectivization Lemma (Theorem 1.17) to the POVM $\{Q_{\vec{a}}\}$ to obtain a projective measurement $R = \{R_{\vec{a}}\}$ such that

$$R_{\vec{a}} \approx_\eta Q_{\vec{a}}$$

where $\eta = \delta_{proj}(8M^2\varepsilon)$ where $\delta_{proj}(\cdot)$ is the error function from the Projectivization Lemma. Using the fact that R is projective, we get from Theorem 1.14 that

$$R_{\vec{a}} \simeq_\eta Q_{\vec{a}}.$$

Using the Data Processing Lemma for consistency (Theorem 1.12), we get that

$$R_{[\vec{a}\mapsto\vec{a}_i|b]} \simeq_\eta Q_{[\vec{a}\mapsto\vec{a}_i|b]} \ .$$

Converting from consistency to closeness (Theorem 1.13) we get

$$R_{[\vec{a}\mapsto\vec{a}_i|b]} \approx_{\sqrt{2\eta}} Q_{[\vec{a}\mapsto\vec{a}_i|b]}$$

Finally, we get

$$\begin{aligned} \|R_{[\vec{a}\mapsto\vec{a}_i]} - A^{(i)}\|_\tau &\leq \left\|R_{[\vec{a}\mapsto\vec{a}_i]} - Q_{[\vec{a}\mapsto\vec{a}_i]}\right\|_\tau + \left\|Q_{[\vec{a}\mapsto\vec{a}_i]} - A^{(i)}\right\|_\tau \\ &\leq \sqrt{2\eta} + \sqrt{2M\varepsilon} \ . \end{aligned}$$

Thus we get

$$R_{[\vec{a}\mapsto\vec{a}_i|b]} \approx_{\sqrt{2\eta}+\sqrt{2M\varepsilon}} A_b^{(i)} \ .$$

Setting $\delta_{pasting}(M, \mathcal{A}, \varepsilon) = \sqrt{2\eta} + \sqrt{2M\varepsilon}$ proves the Lemma.

1.8 Appendix B: Complexity of noncommutative polynomial optimization

Recall the (commutative) polynomial optimization problem: given polynomials $p, q_1, \ldots, q_m$ in n-real variables $(x_1, \ldots, x_n)$ with coefficients over $\mathbb{R}$, compute the value of the following optimization program

$$\begin{aligned} \sup \quad & p(x_1, \ldots, x_n) \\ \text{s.t.} \quad & q_i(x_1, \ldots, x_n) \geq 0 \qquad \text{for } i = 1, \ldots, m \end{aligned}$$

Given a commutative polynomial optimization program P and a real number c deciding if its value, denoted by $\omega(P)$, is at least c is NP-hard. In terms of upper bounds, we know that this problem belongs to PSPACE. This is a simple corollary of the following theorem that states that the existential theory of reals is in PSPACE [18].

Theorem 1.52. *There is an algorithm in* PSPACE *such that given any polynomials* $q_1, \ldots, q_m \in \mathbb{R}[x_1, \ldots, x_n]$ *decides if* $\exists x_1, \ldots, x_n \in \mathbb{R}\ q_1 \geq 0, \ldots, q_m \geq 0$.

We now recall the general formulation of noncommutative polynomial optimization (ncPO for short) over Hermitian variables: given polynomials $p, q_1, \ldots, q_m$ in n-noncommutative variables $(x_1, \ldots, x_n)$ with coefficients over $\mathbb{R}$, compute the value of the following optimization program:

$$\begin{aligned} \sup \quad & \langle \phi | p(X) | \phi \rangle \\ \text{s.t.} \quad & q_i(X) \geq 0 \qquad \text{for } i = 1, \ldots, m \end{aligned}$$

The supremum is taken over all choices of tuples $(\mathcal{H}, X, \phi)$ where $\mathcal{H}$ is a Hilbert space, X is an n-tuple of bounded Hermitian operators acting on $\mathcal{H}$, and $|\phi\rangle$ is a unit vector on $\mathcal{H}$. The notation $p(X)$ and $q_i(X)$ indicates that we evaluate each of the indeterminates x_i with the Hermitian operator X_i. We consider two different variations of a ncPO program P; if we restrict the supremum to vary only over finite – but unbounded – dimensional Hilbert spaces then we call the program *finite-dimensional* and let $\omega_{\text{fin}}(P)$ denote the value of the program. Otherwise we call the program *infinite-dimensional* and let $\omega_\infty(P)$ denote its value.

Proposition 1.53. *Given a nonlocal game $G = (\mathcal{X}, \mathcal{A}, \mu, D)$ there exists a ncPO program P where $\omega_{\text{fin}}(P) = \omega_q(G)$ and $\omega_\infty(P) = \omega_{co}(G)$.*

Proof. Define the following optimization problem P over $2|\mathcal{X}||\mathcal{A}|$ variables $\{A_a^x\}, \{B_b^y\}$. The objective polynomial p to be optimized is

$$p = \sum_{x,y\in\mathcal{X}} \sum_{a,b\in\mathcal{A}} \mu(x,y)\, A_a^x B_b^y\, D(x,y,a,b)\ .$$

To enforce that the operators $\{A_a^x\}, \{B_b^y\}$ correspond to POVMs, we add the constraints

1. $A_a^x, B_b^y \geq 0$ (i.e. operators are positive);
2. $\sum_a A_a^x = \sum_b B_b^y = 1$ for all x, y (i.e. operators form POVMs);
3. $[A_a^x, B_b^y] = 0$ (i.e. Alice's and Bob's operators commute) .

It is easy to see that all these constraints can be expressed as polynomial inequalities. The value of this optimization problem corresponds exactly to the definition of ω_q (in the finite-dimensional case) and ω_{co} (in the infinite-dimensional case). □

Theorem 1.54. *Deciding if $\omega_{\text{fin}}(P) \geq c$ or $\omega_{\text{fin}}(P) \leq c - \varepsilon$ for fixed $\varepsilon > 0$ is complete for Σ_1.*

proof of Theorem 1.54. Σ_1-hardness follows from Proposition 1.53 and the Σ_1-hardness of approximating ω_q [4].

To show that the problem is contained in Σ_1, we first argue that, when restricting the Hilbert space to have a *fixed* dimension d, a ncPO program P can be recast as a *commutative* polynomial optimization problem P_d over $\mathbb{C}$. Let p denote the objective polynomial and let $q_1, \ldots, q_m$ denote the constraint polynomials. Let $x_1, \ldots, x_n$ denote the indeterminates of the program.

The optimization problem P_d is defined as follows. To every noncommutative indeterminate x_i we associate d^2 commutative indeterminates x_i^{ab} for $1 \leq a, b \leq d$ over $\mathbb{C}$. Intuitively these indeterminates correspond to the entries of the $d \times d$ Hermitian matrix that is supposed to be substituted in for x_i. We also introduce d indeterminates $y_1, \ldots, y_d$ to represent the unit vector $|\phi\rangle \in \mathbb{C}^d$.

The objective polynomial of P_d is a polynomial p_d that expresses the quantity $\langle\phi|p(x_1, \ldots, x_n)|\phi\rangle$ when $|\phi\rangle$ and the indeterminates x_i are substituted with the corresponding complex numbers. There are constraint polynomials in P_d that encode the fact that the x_i matrices are self-adjoint, and furthermore the vector $(y_1, \ldots, y_d)$ is a unit vector. To check the positivity constraints $q_i \geq 0$ in P we can instead check that all the leading principal minors of q_i are positive. The order k leading principal minor of a $d \times d$ matrix is the determinant of the submatrix obtained from deleting the last $d - k$ rows and columns of the matrix.

Thus, by construction, the value of P_d is the value of P when restricted to d-dimensional Hilbert spaces. We thus have $\omega_{\text{fin}}(P) = \lim_{d\to\infty} \omega(P_d)$. Therefore $\omega_{\text{fin}}(P) \geq c$ if and only if there exists $d \in \mathbb{N}$ such that $c - \omega(P_d) < \varepsilon$.

Therefore we have reduced the problem to deciding whether there exists a dimension d such that $c - \omega(P_d) < \varepsilon$. This corresponds to deciding the Σ_1-sentence $\exists d \; c - \omega(P_d) < \varepsilon$. This sentence is in Σ_1 because determining whether $c - \omega(P_d) \leq \varepsilon$ is in PSPACE (and hence is decidable) by Theorem 1.52.

□

Theorem 1.55. *Deciding if $\omega_{\text{fin}}(P) \geq c$ is complete for Π_2.*

Proof. Π_2-hardness follows from Proposition 1.53 and Theorem 1.45.

Furthermore, deciding if $\omega_{\text{fin}}(P) \geq c$ is equivalent to deciding if for all $n \in \mathbb{N}$ there exists $d \in \mathbb{N}$ such that $c - \omega(P_d) < \frac{1}{n}$ where P_d is as defined in the proof of the previous theorem. Thus we can state the decision problem $\omega_{\text{fin}}(P) \geq c$ as a Π_2-sentence. □

Theorem 1.56. *Deciding if $\omega_\infty(P) \geq c$ is complete for Π_1.*

Proof. Π_1-hardness follows from Proposition 1.53 and Theorem 1.40. The inclusion is due to the NPA-hierarchy of [51]. More precisely [51] constructs an infinite sequence of commutative polynomial optimization relaxations $\{P_i\}_{i\in\mathbb{N}}$ where their values converge, from above, to the value of a given ncPO. Then we can decide if $\omega_\infty(P) \geq c$ by the Π_1-sentence

$$\forall i \in \mathbb{N},\ \ \omega(P_i) \geq c$$

where the $\omega(P_i)$'s converge from above to the the value of $\omega_\infty(P)$. □

Chapter 2: Sum-of-squares approach to noncommutative polynomial optimization

This chapter is taken verbatim from our paper "A generalization of CHSH and the algebraic structure of optimal strategies" [52]. All authors of this work contributed equally.

2.1 Introduction

In 1964, Bell showed that local hidden-variable theories, which are classical in nature, cannot explain all quantum mechanical phenomena [53]. This is obtained by exhibiting a violation of a *Bell inequality* by correlations arising from local measurements on an entangled state. Furthermore, in some instances, it is known that only certain measurements can produce these correlations. So through local measurements not only is it possible to verify that nature is not solely governed by classical theories, it is also possible to obtain conclusive statistical evidence that a specific quantum state was present and specific measurements were performed. Results of this nature are often referred to as *self-testing* (also known as *rigidity*), first formalized by Mayers and Yao in [54]. Self-testing has wide reaching applications in areas of theoretical computer science including complexity theory [55, 56, 57], certifiable randomness [58], device independent quantum cryptography [59, 60], and delegated quantum computation [61]. See [62] for a comprehensive review. Below we visit five natural questions on the topic of self-testing that we answer in this paper.

The CHSH game [63] is the prototypical example of a *non-local game*. In CHSH, two separated players, Alice and Bob, are each provided with a single classical bit, s and t, respectively, chosen uniformly at random by a referee; the players reply with single classical bits a and b to the referee; and win the game if and only if $a \oplus b = s \wedge t$. Classically, the players can win the CHSH game with probability at most 75%. Remarkably, if we allow Alice and Bob to share an entangled state and employ a *quantum strategy*, then the optimal winning probability is approximately 85%. For an introduction to non-local games, see [64].

CHSH is also a canonical example of a self-testing game. Prior to the formalization of self-testing by Mayers and Yao it was already known [65, 66] that any optimal quantum strategy for CHSH must be, up to application of local isometries, using the Einstein-Podolsky-Rosen (EPR) state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right).$$

Self-testing can be framed either as an statement about non-local games, Bell inequalities, or more generally correlations. CHSH is an instance of a *non-pseudo-telepathic* game. A *pseudo-telepathic* game is one that exhibits *quantum advantage* (i.e, its quantum value is strictly larger than that of its classical value) and its quantum value is 1. CHSH can also be viewed as a *linear constraint system* (LCS) game over $\mathbb{Z}_2$ [67]. LCS games are non-local games in which Alice and Bob cooperate to convince the referee that they have a solution to a system of linear equations. We introduce a new generalization of CHSH to a family of non-pseudo-telepathic LCS games over $\mathbb{Z}_n$ for all $n \geq 2$. These games resolve the following questions.

Question 2.1. *Are there states other than the maximally entangled state that can be self-tested by a non-local game?*

To date much has been discovered about self-testing the maximally entangled state, $\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle|j\rangle$. Mermin's *magic square* game [68] can be used to self-test two copies of the EPR state and the *parallel-repeated magic square* game can be used to self-test $2n$ copies of the EPR state [69].

The sum of squares (SOS) decomposition technique in [70] shows that the *tilted CHSH* is a self-test for any pure state of two entangled qubits. This self-testing is stated in terms of violation of Bell inequalities. It is an open problem if the same applies for non-local games. The case for self-testing in higher dimensions has proven more difficult to analyze. Remarkably, it is still possible to self-test any bipartite entangled state, in any dimension [71]. However, these self-test results are presented in terms of violations of correlations, unlike the CHSH game which arises from a non-local game (with binary payoff). Our games also resolve in the negative the question "Can every LCS game be played optimally using the maximally entangled state?" posed in [67].

Question 2.2. *Are there non-local games that provide a self-test for measurements that are not constructed from qubit Pauli operators?*

The protocols in all of the above examples also provide a self-test for the measurement operators. That is if the players are playing optimally then they must, up to application of local isometries, have performed certain measurements. Self-testing proofs rely on first showing that operators in optimal strategies must satisfy certain algebraic relations. These relations help identify optimal operators as representations of some group. This is then used to determine the measurements and state up to local isometries. In the case of CHSH, one can verify that Alice and Bob's measurements must anti-commute if they are to play optimally. These relations are then enough to conclude that operators of optimal strategies generate the dihedral group of degree 4 (i.e., the Pauli group). Thus CHSH is a self-test for the well-known Pauli matrices σ_X and σ_Z [72].

Self-tests for measurements in higher dimensions have been primarily focused on self-testing n-fold tensor-products of σ_X and σ_Z [73, 74, 75]. It is natural to ask if there are self-tests for operators that are different than ones constructed from qubit Pauli operators. Self-testing Clifford observables has also been shown in [76]. Our games provides another example that is neither Pauli nor Clifford. Since our games are LCS this resolves the question, first posed by [77], in the affirmative.

Question 2.3. *Can we extend the solution group formalism for pseudo-telepathic LCS games to a framework for proving self-testing for all LCS games?*

The *solution group* introduced in [6] is an indispensable tool for studying pseudo-telepathic LCS games. To each such game there corresponds a group known as the solution group. Optimal strategies for these games are characterized by their solution group in the sense that any perfect quantum strategy must induce certain representations of this group. Additionally, the work in [77] takes this further by demonstrating a streamlined method to prove self-testing certain LCS games.

It is natural to ask whether these methods can be extended to cover all LCS games. In this paper we make partial progress in answering this question by introducing a SOS framework, and use it to prove self-testing for our games. At its core, this framework utilizes the interplay between sum of squares proofs, non-commutative ring theory, and the Gowers-Hatami theorem [78, 79] from approximate representation theory.

Question 2.4. *Is there a systematic approach to design self-tests for arbitrary finite groups?*

Informally a game is a self-test for a group if every optimal strategy induces a *state dependent representation* of the group. In every example that we are aware of, the self-tested solution group for pseudo-telepathic LCS games is the Pauli group. Slofstra, in [80], introduced an embedding theorem that embeds (almost) any finite group into the solution group of some LCS game. With the embedding theorem, the problem of designing games with certain properties reduces to finding groups with specific properties. Slofstra uses this connection to design games that exhibit separations between correlation sets resolving the 'middle' Tsirelson's Problem.

However, there are three shortcomings to this approach. Firstly, the resulting game is very complex. Secondly, not all properties of the original group are necessarily preserved. Finally, the game is not a self-test for the original group. Our games self-test an infinite family of groups, non of which are the Paulis. One such example is the alternating group of degree 4. The SOS framework makes partial progress towards a general theory for self-testing arbitrary groups.

Question 2.5. *Is there a non-local game that is not a self-test?*

In addition to the infinite family of games, we introduce an LCS game that is obtained from "gluing" together two copies of the magic square game. This *glued magic square* provides an example of a game that is not a self-test [68].

2.1.1 Main Results

We introduce a family of non-local games $\mathcal{G}_n$ defined using the following system of equations over $\mathbb{Z}_n$

$$x_0 x_1 = 1,$$

$$x_0 x_1 = \omega_n.$$

We are identifying $\mathbb{Z}_n$ as a multiplicative group and ω_n as the primitive nth root of unity. Note that the equations are inconsistent, but this does not prevent the game from being interesting. Alice and Bob try to convince a referee that they have a solution to this system of equations. Each player receives a single bit, specifying an equation for Alice and a variable for Bob, and subsequently each player returns a single number in $\mathbb{Z}_n$. Alice's response should be interpreted as an assignment to variable x_0 in the context of the equation she received, and Bob's response is interpreted as an assignment to the variable he received. The referee accepts their response iff their assignments are consistent and satisfy the corresponding equation. The case $n = 2$ is the CHSH game. The classical value of these games is $\frac{3}{4}$. In Section 2.4, we give a lower-bound on the *quantum value* of this family of games. Specifically in Theorem 2.4.9, we show that the quantum value is bounded below by

$$\frac{1}{2} + \frac{1}{2n \sin\left(\frac{\pi}{2n}\right)} > \frac{3}{4}.$$

We show that the lower-bound is tight in the case of $n \leq 5$. We have numerical evidence that these lower-bounds are tight for all n. Specifically, we can find an upper-bound on the quantum value of a non-local game using the well-known hierarchy of semi-definite programs due to [81]. It is of interest to note that the upper-bound is not obtained using the first level of the NPA hierarchy, as is the case with the CHSH game. Instead, the second level of this hierarchy was needed for $n \geq 3$.

The optimal *quantum strategy* for these games uses the entangled state

$$|\psi_n\rangle = \frac{1}{\gamma_n}\sum_{i=0}^{n-1}(1 - z^{n+2i+1})|\sigma^i(0), \sigma^{-i}(0)\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B,$$

where γ_n is the normalization factor, $\sigma_n = (0, 1, \ldots, n-1)$ is a permutation, and z_n is a $4n$'th root of unity. Observe that the state $|\psi_n\rangle$ has full Schmidt rank. Despite this, in all cases except $n = 2$, the state $|\psi_n\rangle$ is not the maximally entangled state. For $n > 2$, the entropy of our state is not maximal, but approaches the maximal entropy of $\log(n)$ in the limit.

In Section 2.5, we show that the group generated by the optimal strategy has the following presentation

$$G_n = \left\langle P_0, P_1, J \mid P_0^n, P_1^n, J^n, [J, P_0], [J, P_1], J^i \left(P_0^i P_1^{-i}\right)^2 \text{ for } i = 1, 2, \ldots, \lfloor n/2 \rfloor \right\rangle.$$

For example $G_3 = \mathbb{Z}_3 \times A_4$ where A_4 is the alternating group of degree 4. We show that our games are a self-test for these groups, for $n \leq 5$, in the sense that every optimal play of this game induces a representation of this group. We conjecture that this is true for all n. This partially resolves Question 2.4.

In section 2.7, we analyze our game in the case $n = 3$ and show that it can be used as a robust self-test for the following state

$$\frac{1}{\sqrt{10}}\left((1 - z^4)|00\rangle + 2|12\rangle + (1 + z^2)|21\rangle\right) \in \mathbb{C}^3 \otimes \mathbb{C}^3,$$

where $z := e^{i\pi/6}$ is the primitive 12th root of unity. Since this state is not the maximally entangled state, we have thus provided an answer to Question 2.1. This game also answers Question 2.2 since it provides a robust self-test for the following operators

$$A_0 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & -z^2 \\ z^2 & 0 & 0 \\ 0 & z^2 & 0 \end{pmatrix},$$

$$B_0 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 0 & -z^2 & 0 \\ 0 & 0 & z^2 \\ z^2 & 0 & 0 \end{pmatrix},$$

which do not generate the Pauli group of dimension 3.

In Section 2.6, we introduce the sum of squares framework, using an important lemma proven in Section 2.2.4, that gives a streamlined method for proving self-testing. We then use this framework to prove self-testing for our games. Furthermore, in Section 2.8, we show that when restricted to pseudo-telepathic games, the SOS framework reduces to the solution group formalism of Cleve, Liu, and Slofstra [6].

In section 2.9, we construct an LCS game that is obtained from "gluing" two copies of the magic square game together. This game is summarized in Figure 2.1. We exhibit two inequivalent perfect strategies and thus provide an answer to Question 2.5.

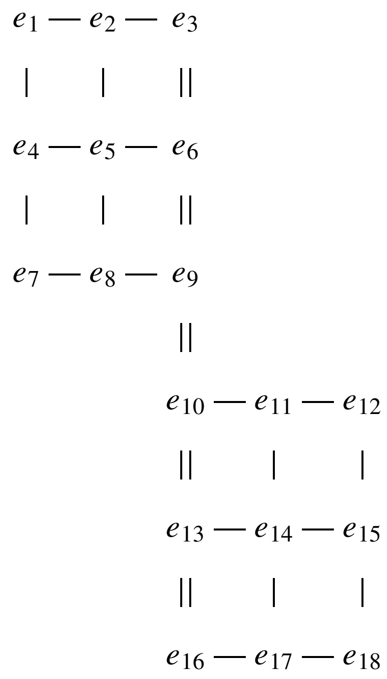

Figure 2.1: This describes an LCS game with 18 variables $e_1, e_2, \ldots, e_{18}$. Each single-line indicates that the variables along the line multiply to 1, and the double-line indicates that the variables along the line multiply to -1.

2.1.2 Proof techniques

We prove self-testing in this paper following a recipe that we refer to as the *SOS framework*. At its core it applies the Gowers-Hatami (GH) theorem which is a result in approximate-representation theory. GH has been used previously in proving self-testing, but some of the details have been overlooked in the literature. In this paper, we prove Lemma 2.2.4 that encapsulates the use of GH in proving self-testing. In Section 2.2.4, we define approximate representations, irreducible strategies, the Gowers-Hatami theorem and present the proof of the following lemma.

Lemma (informal)**.** *Let G_A, G_B be groups. Suppose every optimal strategy of the game $\mathcal{G}$ induces a pair of approximate representations of G_A and G_B. Further suppose that there is a unique optimal irreducible strategy $(\rho, \sigma, |\psi\rangle)$ where ρ, σ are irreps of G_A, G_B, respectively. Then $\mathcal{G}$ is a self-test.*

Applying this lemma requires us to ascertain two properties of the game:

1. Every optimal strategy induces approximate representations of some groups G_A and G_B.

2. There is a unique irreducible strategy $(\rho, \sigma, |\psi\rangle)$ for the game $\mathcal{G}$.

The first step is to obtain the bias expression for the game $\mathcal{G}$ that allows for a simple calculation of the wining probability of any startegy $\mathcal{S} = (\{A_i\}, \{B_j\}, |\psi\rangle)$ (here A_i and B_j are Alice and Bob's measurement observables, respectively, and $|\psi\rangle$ is the shared state). The bias expression for $\mathcal{G}_n$ is given by

$$\mathcal{B}_n(A_0, A_1, B_0, B_1) = \sum_{i=1}^{n-1} A_0^i B_0^{-i} + A_0^i B_1^i + A_1^i B_0^{-i} + \omega^{-i} A_1^i B_1^i.$$

Then the winning probability of $\mathcal{S}$ is given by $\nu(\mathcal{G}, \mathcal{S}) = \langle\psi|(\frac{1}{4n}\mathcal{B}_n(A_0, A_1, B_0, B_1) + \frac{1}{n})|\psi\rangle$. For any real λ for which there exist some polynomials T_k giving a sum of squares decomposition such as

$$\lambda I - \mathcal{B}_n(A_0, A_1, B_0, B_1) = \sum_k T_k^*(A_0, A_1, B_0, B_1) T_k(A_0, A_1, B_0, B_1),$$

provides an upper bound of $\frac{\lambda}{4n} + \frac{1}{n}$ on the optimal value of the game (which we denote by $\nu^*(\mathcal{G}_n)$). This follows since expressing $\lambda I - \mathcal{B}_n$ as an SOS proves that it is a positive semidefinite operator and consequently $\langle\psi|\mathcal{B}_n|\psi\rangle \leq \lambda$ for all states $|\psi\rangle$.

Now if we have an SOS for $\lambda = 4n\nu^*(\mathcal{G}) - 4$, then we can obtain some algebraic relations that every optimal strategy must satisfy. This follows since every optimal strategy must satisfy $\langle\psi|(\lambda I - B_n)|\psi\rangle = 0$, from which it follows $T_k|\psi\rangle = 0$ for all k.

Let $(M_j(A_0, A_1) - I)|\psi\rangle = 0$ be all the relations derived from the SOS relations $T_k|\psi\rangle = 0$ such that M_i are monomials only in Alice's operators, and let G_A be the group with the presentation

$$G_A = \langle P_0, P_1 : M_i(P_0, P_1)\rangle$$

We similarly obtain a group G_B for Bob. These are the group referred in the above lemma. For the first assumption one must show that any optimal strategy gives approximate representations of these groups.

The next step is to prove the second assumption. We need to show that among all the pairs of irreps of G_A and G_B only one could give rise to an optimal strategy. To this end, we let $R_i(A_0, A_1)|\psi\rangle = 0$ be all the relations derived from relations $T_k|\psi\rangle = 0$. These R_i are allowed to be arbitrary polynomials (as opposed to monomials in the case of group relations). So any optimal irrep must satisfy all these polynomial relations. In some special cases, e.g., games $\mathcal{G}_n$, there is one polynomial relation that is enough to identify the optimal irreps.

2.1.3 Relation to prior work

Much work has been done to generalize CHSH to games over $\mathbb{Z}_n$. The first generalization appeared in Buhrman and Massar [82], which was then investigated also by Bavarian and Shor [83] and later extended in [84]. The game we present in section 2.3 provides a different generalization by viewing CHSH as an LCS game. The classical value of our games is found to be $\frac{3}{4}$ from casual observation. Furthermore, we showcase quantum advantage by providing a lower bound on the quantum value for all n.

In contrast the generalization of CHSH discussed in Kaniewski et al. is so difficult to analyze that even the classical value is not known except in the cases of $n = 3, 5, 7$. Additionally the quantum value of their Bell inequality is only determined after multiplying by choices of "phase" coefficients. Self-testing for this generalization is examined by Kaniewski et al., where they prove self-testing for $n = 3$ and show a weaker form of self-testing in the cases of $n = 5, 7$. For the games we introduce, we have self-testing for $n = 3, 4, 5$ and we conjecture that they are self-tests, in the strict sense, for all n.

Furthermore, in [85], Slofstra exhibits a game whose correlations are not extreme point, which suggests that it is also not a self-test, his result is not formulated in the language of self-testing and it would be interesting to rigorously show this to be the case. Independently of our work, in [86], a family of Bell inequalities, which includes the I_{3322} game, is shown to self-test the maximally entangled state but no measurement operators.

2.1.4 Further work

This paper leaves many open problems and avenues for further investigation. The most important of these follow.

1. We conjecture that the class of games $\mathcal{G}_n$ are rigid for all n. The step missing from resolving this conjecture is an SOS decomposition $\nu(\mathcal{G}_n, \mathcal{S}_n)I - \mathcal{B}_n = \sum_k \alpha_{n,k} T^*_{n,k} T_{n,k}$ for $n > 5$ where polynomials $T_{n,k}$ viewed as vectors have unit norms and $\alpha_{n,k}$ are positive real numbers.

   If this conjecture is true, then we have a simple family of games with 1 bit question and $\log n$ bit answer sizes that are self-testing full-Schmidt rank entangled states of any dimension. In fact, we show that the amount of entanglement in these self-tested states rapidly approaches the maximum amount of entanglement. To the best of our knowledge this is the first example of a family of games with such parameters.

2. In Section 2.5, we give efficient explicit presentations for G_n and its multiplication table. Can we go further and characterize these groups in terms of direct and semidirect products of small well-known groups? The first few cases are as follows

$$G_3 \cong \mathbb{Z}_3 \times A_4, G_4 \cong (\mathbb{Z}_2^3 \rtimes \mathbb{Z}_4) \rtimes \mathbb{Z}_4, G_5 \cong (\mathbb{Z}_2^4 \rtimes \mathbb{Z}_5) \times \mathbb{Z}_5,$$

$$G_6 \cong \mathbb{Z}_3 \times \Big((((\mathbb{Z}_4 \times \mathbb{Z}_2^3) \rtimes \mathbb{Z}_2) \rtimes \mathbb{Z}_2) \rtimes \mathbb{Z}_3\Big).$$

3. The third problem is to characterize all mod n games over two variables and two equations. Let $(\mathbb{Z}_n, m_1, m_2)$ be the LCS game mod n based on the system of equations

$$x_0 x_1 = \omega_n^{m_1}$$

$$x_0 x_1 = \omega_n^{m_2}.$$

   So for example $(\mathbb{Z}_n, 0, 1) = \mathcal{G}_n$. A full characterization includes explicit construction of optimal strategies, a proof of self-testing, and a characterization of the group generated by optimal strategies (i.e., the *self-tested group*). Interesting observations can be made about these games. For example $(\mathbb{Z}_4, 0, 2)$ self-tests the same strategy as CHSH. Another interesting observation is that the self-tested group of $(\mathbb{Z}_3, 0, 1)$ and $(\mathbb{Z}_3, 0, 2)$ is $G_3 \cong \mathbb{Z}_3 \times A_4$, whereas the self-tested group of $(\mathbb{Z}_3, 1, 2)$ is A_4.

These games have similar bias expressions to those of $\mathcal{G}_n$. It is likely that the same kind of methods can be used to find optimal strategies and establish self-testing for these games. For example $(\mathbb{Z}_n, 0, m)$ for all $m \in [n] \setminus \{0\}$ self-test the same group G_n. Just like $\mathcal{G}_n$, the representation theory of G_n dictates the optimal strategies of all these games: the optimal irreducible strategies of $(\mathbb{Z}_n, 0, m)$ for all $m \in [n] \setminus \{0\}$ are distinct irreps of G_n of degree n.

For example optimal strategies for all games $(\mathbb{Z}_5, 0, m)$, where $m \in [5] \setminus \{0\}$, generate G_5. This group has 15 irreps of degree five. For each $m \in [5]$, there are three irreps sending $J \rightarrow \omega_5^m I_5$. For each $m \in [5] \setminus \{0\}$, the unique optimal irrep strategy of $(\mathbb{Z}_5, 0, m)$ is one of these three irreps.

These games are a rich source of examples for self-testing of groups. A full characterization is a major step toward resolving Question 2.4.

4. One drawback of $\bmod n$ games is that the size of the self-tested groups grows exponentially, $|G_n| = 2^{n-1}n^2$. Where are the games that self-test smaller groups for example the dihedral group of degree 5, D_5? It seems that to test more groups, we need to widen our search space.

   In a similar fashion to mod n games, define games (G, g_1, g_2) where G is a finite group and $g_1, g_2 \in G$, based on the system of equations

$$x_0 x_1 = g_1$$
$$x_0 x_1 = g_2.$$

   Understanding the map that sends (G, g_1, g_2) to the self-tested group helps us develop a richer landscape of group self-testing.

5. How far can the SOS framework be pushed to prove self-testing? The first step in answering this question is perhaps a characterization of games (G, g_1, g_2) (and their variants, e.g., system of equations with more variables and equations) using this framework.

6. Glued magic square, as presented in Section 2.9, is not a self-test for any operator solution, but both inequivalent strategies that we present use the maximally entangled state. Is the glued magic square a self-test for the maximally entangled state? If true, this would give another example of a non-local game that only self-tests the state and not the measurement operators.

   After the publication of our work, Mančinska et al. [87] showed that this is indeed the case; specifically they showed that the glued magic square self-tests convex combinations of the two inequivalent strategies we presented in our work. Along with [86], these positively resolve a question asked in [62] in the context of non-local games.

2.1.5 Organization of paper

In section 2.2, we fix the nomenclature and give basic definitions for non-local games, winning strategies, self-testing, LCS games, approximate representation, and the Gowers-Hatami theorem. In section 2.3, we give the generalization of CHSH and derive the bias operator of these games, that is used in the rest of the paper. In Section 2.4, we establish lower-bounds on the quantum value for these games by presenting explicit strategies. In this section we also analyse the entanglement entropy of the shared states in these explicit strategies. In Section 2.5, we give a presentation for the groups generated by Alice and Bob's observables. In Section 2.6, we present the SOS framework and give a basic example of its application in proving self-testing. In section 2.7, we use the SOS framework to show that our lower-bound is tight in the case of $n = 3$, and answer the questions we posed about self-testing. In section 2.8, we show that the SOS framework reduces to the solution group formalism in the case of pseudo-telepathic LCS games. Finally, in Section 2.9 we provide an example of a non-rigid game.

2.2 Preliminaries

We assume the reader has a working understanding of basic concepts from the field of quantum information theory. For an overview of quantum information, refer to [88, 89, 90].

2.2.1 Notation

We use G to refer to a group, while $\mathcal{G}$ is reserved for a non-local game. Let $[n, m]$ denote the set $\{n, n+1, \ldots, m\}$ for integers $n \leq m$, and the shorthand $[n] = [0, n-1]$. This should not be confused with $[X, Y]$, which is used to denote the commutator $XY - YX$. We let I_n denote the $n \times n$ identity matrix and e_i, for $i \in [n]$, be the ith standard basis vector. The pauli observables are denoted σ_x, σ_y, and σ_z. The Kronecker delta is denoted by $\delta_{i,j}$.

We will let $\mathcal{H}$ denote a finite dimensional Hilbert space and use the notation $|\psi\rangle \in \mathcal{H}$ to refer to vectors in $\mathcal{H}$. We use $\mathrm{L}(\mathcal{H})$ to denote the set of linear operators in the Hilbert space $\mathcal{H}$. We use $\mathrm{U}_n(\mathbb{C})$ to denote the set of unitary operators acting on the Hilbert space $\mathbb{C}^n$. The set of projection operators acting on $\mathcal{H}$ are denoted by $\mathrm{Proj}(\mathcal{H})$. Given a linear operator $A \in \mathrm{L}(\mathcal{H})$, we let $A^* \in \mathrm{L}(\mathcal{H})$ denote the adjoint operator. For $X, Y \in \mathrm{L}(\mathcal{H})$, the Hilber-Schmidt inner product is given by $\langle X, Y\rangle = \mathrm{TR}(X^*Y)$. We also use the following shorthands $\mathrm{TR}_\rho(X) = \mathrm{TR}(X\rho)$ and $\langle X, Y\rangle_\rho = \mathrm{TR}_\rho(X^*Y)$ where $X, Y \in \mathrm{L}(\mathcal{H})$ and ρ is a density operator acting on $\mathcal{H}$ (i.e., positive semidefinite with trace 1). The von Neumann entropy of a density matrix ρ is given by $S(\rho) = -\mathrm{TR}(\rho \log \rho)$.

We use $\Re(\alpha)$ to denote the real part of a complex number α. We let $\omega_n = e^{2i\pi/n}$ be the nth root of unity. The Dirichlet kernel is $\mathcal{D}_m(x) = \frac{1}{2\pi}\sum_{k=-m}^{m} e^{ikx}$ which by a well known identity is equal to $\frac{\sin\left(\left(m+\frac{1}{2}\right)x\right)}{2\pi\sin\left(\frac{x}{2}\right)}$.

The maximally entangled state with local dimension n is given by $|\Phi_n\rangle = \frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}|i\rangle|i\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$.

Let $\mathcal{H}_A, \mathcal{H}_B$ be Hilbert spaces of dimension n and $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite state. Then there exists orthonormal bases $\{|i_A\rangle\}_{i=0}^{n-1}$ for $\mathcal{H}_A$ and $\{|i_B\rangle\}_{i=0}^{n-1}$ for $\mathcal{H}_B$ and unique non-negative real numbers $\{\lambda_i\}_{i=0}^{n-1}$ such that $|\psi\rangle = \sum_{i=0}^{n-1} \lambda_i |i_A\rangle|i_B\rangle$. The λ_i's are known as Schmidt coefficients.

The Schmidt rank of a state is the number of non-zero Schmidt coefficients λ_i. The Schmidt rank is a rough measure of entanglement. In particular, a pure state $|\psi\rangle$ is entangled if and only if it has Schmidt rank greater than one.

Another measure of entanglement is the *entanglement entropy*. Given the Schmidt decomposition of a state $|\psi\rangle = \sum_{i=0}^{n-1} \lambda_i |i_A\rangle|i_B\rangle$, the entanglement entropy S_ψ is given by $-\sum_{i=0}^{n-1} \lambda_i^2 \log(\lambda_i^2)$. The maximum entanglement entropy is $\log(n)$. A pure state is separable (i.e. not entangled) when the entanglement entropy is zero. If the entanglement entropy of a state $|\psi\rangle$ is maximum, then the state is the maximally entangled state up to local unitaries, i.e., there exist unitaries $U_A, U_B \in \mathrm{U}_n(\mathbb{C})$, such that $|\psi\rangle = U_A \otimes U_B |\Phi_n\rangle$.

2.2.2 Non-local games

A *non-local game* is played between a referee and two cooperating players Alice and Bob who cannot communicate once the game starts. The referee provides each player with a question (input), and the players each respond with an answer (output). The referee determines whether the players win with respect to fixed conditions known to all parties. Alice does not know Bob's question and vice-versa as they are not allowed to communicate once the game starts. However, before the game starts, the players could agree upon a strategy that maximizes their success probability. Below we present the formal definition and some accompanying concepts.

Definition 2.2.1. A non-local game $\mathcal{G}$ is a tuple $(\mathcal{I}_A, \mathcal{I}_B, O_A, O_B, \pi, V)$ where $\mathcal{I}_A$ and $\mathcal{I}_B$ are finite question sets, O_A and O_B are finite answer sets, π denotes the probability distribution on the set $\mathcal{I}_A \times \mathcal{I}_B$ and $V : \mathcal{I}_A \times \mathcal{I}_B \times O_A \times O_B \to \{0, 1\}$ defines the winning conditions of the game.

When the game begins, the referee chooses a pair $(i, j) \in \mathcal{I}_A \times \mathcal{I}_B$ according to the distribution π. The referee sends i to Alice and j to Bob. Alice then responds with $a \in O_A$ and Bob with $b \in O_B$. The players win if and only if $V(i, j, a, b) = 1$.

A *classical strategy* is defined by a pair of functions $f_A : \mathcal{I}_A \to O_A$ for Alice and $f_B : \mathcal{I}_B \to O_B$

for Bob. The winning probability of this strategy is

$$\sum_{i,j} \pi(i,j)V(i,j,f_A(i),f_B(j)).$$

The *classical value*, $v(\mathcal{G})$, of a game is the supremum of this quantity over all classical strategies (f_A, f_B).

A *quantum strategy* $\mathcal{S}$ for $\mathcal{G}$ is given by Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$, a state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, and projective measurements $\{E_{i,a}\}_{a\in O_A} \subset \text{Proj}(\mathcal{H}_A)$ and $\{F_{j,b}\}_{b\in O_B} \subset \text{Proj}(\mathcal{H}_B)$ for all $i \in \mathcal{I}_A$ and $j \in \mathcal{I}_B$.

Alice and Bob each have access to Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. On input (i, j), Alice and Bob measure their share of the state $|\psi\rangle$ according to $\{E_{i,a}\}_{a\in O_A}$ and $\{F_{j,b}\}_{b\in O_B}$. The probability of obtaining outcome a, b is given by $\langle\psi|E_{i,a} \otimes F_{j,b}|\psi\rangle$. The winning probability of strategy $\mathcal{S}$, denoted by $v(\mathcal{G}, \mathcal{S})$ is therefore

$$v(\mathcal{G},\mathcal{S}) = \sum_{i,j,a,b} \pi(i,j)\langle\psi|E_{i,a} \otimes F_{j,b}|\psi\rangle V(i,j,a,b).$$

The quantum value of a game, written $v^*(\mathcal{G})$, is the supremum of the winning probability over all quantum strategies.

The famous CHSH game [63] is the tuple $(\mathcal{I}_A, \mathcal{I}_B, O_A, O_B, \pi, V)$ where $\mathcal{I}_A = \mathcal{I}_B = O_A = O_B = \{0, 1\}$, π is the uniform distribution on $\mathcal{I}_A \times \mathcal{I}_B$, and $V(i, j, a, b) = 1$ if and only if

$$a + b \equiv ij \mod 2.$$

The CHSH game has a classical value of 0.75 and a quantum value of $\frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.85$ [63].

A strategy $\mathcal{S}$ is optimal if $v(\mathcal{G}, \mathcal{S}) = v^*(\mathcal{G})$. When a game's quantum value is larger than the classical value we say that the game exhibits *quantum advantage*. A game is *pseudo-telepathic* if it exhibits quantum advantage and its quantum value is 1.

An *order-n generalized observable* is a unitary U for which $U^n = I$. It is customary to assign an order-n generalized observable to a projective measurement system $\{E_0, \dots, E_{n-1}\}$ as

$$A = \sum_{i=0}^{n-1} \omega_n^i E_i.$$

Conversely, if A is an order-n generalized observable, then we can recover a projective measurement system $\{E_0, \dots, E_{n-1}\}$ where

$$E_i = \frac{1}{n} \sum_{k=0}^{n-1} \left(\omega_n^{-i} A\right)^k .$$

In this paper, present strategies in terms of generalized observables.

Consider the strategy $\mathcal{S}$ consisting of the shared state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and observables $\{A_i\}_{i \in \mathcal{I}_A}$ and $\{B_j\}_{j \in \mathcal{I}_B}$ for Alice and Bob. We say the game $\mathcal{G}$ is a *self-test* for the strategy $\mathcal{S}$ if there exist $\varepsilon_0 \geq 0$ and $\delta : \text{real}^+ \rightarrow \text{real}^+$ a continuous function with $\delta(0) = 0$, such that the following hold

1. $\mathcal{S}$ is optimal for $\mathcal{G}$.
2. For any $0 \leq \varepsilon \leq \varepsilon_0$ and any strategy $\widetilde{\mathcal{S}} = (\{\widetilde{A}_i\}_{i \in \mathcal{I}_A}, \{\widetilde{B_j}\}_{j \in \mathcal{I}_B}, |\widetilde{\psi}\rangle)$ where $|\widetilde{\psi}\rangle \in \widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B$ and $\nu(\mathcal{G}, \widetilde{\mathcal{S}}) \geq \nu^*(\mathcal{G}) - \varepsilon$, there exist local isometries V_A and V_B, and a state $|\text{junk}\rangle$ such that the following hold
    - $\left\| V_A \otimes V_B |\widetilde{\psi}\rangle - |\psi\rangle|\text{junk}\rangle \right\| \leq \delta(\varepsilon)$,
    - $\left\| V_A \widetilde{A}_i \otimes V_B |\widetilde{\psi}\rangle - (A_i \otimes I|\psi\rangle)|\text{junk}\rangle \right\| \leq \delta(\varepsilon)$ for all $i \in \mathcal{I}_A$,
    - $\left\| V_A \otimes V_B \widetilde{B_j} |\widetilde{\psi}\rangle - (I \otimes B_j|\psi\rangle)|\text{junk}\rangle \right\| \leq \delta(\varepsilon)$ for all $j \in \mathcal{I}_B$.

We use the terminology *rigidity* and self-testing interchangeably. *Exact rigidity* is a weaker notion in which, we only require the second condition to hold for $\varepsilon = 0$. In Section 2.6, we give as an example the proof of exact rigidity of the CHSH game.

2.2.3 Linear constraint system games

A *linear constraint system* (LCS) game is a non-local game in which Alice and Bob cooperate to convince the referee that they have a solution to a system of linear equations over $\mathbb{Z}_n$. The referee sends Alice an equation and Bob a variable in that equation, uniformly at random. In response, Alice specifies an assignment to the variables in her equation and Bob specifies an assignment to his variable. The players win exactly when Alice's assignment satisfies her equation and Bob's assignment agrees with Alice. It follows that an LCS game has a perfect classical strategy if and only if the system of equations has a solution over $\mathbb{Z}_n$. Similarly the game has a perfect quantum strategy if and only if the system of equations, when viewed in the multiplicative form, has an *operator solution* [67].

To each LCS game there corresponds a group referred to as the *solution group*. The representation theory of solution group is an indispensable tool in studying pseudo-telepathic LCS games [6, 77]. In what follows we define these terms formally, but the interested reader is encouraged to consult the references to appreciate the motivations. In this paper, we are interested in extending solution group formalism to general LCS games using the sum of squares approach. We explore this extension in Section 2.7. When restriced to psuedo-telepathic LCS games, our SOS approach is identical to the solution group formalism. We present this in section 2.8 for completeness.

Consider a system of linear equations $Ax = b$ where $A \in \mathbb{Z}_n^{r\times s}$, $b \in \mathbb{Z}_n^r$. We let V_i denote the set of variables occurring in equation i

$$V_i = \{j \in [s] : a_{i,j} \neq 0\}.$$

To view this system of linear equations in multiplicative form, we identify $\mathbb{Z}_n$ multiplicatively as $\{1, \omega_n, \ldots, \omega_n^{n-1}\}$. Then express the ith equation as

$$\prod_{j\in V_i} x_j^{a_{ij}} = \omega_n^{b_i}.$$

In this paper we only use this multiplicative form. We let S_i denote the set of satisfying assignments to equation i. In the LCS game $\mathcal{G}_{A,b}$, Alice receives an equation $i \in [r]$ and Bob receives a variable $j \in V_i$, uniformly at random. Alice responds with an assignment x to variables in V_i and Bob with an assignment y to his variable j. They win if $x \in S_i$ and $x_j = y$.

The solution group $G_{A,b}$ associated with $\mathcal{G}_{A,b}$, is the group generated by $g_1, \dots, g_s, J$, satisfying the relations

1. $g_j^n = J^n = 1$ for all j,
2. $g_j J = J g_j$ for all j,
3. $g_j g_k = g_k g_j$ for $j, k \in V_i$ for all i, and
4. $\prod_{j \in V_i} g_j^{A_{ij}} = J^{b_i}$.

2.2.4 Gowers-Hatami theorem and its application to self-testing

In order to precisely state our results about self-testing in Section 2.7, we recall the Gowers-Hatami theorem and $(\varepsilon, |\psi\rangle)$-representation [78, 77, 79].

Definition 2.2.2. Let G be a finite group, n an integer, Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ of dimension n, and $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ a state with the reduced density matrix $\sigma \in \mathrm{L}(\mathcal{H}_A)$. An $(\varepsilon, |\psi\rangle)$-representation of G, for $\varepsilon \geq 0$, is a function $f : G \to U_n(\mathbb{C})$ such that

$$\mathbb{E}_{x,y} \Re \left(\langle f(x)^* f(y), f(x^{-1}y) \rangle_\sigma \right) \geq 1 - \varepsilon. \tag{2.2.1}$$

In the case of $\varepsilon = 0$, we abbreviate and call such a map a $|\psi\rangle$-representation, in which case the condition 2.2.1 simplifies to

$$\langle f(x)^* f(y), f(x^{-1}y) \rangle_\sigma = 1,$$

or equivalently

$$f(y)^* f(x) f(x^{-1}y)|\psi\rangle = |\psi\rangle, \tag{2.2.2}$$

for all $x, y \in G$. In Condition (2.2.2), we are implicitly dropping the tensor with identity on $\mathcal{H}_B$. Note that a $|\psi\rangle$-representation f is just a group representation when restricted to the Hilbert space $\mathcal{H}_0 = \operatorname{span}\{f(g)|\psi\rangle : g \in G\}$, i.e., the Hilbert space generated by the image of f acting on $|\psi\rangle$. To see this, we first rewrite (2.2.2) as

$$f(x^{-1}y)|\psi\rangle = f(x)^* f(y)|\psi\rangle.$$

Thus for any $x, y \in G$ we have

$$f(x^{-1})^* f(x^{-1}y)|\psi\rangle = f(xx^{-1}y)|\psi\rangle = f(y)|\psi\rangle.$$

We can multiply both sides by $f(x^{-1})$ to obtain $f(x^{-1}y)|\psi\rangle = f(x^{-1})f(y)|\psi\rangle$ for all $x, y \in G$ or equivalently

$$f(x)f(y)|\psi\rangle = f(xy)|\psi\rangle \text{ for all } x, y \in G. \tag{2.2.3}$$

This shows that for all $x \in G$, the operator $f(x)$ leaves the subspace H_0 invariant. Thus we can view $f(x)|_{H_0}$, the restriction of $f(x)$ to this subspace, as an element of $\mathrm{L}(H_0)$. Furthermore, by (2.2.3), the map $x \mapsto f(x)|_{H_0}$ is a homormorphism and thus a representation of G on H_0.

We need the following special case of the Gowers-Hatami (GH) theorem as presented in [79]. The analysis of the robust rigidity of these games uses the general statement of GH, using $(\varepsilon, |\psi\rangle)$-representation. Although skipped in this paper, the tools are in place to analyse the robust case.

Theorem 2.2.3 (Gowers-Hatami)**.** *Let d be an integer, $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ a bipartite state, G a finite group, and $f : G \to \mathrm{U}_d(\mathbb{C})$ a $|\psi\rangle$-representation. Then there exist $d' \geq d$, a representation*

$g : G \to \mathrm{U}_{d'}(\mathbb{C})$, and an isometry $V : \mathbb{C}^d \to \mathbb{C}^{d'}$ such that $f(x) \otimes I|\psi\rangle = V^* g(x) V \otimes I|\psi\rangle$.

From the proof of this theorem in [79], we can take $g = \oplus_\rho I_d \otimes I_{d_\rho} \otimes \rho$ where ρ ranges over irreducible representations of G and d_ρ is the dimension of ρ. Additionally, in the same bases, we can factorize V into a direct sum over irreps such that $Vu = \oplus_\rho(V_\rho u)$, for all $u \in \mathbb{C}^d$ where $V_\rho \in \mathrm{L}(\mathbb{C}^d, \mathbb{C}^d \otimes \mathbb{C}^{d_\rho} \otimes \mathbb{C}^{d_\rho})$ are some linear operators. It holds that $\sum_\rho V_\rho^* V_\rho = V^* V = I_d$.

In some special cases, such as in our paper, we can restrict g to be a single irreducible representation of G. In such cases we have a streamlined proof of self-testing. Lemma 2.2.4 below captures how GH is applied in proving self-testing in these cases.

Let $\mathcal{G} = (\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B, \pi, V)$ be a game, G_A and G_B be groups with generators $\{P_i\}_{i \in I_A}$ and $\{Q_j\}_{j \in I_B}$, $\widehat{G}_A$ and $\widehat{G}_B$ be free groups over $\{P_i\}_{i \in I_A}$ and $\{Q_j\}_{j \in I_B}$, and $\mathcal{S} = (\{A_i\}, \{B_j\}, |\psi\rangle)$ be a strategy where $|\psi\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. We define two functions $f_A^{\mathcal{S}} : \widehat{G}_A \to \mathrm{U}_{d_A}(\mathbb{C})$, $f_B^{\mathcal{S}} : \widehat{G}_B \to \mathrm{U}_{d_B}(\mathbb{C})$ where $f_A^{\mathcal{S}}(P_i) = A_i$ and $f_B^{\mathcal{S}}(Q_j) = B_j$ and they are extended homomorphically to all of $\widehat{G}_A$ and $\widehat{G}_B$, respectively. Suppose that the game $\mathcal{G}$ has the property that for every optimal strategy $\widetilde{\mathcal{S}} = (\{\widetilde{A}_i\}, \{\widetilde{B}_j\}, |\widetilde{\psi}\rangle)$, $f_A^{\widetilde{\mathcal{S}}}$ and $f_B^{\widetilde{\mathcal{S}}}$ are $|\widetilde{\psi}\rangle$-representations for G_A and G_B, respectively.

Now applying GH, for every optimal strategy $\widetilde{\mathcal{S}}$, there exist representations g_A, g_B of G_A, G_B, respectively, and isometries V_A, V_B such that

$$f_A^{\widetilde{\mathcal{S}}}(x) \otimes I|\widetilde{\psi}\rangle = V_A^* g_A(x) V_A \otimes I|\widetilde{\psi}\rangle \text{ for all } x \in G_A,$$
$$I \otimes f_B^{\widetilde{\mathcal{S}}}(y)|\widetilde{\psi}\rangle = I \otimes V_B^* g_B(y) V_B|\widetilde{\psi}\rangle \text{ for all } y \in G_B.$$

Unfortunately this is not enough to establish rigidity for $\mathcal{G}$ as defined in Section 2.2.2. To do this, we need and extra assumption on $\mathcal{G}$ that we deal with in the following lemma.

For any pair of representations ρ, σ of G_A, G_B respectively, and state $|\psi\rangle \in \mathbb{C}^{d_\sigma} \otimes \mathbb{C}^{d_\rho}$, let $\mathcal{S}_{\rho,\sigma,|\psi\rangle} = (\{\rho(P_i)\}_{i \in \mathcal{I}_A}, \{\sigma(Q_j)\}_{j \in \mathcal{I}_B}, |\psi\rangle)$ be the strategy induced by the pair of representations (ρ, σ). Also let $\nu(\mathcal{G}, \rho, \sigma) = \max_{|\psi\rangle} \nu(\mathcal{G}, \mathcal{S}_{\rho,\sigma,|\psi\rangle})$.

Lemma 2.2.4. *Suppose that there is only one pair of irreps $\bar{\rho}, \bar{\sigma}$ for which $\nu(\mathcal{G}, \bar{\rho}, \bar{\sigma}) = \nu^*(\mathcal{G})$. Additionally assume that $|\psi\rangle$ is the unique state (up to global phase) for which $\mathcal{S}_{\bar{\rho},\bar{\sigma},|\psi\rangle}$ is an* *optimal strategy. Let $\widetilde{\mathcal{S}} = (\{\widetilde{A}_i\}, \{\widetilde{B}_j\}, |\widetilde{\psi}\rangle)$ be an optimal strategy of $\mathcal{G}$ such that $|\widetilde{\psi}\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$, $f_A^{\widetilde{S}}$ and $f_B^{\widetilde{S}}$ are $|\widetilde{\psi}\rangle$-representations for G_A and G_B, respectively. Then there exist isometries $V_A : \mathbb{C}^{d_A} \longrightarrow \mathbb{C}^{d_A|G_A|}, V_B : \mathbb{C}^{d_B} \longrightarrow \mathbb{C}^{d_B|G_B|}$, and a state $|junk\rangle$ such that*

$$V_A \otimes V_B|\widetilde{\psi}\rangle = |junk\rangle|\psi\rangle,$$

$$V_A\widetilde{A}_i \otimes V_B|\widetilde{\psi}\rangle = |junk\rangle\bar{\rho}(P_i) \otimes I_{d_{\bar{\sigma}}}|\psi\rangle,$$

$$V_A \otimes V_B\widetilde{B}_j|\widetilde{\psi}\rangle = |junk\rangle I_{d_{\bar{\rho}}} \otimes \bar{\sigma}(Q_j)|\psi\rangle,$$

for all $i \in I_A, j \in I_B$.

Proof. For simplicity, we only prove the case of binary games, i.e., we assume $|O_A| = |O_B| = 2$. The general case follows similarly. For binary games we only need to consider strategies comprised of binary observables (A is a binary observable if it is Hermitian and $A^2 = I$). Without loss of generality, we can assume that there exist some complex numbers $\lambda_{ij}, \lambda_i, \lambda_j, \lambda$ such that for any strategy $\mathcal{S} = (\{A_i\}, \{B_j\}, |\psi\rangle)$

$$v(\mathcal{G}, \mathcal{S}) = \langle\psi| \left(\sum_{i\in I_A, j\in I_B} \lambda_{ij} A_i \otimes B_j + \sum_{i\in I_A} \lambda_i A_i \otimes I + \sum_{j\in I_B} \lambda_j I \otimes B_j + \lambda I \otimes I \right) |\psi\rangle. \tag{2.2.4}$$

As argued earlier, by GH, we have

$$f_A^{\widetilde{S}}(x) \otimes I|\widetilde{\psi}\rangle = V_A^* g_A(x) V_A \otimes I|\widetilde{\psi}\rangle, \tag{2.2.5}$$

$$I \otimes f_B^{\widetilde{S}}(x)|\widetilde{\psi}\rangle = I \otimes V_B^* g_B(x) V_B|\widetilde{\psi}\rangle, \tag{2.2.6}$$

where $g_A = \oplus_\rho I_{d_A d_\rho} \otimes \rho, g_B = \oplus_\sigma I_{d_B d_\sigma} \otimes \sigma$, where ρ and σ range over irreducible representations of G_A and G_B, respectively. We also have the factorization $V_A u = \oplus_\rho (V_{A,\rho} u)$, for all $u \in \mathbb{C}^{d_A}$ as well as $V_B u = \oplus_\sigma (V_{B,\sigma} u)$, for all $u \in \mathbb{C}^{d_B}$. As mentioned above in the discussion that followed Theorem 2.2.3, $V_{A,\rho}$ and $V_{B,\sigma}$ are some linear operators for which $\sum_\rho V_{A,\rho}^* V_{A,\rho} = I_{d_A}$ and $\sum_\sigma V_{B,\sigma}^* V_{B,\sigma} = I_{d_B}$.

We want to write the winning probability of $\widetilde{\mathcal{S}}$ in terms of the winning probabilities of irrep strategies. To this end, let

$$p_{\rho,\sigma} = \|V_{A,\rho} \otimes V_{B,\sigma}|\widetilde{\psi}\rangle\|^2,$$
$$|\widetilde{\psi}_{\rho,\sigma}\rangle = \begin{cases} \frac{1}{\sqrt{p_{\rho,\sigma}}} V_{A,\rho} \otimes V_{B,\sigma}|\widetilde{\psi}\rangle & p_{\rho,\sigma} > 0, \\ 0 & p_{\rho,\sigma} = 0, \end{cases}$$

and consider strategies

$$\mathcal{S}_{I\otimes\rho, I\otimes\sigma, |\widetilde{\psi}_{\rho,\sigma}\rangle} = (\{I_{d_A d_\rho} \otimes \rho(P_i)\}, \{I_{d_B d_\sigma} \otimes \sigma(Q_j)\}, |\widetilde{\psi}_{\rho,\sigma}\rangle).$$

Using (2.2.4), we can write

$$\begin{aligned} \nu(\mathcal{G}, \widetilde{\mathcal{S}}) &= \langle\widetilde{\psi}| \left(\sum_{i\in I_A, j\in I_B} \lambda_{ij} \widetilde{A}_i \otimes \widetilde{B}_j + \sum_{i\in I_A} \lambda_i \widetilde{A}_i \otimes I + \sum_{j\in I_B} \lambda_j I \otimes \widetilde{B}_j + \lambda I \otimes I \right) |\widetilde{\psi}\rangle \\ &= \sum_{\rho,\sigma} \langle\widetilde{\psi}| V_{A,\rho}^* \otimes V_{B,\sigma}^* \Big(\sum_{i\in I_A, j\in I_B} \lambda_{ij} (I_{d_A d_\rho} \otimes \rho(P_i)) \otimes (I_{d_B d_\sigma} \otimes \sigma(Q_j)) + \sum_{i\in I_A} \lambda_i (I_{d_A d_\rho} \otimes \rho(P_i)) \otimes I \\ &\qquad + \sum_{j\in I_B} \lambda_j I \otimes (I_{d_B d_\sigma} \otimes \sigma(Q_j)) + \lambda I \otimes I \Big) V_{A,\rho} \otimes V_{B,\sigma} |\widetilde{\psi}\rangle \\ &= \sum_{\rho,\sigma} p_{\rho,\sigma} \nu(\mathcal{G}, \mathcal{S}_{I\otimes\rho, I\otimes\sigma, |\widetilde{\psi}_{\rho,\sigma}\rangle}). \end{aligned}$$

Note that $\sum_{\rho,\sigma} p_{\rho,\sigma} = 1$. In other words, the winning probability of $\widetilde{\mathcal{S}}$ is a convex combination of the winning probabilities of irreducible strategies $\mathcal{S}_{I\otimes\rho, I\otimes\sigma, |\widetilde{\psi}_{\rho,\sigma}\rangle}$. It is easily verified that $\nu(\mathcal{G}, \mathcal{S}_{I\otimes\rho, I\otimes\sigma, |\widetilde{\psi}_{\rho,\sigma}\rangle}) \leq \nu(\mathcal{G}, \rho, \sigma)$. By assumption of the lemma $\nu(\mathcal{G}, \rho, \sigma) < \nu^*(\mathcal{G})$ except when $(\rho, \sigma) = (\bar{\rho}, \bar{\sigma})$. Now since $\widetilde{\mathcal{S}}$ is an optimal strategy, we have

$$p_{\rho,\sigma} = \begin{cases} 1 & (\rho, \sigma) = (\bar{\rho}, \bar{\sigma}), \\ 0 & \text{otherwise.} \end{cases}$$

Therefore $\nu(\mathcal{G}, \widetilde{\mathcal{S}}) = \nu(\mathcal{G}, \mathcal{S}_{I\otimes\rho, I\otimes\sigma, |\widetilde{\psi}_{\rho,\sigma}\rangle})$ and hence $\mathcal{S}_{I\otimes\bar{\rho}, I\otimes\bar{\sigma}, |\widetilde{\psi}_{\bar{\rho},\bar{\sigma}}\rangle}$ is an optimal strategy. From the assumption of the lemma ,$|\psi\rangle$ is the unique state optimizing the strategy induced by $(\bar{\rho}, \bar{\sigma})$. Therefore $|\widetilde{\psi}_{\bar{\rho},\bar{\sigma}}\rangle = |\text{junk}'\rangle|\psi\rangle$ where both $|\text{junk}'\rangle$ and $|\psi\rangle$ are shared between Alice and Bob such that $|\text{junk}'\rangle$ is the state of the register upon which the identities of Alice and Bob in the operators $(I \otimes \rho)_A \otimes (I \otimes \sigma)_B$ are applied. In summary

$$|\widetilde{\psi}_{\rho,\sigma}\rangle = \begin{cases} |\text{junk}'\rangle|\psi\rangle & (\rho, \sigma) = (\bar{\rho}, \bar{\sigma}), \\ 0 & \text{otherwise.} \end{cases} \tag{2.2.7}$$

Now using (2.2.5), it follows that

$$\widetilde{A}_i \otimes V_B|\widetilde{\psi}\rangle = V_A^* g_A(P_i) V_A \otimes V_B|\widetilde{\psi}\rangle,$$

from which

$$V_A\widetilde{A}_i \otimes V_B|\widetilde{\psi}\rangle = V_A V_A^* g_A(P_i) V_A \otimes V_B|\widetilde{\psi}\rangle.$$

Since $V_A V_A^*$ is a projection and $V_A\widetilde{A}_i \otimes V_B|\widetilde{\psi}\rangle$ and $g_A(P_i)V_A \otimes V_B|\widetilde{\psi}\rangle$ are both unit vectors, it holds that

$$\begin{aligned} V_A\widetilde{A}_i \otimes V_B|\widetilde{\psi}\rangle &= g_A(P_i)V_A \otimes V_B|\widetilde{\psi}\rangle \\ &= \bigoplus_{\rho,\sigma} (I_{d_A d_\rho} \otimes \rho(P_i)) \otimes I_{d_B d_\sigma^2}|\widetilde{\psi}_{\rho,\sigma}\rangle \\ &= \big(|\text{junk}'\rangle\bar{\rho}(P_i) \otimes I_{d_{\bar{\sigma}}}|\psi\rangle\big) \oplus_{(\rho,\sigma)\neq(\bar{\rho},\bar{\sigma})} 0_{d_A d_\rho^2 d_B d_\sigma^2} \\ &= |\text{junk}\rangle\bar{\rho}(P_i) \otimes I_{d_{\bar{\sigma}}}|\psi\rangle, \end{aligned}$$

where the third equality follows from (2.2.7), and in the fourth equality $|\text{junk}\rangle = |\text{junk}'\rangle \oplus 0$ where $0 \in \mathbb{C}^{d_A d_B(\frac{|G_A||G_B|}{d_{\bar{\rho}} d_{\bar{\sigma}}} - d_{\bar{\rho}} d_{\bar{\sigma}})}$. Note that $d_A d_B(\frac{|G_A||G_B|}{d_{\bar{\rho}} d_{\bar{\sigma}}} - d_{\bar{\rho}} d_{\bar{\sigma}})$ is a positive integer because the degree of an irreducible representation divides the order of the group. □

Corollary 2.2.5. *If in addition to the assumptions of Lemma 2.2.4, it holds that for every optimal strategy* $\widetilde{\mathcal{S}} = (\{\widetilde{A}_i\}, \{\widetilde{B}_j\}, |\widetilde{\psi}\rangle)$*,* $f_A^{\widetilde{\mathcal{S}}}$ *and* $f_B^{\widetilde{\mathcal{S}}}$ *are* $|\widetilde{\psi}\rangle$*-representations, then* $\mathcal{G}$ *is a self-test for the strategy* $\mathcal{S}_{\bar{\rho},\bar{\sigma},|\psi\rangle}$*.*

Note that all these results can be stated robustly using the notion of $(\varepsilon, |\psi\rangle)$-representation, but in this paper we focus our attention on exact rigidity. In this paper we use SOS to obtain the extra assumption of Corollary 2.2.5 as seen in Sections 2.6 and 2.7.

2.3 A generalization of CHSH

The CHSH game can also be viewed as an LCS game where the linear system, over multiplicative $\mathbb{Z}_2$, is given by

$$x_0x_1 = 1,$$
$$x_0x_1 = -1.$$

The CHSH viewed as an LCS is first considered in [67]. We generalize this to a game $\mathcal{G}_n$ over $\mathbb{Z}_n$ for each $n \geq 2$

$$x_0x_1 = 1,$$
$$x_0x_1 = \omega_n.$$

As is the case for $\mathcal{G}_2 = CHSH$, the classical value of $\mathcal{G}_n$ is easily seen to be 0.75. In Section 2.4, we exhibit quantum advantage by presenting a strategy $\mathcal{S}_n$ showing that $\nu^*(\mathcal{G}_n) \geq \nu(\mathcal{G}_n, \mathcal{S}_n) = \frac{1}{2} + \frac{1}{2n\sin\left(\frac{\pi}{2n}\right)} > \frac{1}{2} + \frac{1}{\pi} \approx 0.81$. In Section 2.5, we present the group G_n generated by the operators in $\mathcal{S}_n$. In Section 2.7, we show that $\mathcal{G}_3$ is a self-test, and conjecture that this is true for all $n \geq 2$.

As defined in the preliminaries, conventionally, in an LCS game, Alice has to respond with an assignment to all variables in her equation. It is in Alice's best interest to always respond with a satisfying assignment. Therefore, the referee could always determine Alice's assignment to x_1

from her assignment to x_0. Hence, without loss of generality, in our games, Alice only responds with an assignment to x_0.

Formally $\mathcal{G}_n = ([2],[2],\mathbb{Z}_n,\mathbb{Z}_n,\pi,V)$ where $\mathbb{Z}_n = \{1,\omega_n,\ldots,\omega_n^{n-1}\}$, π is the uniform distribution on $[2]\times[2]$, and

$$\begin{aligned} V(0,0,a,b) = 1 &\iff a = b, \\ V(0,1,a,b) = 1 &\iff ab = 1, \\ V(1,0,a,b) = 1 &\iff a = b, \\ V(1,1,a,b) = 1 &\iff ab = \omega_n. \end{aligned}$$

Consider the quantum strategy $\mathcal{S}$ given by the state $|\psi\rangle$, and projective measurements $\{E_{0,a}\}_{a\in[n]}$ and $\{E_{1,a}\}_{a\in[n]}$ for Alice, and $\{F_{0,b}\}_{b\in[n]}$ and $\{F_{1,b}\}_{b\in[n]}$ for Bob. Note that in our measurement systems, we identify outcome $a \in [n]$ with answer $\omega_n^a \in \mathbb{Z}_n$. As done in the preliminaries, define the generalized observables $A_0 = \sum_{i=0}^{n-1}\omega_n^i E_{0,i}, A_1 = \sum_{i=0}^{n-1}\omega_n^i E_{1,i}, B_0 = \sum_{i=0}^{n-1}\omega_n^i F_{0,i}, B_1 = \sum_{i=0}^{n-1}\omega_n^i F_{1,i}$. We derive an expression for the winning probability of this strategy in terms of the these generalized observables. We do so by introducing the bias operator

$$\mathcal{B}_n = \mathcal{B}_n(A_0,A_1,B_0,B_1) = \sum_{i=1}^{n-1} A_0^i B_0^{-i} + A_0^i B_1^i + A_1^i B_0^{-i} + \omega_n^{-i} A_1^i B_1^i,$$

in which we dropped the tensor product symbol between Alice and Bob's operators.

Proposition 2.3.1. *Given the strategy $\mathcal{S}$ above, it holds that $v\left(\mathcal{G}_n,\mathcal{S}\right) = \frac{1}{4n}\langle\psi|\mathcal{B}_n|\psi\rangle + \frac{1}{n}$.*

Proof.

$$\begin{aligned}
\mathcal{B}_n + 4I &= \sum_{i=0}^{n-1} A_0^i B_0^{-i} + A_0^i B_1^i + A_1^i B_0^{-i} + \omega_n^{-i} A_1^i B_1^i \\
&= \sum_{i=0}^{n-1} \sum_{a,b=0}^{n-1} \omega_n^{i(a-b)} E_{0,a} F_{0,b} + \omega_n^{i(a+b)} E_{0,a} F_{1,b} + \omega_n^{i(a-b)} E_{1,a} F_{0,b} + \omega_n^{i(a+b-1)} E_{1,a} F_{1,b} \\
&= \sum_{a,b=0}^{n-1} \sum_{i=0}^{n-1} \omega_n^{i(a-b)} E_{0,a} F_{0,b} + \omega_n^{i(a+b)} E_{0,a} F_{1,b} + \omega_n^{i(a-b)} E_{1,a} F_{0,b} + \omega_n^{i(a+b-1)} E_{1,a} F_{1,b} \\
&= n \sum_{a=0}^{n-1} E_{0,a} F_{0,a} + E_{0,a} F_{1,-a} + E_{1,a} F_{0,a} + E_{1,a} F_{1,1-a}
\end{aligned}$$

in which in the last equality we used the identity $1 + \omega_n + \ldots + \omega_n^{n-1} = 0$. Also note that in $F_{1,-a}$ and $F_{1,1-a}$ second indices should be read mod n. Finally notice that

$$\nu(\mathcal{G}, \mathcal{S}) = \frac{1}{4} \langle \psi | \left(\sum_{a=0}^{n-1} E_{0,a} F_{0,a} + E_{0,a} F_{1,-a} + E_{1,a} F_{0,a} + E_{1,a} F_{1,1-a} \right) | \psi \rangle.$$

□

2.4 Strategies for $\mathcal{G}_n$

In this section, we present quantum strategies $\mathcal{S}_n$ for $\mathcal{G}_n$ games. In Section 2.4.2, we show that $\nu(\mathcal{G}_n, \mathcal{S}_n) = \frac{1}{2} + \frac{1}{2n \sin\left(\frac{\pi}{2n}\right)}$ and that this value approaches $\frac{1}{2} + \frac{1}{\pi}$ from above as n tends to infinity. This lower bounds the quantum value $\nu^*(\mathcal{G}_n)$, and proves that these games exhibit quantum advantage with a constant gap $> \frac{1}{\pi} - \frac{1}{4}$. We also show that the states in these strategies have full-Schmidt rank. Furthermore the states tend to the maximally entangled state as $n \to \infty$.

We conjecture that $\mathcal{S}_n$ are optimal and that the games $\mathcal{G}_n$ are self-tests for $\mathcal{S}_n$. In Section 2.7, we prove this for $n = 3$. Using the NPA hierarchy, we verify the optimality numerically up to $n = 7$. If the self-testing conjecture is true, we have a family of games with one bit questions and $\log(n)$ bits answers, that self-test entangled states of local dimension n for any n.

2.4.1 Definition of the strategy

Let $\sigma_n = (0\,1\,2\,\ldots\,n-1) \in S_n$ denote the cycle permutation that sends i to $i+1 \bmod n$. Let $z_n = \omega_n^{1/4} = e^{i\pi/2n}$. Let $D_{n,j} = I_n - 2e_j e_j^*$ be the diagonal matrix with -1 in the (j,j) entry, and 1 everywhere else in the diagonal. Then let $D_{n,S} := \prod_{j\in S} D_{n,j}$, where $S \subset [n]$. Finally, let X_n be the shift operator (also known as the generalized Pauli X), i.e., $X_n e_i = e_{\sigma_n(i)}$. For convenience, we shall often drop the n subscript when the dimension is clear from context, and so just refer to $z_n, D_{n,j}, D_{n,S}, X_n$ as z, D_j, D_S, X, respectively.

Let $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^n$. Then Alice and Bob's shared state in $\mathcal{S}_n$ is defined to be

$$|\psi_n\rangle = \frac{1}{\gamma_n}\sum_{i=0}^{n-1}(1 - z^{n+2i+1})|\sigma^i(0), \sigma^{-i}(0)\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B,$$

where $\gamma_n = \sqrt{2n + \frac{2}{\sin(\frac{\pi}{2n})}}$ is the normalization factor. The generalized observables in $\mathcal{S}_n$ are

$$\begin{aligned} A_0 &= X \\ A_1 &= z^2 D_0 X \\ B_0 &= X \\ B_1 &= z^2 D_0 X^*. \end{aligned}$$

Example 2.4.1. In $\mathcal{S}_2$, Alice and Bob's observables are

$$A_0 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_1 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$
$$B_0 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B_1 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

and their entangled state is

$$|\psi_2\rangle = \frac{1}{\sqrt{4+2\sqrt{2}}}\left(\left(1+\frac{1-i}{\sqrt{2}}\right)|00\rangle - \left(1+\frac{1+i}{\sqrt{2}}\right)|11\rangle\right).$$

One can verify that this indeed give us the quantum value for CHSH $\frac{1}{2}+\frac{\sqrt{2}}{4}$.

Example 2.4.2. In $\mathcal{S}_3$, Alice and Bob's observables are

$$A_0 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & -z^2 \\ z^2 & 0 & 0 \\ 0 & z^2 & 0 \end{pmatrix},$$

$$B_0 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 0 & -z^2 & 0 \\ 0 & 0 & z^2 \\ z^2 & 0 & 0 \end{pmatrix},$$

with the entangled state

$$|\psi_3\rangle = \frac{1}{\sqrt{10}}\left((1-z^4)|00\rangle + 2|12\rangle + (1+z^2)|21\rangle\right).$$

One can compute that $\langle\psi|\mathcal{B}_3|\psi\rangle = 6$. Hence, by Proposition 2.3.1, we have $v^*(\mathcal{G}_3) \geq \frac{5}{6}$.

2.4.2 Analysis of the strategy

In this section, we prove that $\mathcal{S}_n$ is a quantum strategy and calculate its winning probability. We then prove that the entanglement entropy of $|\psi_n\rangle$ approaches the maximum entropy as n tends to infinity.

Proposition 2.4.3. *For $n \in \mathbb{N}$, it holds that $\sum_{j=0}^{n-1} z_n^{2j+n+1} = \sum_{j=0}^{n-1} z_n^{-(2j+n+1)}$.*

Proof. A direct computation gives

$$\sum_{j=0}^{n-1} z^{2j+n+1} = \frac{2z^{n+1}}{1-z^2} = \frac{2z^{-n-1}}{1-z^{-2}} = \sum_{j=0}^{n-1} z^{-(2j+n+1)},$$

where we have used the fact that $z^{2n} = -1$. □

Proposition 2.4.4. *For $n \in \mathbb{N}$, it holds that* $\sum_{j=0}^{n-1} z_n^{2j+n+1} = -\frac{1}{\sin\left(\frac{\pi}{2n}\right)}$.

Proof. We handle the even and odd case separately, and in both cases we use the well-known identity for the Dirichlet kernel mentioned in preliminaries. For odd n

$$
\begin{aligned}
-\sum_{j=0}^{n-1} z^{2j+n+1} &= \sum_{j=0}^{n-1} z^{2j-(n-1)} = \sum_{j=-\frac{n-1}{2}}^{\frac{n-1}{2}} z^{2j} = \sum_{j=-\frac{n-1}{2}}^{\frac{n-1}{2}} e^{\frac{\pi i j}{n}} \\
&= 2\pi \mathcal{D}_{\frac{n-1}{2}}\left(\frac{\pi}{n}\right) = \frac{\sin\left(\left(\frac{n-1}{2} + \frac{1}{2}\right)\frac{\pi}{n}\right)}{\sin\left(\frac{\pi}{2n}\right)} = \frac{1}{\sin\left(\frac{\pi}{2n}\right)}.
\end{aligned}
$$

For even n

$$
\begin{aligned}
-\sum_{j=0}^{n-1} z^{2j+n+1} &= z\sum_{j=0}^{n} z^{2j-n} - z^{n+1} = z\sum_{j=-\frac{n}{2}}^{\frac{n}{2}} z^{2j} - z^{n+1} = 2\pi z \mathcal{D}_{\frac{n}{2}}\left(\frac{\pi}{n}\right) - z^{n+1} \\
&= \left(\cos\left(\frac{\pi}{2n}\right) + i\sin\left(\frac{\pi}{2n}\right)\right)\frac{\sin\left(\left(\frac{n}{2} + \frac{1}{2}\right)\frac{\pi}{n}\right)}{\sin\left(\frac{\pi}{2n}\right)} - i\left(\cos\left(\frac{\pi}{2n}\right) + i\sin\left(\frac{\pi}{2n}\right)\right) \\
&= \frac{\cos^2\left(\frac{\pi}{2n}\right) + \sin^2\left(\frac{\pi}{2n}\right)}{\sin\left(\frac{\pi}{2n}\right)} = \frac{1}{\sin\left(\frac{\pi}{2n}\right)}.
\end{aligned}
$$

□

Now let's observe a commutation relation between D_j and X^k.

Proposition 2.4.5. $X^i D_j = D_{\sigma^i(j)} X^i$, *for all* $i, j \in [n]$.

Proof. It suffices to prove $XD_j = D_{\sigma(j)}X$. We show this by verifying $XD_j e_k = D_{\sigma(j)}Xe_k$ for all $k \in [n]$.

$$
XD_j e_k = (-1)^{\delta_{j,k}} e_{\sigma(k)} = (-1)^{\delta_{\sigma(j),\sigma(k)}} e_{\sigma(k)} = D_{\sigma(j)} X e_k
$$

□

Now we prove the strategy defined in section 2.4.1 is a valid quantum strategy.

Proposition 2.4.6. *A_0, A_1, B_0, B_1 are order-n generalized observables and $|\psi_n\rangle$ is a unit vector.*

Proof. Observe that

$$A_0^n = B_0^n = X^n = I,$$

also

$$A_1^n = (z^2 D_0 X)^n = z^{2n} D_{\{0,\sigma^1(0),\ldots,\sigma^{n-1}(0)\}} X^n = (-1)(-I)I = I.$$

Similarly,

$$B_1^n = (z^2 D_0 X^*)^n = z^{2n} (X^*)^n D_{\{0,\sigma^1(0),\ldots,\sigma^{n-1}(0)\}} = (-1)I(-I) = I.$$

It is an easy observation that these operators are also unitary. To see that $|\psi_n\rangle$ is a unit vector write

$$\begin{aligned}
\sum_{i=0}^{n-1} |1 - z^{n+2i+1}|^2 &= \sum_{i=0}^{n-1} \left(1 - \cos\left(\frac{\pi(n+2i+1)}{2n}\right)\right)^2 + \sin\left(\frac{\pi(n+2i+1)}{2n}\right)^2 \\
&= \sum_{i=0}^{n-1} 2\left(1 - \cos\left(\frac{\pi(n+2i+1)}{2n}\right)\right) \\
&= 2n - \sum_{i=0}^{n-1} \Re(z^{n+2i+1}) \\
&= 2n + \frac{2}{\sin(\pi/2n)} \\
&= \gamma_n^2,
\end{aligned}$$

where we have used Proposition 2.4.4 in the third equality.

□

Lemma 2.4.7. *The entangled state $|\psi\rangle$ is an eigenvector for the bias $\mathcal{B} = \sum_{j=1}^{n-1} A_0^j B_0^{-j} + A_0^j B_1^j + A_1^j B_0^{-j} + z^{-4j} A_1^j B_1^j$ with eigenvalue $2n - 4 + \frac{2}{\sin(\frac{\pi}{2n})}$.*

Proof. For the sake of brevity, we drop the normalization factor γ_n in the derivation below, and let $|\varphi\rangle = \gamma_n |\psi_n\rangle$. We write

$$\begin{aligned}\mathcal{B}|\varphi\rangle &= \left(\sum_{j=1}^{n-1} A_0^j \otimes B_0^{-j} + A_0^j \otimes B_1^j + A_1^j \otimes B_0^{-j} + z^{-4j} A_1^j \otimes B_1^j\right)|\varphi\rangle \\ &= \left(\sum_{j=1}^{n-1} (X \otimes X^*)^j + z^{2j}\,(X \otimes D_0X^*)^j + z^{2j}(D_0X \otimes X^*)^j + (D_0X \otimes D_0X^*)^j\right)|\varphi\rangle.\end{aligned}$$

Lemma 2.4.8. $(X \otimes D_0X^*)^j\,|\varphi\rangle = (D_0X \otimes X^*)^j|\varphi\rangle$ *and* $(X \otimes X^*)^j\,|\varphi\rangle = (D_0X \otimes D_0X^*)^j|\varphi\rangle$.

Proof. It suffices to show these identities for $j = 1$ on states $|\sigma^i(0), \sigma^{-i}(0)\rangle$, for all i, in place of $|\varphi\rangle$. The result then follows by simple induction. In other words, we prove

$$\begin{aligned}(X \otimes D_0X^*)\,|\sigma^i(0), \sigma^{-i}(0)\rangle &= (D_0X \otimes X^*)|\sigma^i(0), \sigma^{-i}(0)\rangle, \\ (X \otimes X^*)\,|\sigma^i(0), \sigma^{-i}(0)\rangle &= (D_0X \otimes D_0X^*)|\sigma^i(0), \sigma^{-i}(0)\rangle.\end{aligned}$$

Note that $I \otimes D_0|\sigma^{i+1}(0), \sigma^{-i-1}(0)\rangle = D_0 \otimes I|\sigma^{i+1}(0), \sigma^{-i-1}(0)\rangle$ since $-i - 1 = 0 \bmod n$ iff $i + 1 = 0 \bmod n$. Therefore

$$\begin{aligned}(X \otimes D_0X^*)\,|\sigma^i(0), \sigma^{-i}(0)\rangle &= (I \otimes D_0)\,|\sigma^{i+1}(0), \sigma^{-i-1}(0)\rangle \\ &= (D_0 \otimes I)\,|\sigma^{i+1}(0), \sigma^{-i-1}(0)\rangle \\ &= (D_0X \otimes X^*)|\sigma^i(0), \sigma^{-i}(0)\rangle.\end{aligned}$$

The other identity follows similarly. □

Now we write

$$\begin{aligned}
\mathcal{B}|\varphi\rangle &= 2\left(\sum_{j=1}^{n-1}(X\otimes X^*)^j + z^{2j}(D_0 X\otimes X^*)^j\right)|\varphi\rangle \\
&= 2\sum_{j=1}^{n-1}\left(1+z^{2j}(D_{[j]}\otimes I)\right)(X\otimes X^*)^j|\varphi\rangle \\
&= 2\sum_{j=1}^{n-1}\sum_{i=0}^{n-1}\left(1-z^{2i+n+1}\right)\left(1+z^{2j}(D_{[j]}\otimes I)\right)(X\otimes X^*)^j|\sigma^i(0),\sigma^{-i}(0)\rangle \\
&= 2\sum_{j=1}^{n-1}\sum_{i=0}^{n-1}\left(1-z^{2i+n+1}\right)\left(1+z^{2j}(D_{[j]}\otimes I)\right)|\sigma^{i+j}(0),\sigma^{-(i+j)}(0)\rangle,
\end{aligned}$$

where in the second equality we use Proposition 2.4.5, and in the third equality we just expanded $|\varphi\rangle$. Note that

$$(D_{[j]}\otimes I)|\sigma^{i+j}(0),\sigma^{-(i+j)}(0)\rangle = \begin{cases} -|\sigma^{i+j}(0),\sigma^{-(i+j)}(0)\rangle & i\in[n-j,n-1], \\ |\sigma^{i+j}(0),\sigma^{-(i+j)}(0)\rangle & i\in[0,n-j-1], \end{cases}$$

and we use this to split the sum

$$\begin{aligned}
\mathcal{B}|\varphi\rangle = 2\sum_{j=1}^{n-1}\Bigg(&\sum_{i=0}^{n-j-1}\left(1-z^{2i+n+1}\right)\left(1+z^{2j}\right)|\sigma^{i+j}(0),\sigma^{-(i+j)}(0)\rangle \\
&+\sum_{i=n-j}^{n-1}\left(1-z^{2i+n+1}\right)\left(1-z^{2j}\right)|\sigma^{i+j}(0),\sigma^{-(i+j)}(0)\rangle\Bigg) \\
= 2\sum_{i=0}^{n-1}\Bigg(&\sum_{j=1}^{n-i-1}\left(1-z^{2i+n+1}\right)\left(1+z^{2j}\right)|\sigma^{i+j}(0),\sigma^{-(i+j)}(0)\rangle \\
&+\sum_{j=n-i}^{n-1}\left(1-z^{2i+n+1}\right)\left(1-z^{2j}\right)|\sigma^{i+j}(0),\sigma^{-(i+j)}(0)\rangle\Bigg),
\end{aligned}$$

and make a change of variable $r = i + j$ to get

$$\begin{aligned}\mathcal{B}|\varphi\rangle = 2\sum_{i=0}^{n-1}\Bigg(&\sum_{r=i+1}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)|\sigma^r(0), \sigma^{-r}(0)\rangle \\ &+ \sum_{r=n}^{n+i-1}\left(1 - z^{2i+n+1}\right)\left(1 - z^{2(r-i)}\right)|\sigma^r(0), \sigma^{-r}(0)\rangle\Bigg).\end{aligned}$$

We have $z^{2(r-i)} = z^{2(r-n+n-i)} = z^{2n}z^{2(r-n-i)} = -z^{2(r-n-i)}$ and $\sigma^r(0) = \sigma^{r+n}(0)$, so by another change of variable in the second sum where we are summing over $r = [n, n+i-1]$ we obtain

$$\begin{aligned}\mathcal{B}|\varphi\rangle &= 2\sum_{i=0}^{n-1}\Bigg(\sum_{r=i+1}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)|\sigma^r(0), \sigma^{-r}(0)\rangle \\ &\qquad + \sum_{r=0}^{i-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)|\sigma^r(0), \sigma^{-r}(0)\rangle\Bigg) \\ &= 2\sum_{i=0}^{n-1}\left(\sum_{r=0}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)|\sigma^r(0)\sigma^{-r}(0)\rangle - 2\left(1 - z^{2i+n+1}\right)|\sigma^i(0)\sigma^{-i}(0)\rangle\right) \\ &= 2\sum_{i=0}^{n-1}\left(\sum_{r=0}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)|\sigma^r(0)\sigma^{-r}(0)\rangle\right) - 4|\varphi\rangle \\ &= 2\sum_{r=0}^{n-1}|\sigma^r(0)\sigma^{-r}(0)\rangle\left(\sum_{i=0}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)\right) - 4|\varphi\rangle.\end{aligned}$$

We also have

$$\begin{aligned}\sum_{i=0}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right) &= \sum_{i=0}^{n-1} 1 - z^{2r+n+1} + z^{2(r-i)} - z^{2i+n+1} \\ &= \sum_{i=0}^{n-1} 1 - z^{2r+n+1} + z^{2(r-i)} - z^{-(2i+n+1)} \\ &= (1 - z^{2r+n+1})\sum_{i=0}^{n-1} 1 - z^{-(2i+n+1)} \\ &= \left(n + \frac{1}{\sin(\frac{\pi}{2n})}\right)(1 - z^{2r+n+1}),\end{aligned}$$

where in the second and last equality we used Propositions 2.4.3 and 2.4.4, respectively. Putting these together, we obtain

$$
\begin{aligned}
\mathcal{B}|\varphi\rangle &= 2\left(n+\frac{1}{\sin(\frac{\pi}{2n})}\right)\sum_{r=0}^{n-1}(1-z^{2r+n+1})|\sigma^{r}(0)\sigma^{-r}(0)\rangle - 4|\varphi\rangle \\
&= \left(2n-4+\frac{2}{\sin(\frac{\pi}{2n})}\right)|\varphi\rangle.
\end{aligned}
$$

□

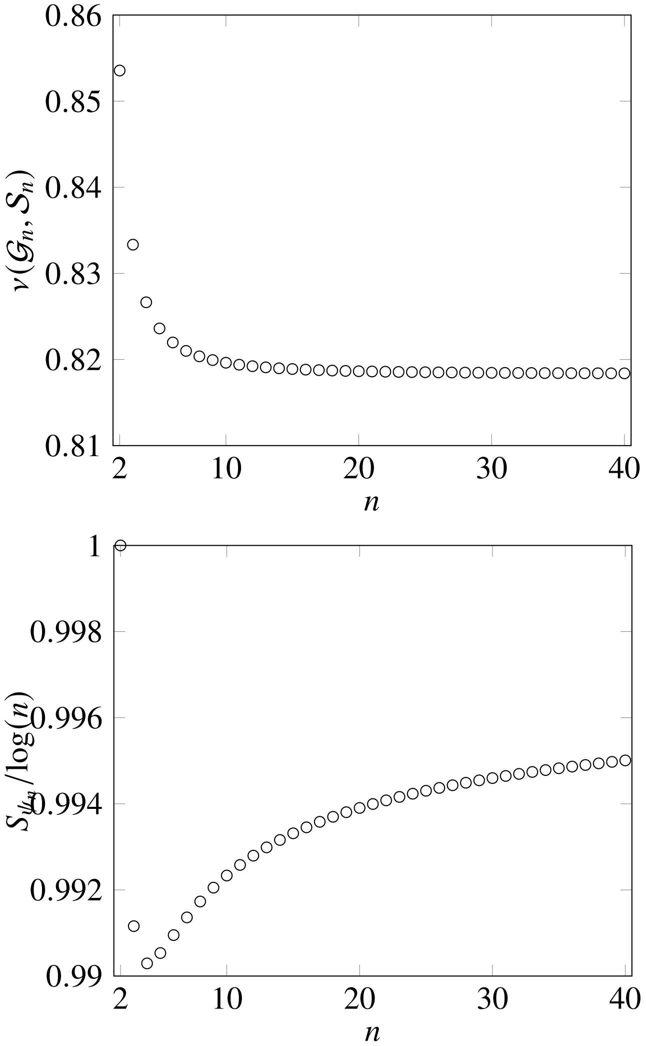

Figure 2.2: The figure on the left illustrates the fast convergence rate of the winning probabilities as they approach the limit $1/2 + 1/\pi$. The figure on the right illustrates the ratio of the entanglement entropy to the maximum entanglement entropy of the states for $n \leq 40$.

Next we calculate $\nu(\mathcal{G}_n, \mathcal{S}_n)$, its limit as n grows and the entanglement entropy of states $|\psi_n\rangle$.

See Figure 2.2.

Theorem 2.4.9. $\nu(\mathcal{G}_n, \mathcal{S}_n) = \frac{1}{2} + \frac{1}{2n\sin\left(\frac{\pi}{2n}\right)}$.

Proof.

$$\begin{aligned}
\nu(\mathcal{G}_n, \mathcal{S}_n) &= \frac{1}{4n}\langle\psi|\mathcal{B}|\psi\rangle + \frac{1}{n} \\
&= \frac{1}{4n}\langle\psi|\left(2n - 4 + \frac{2}{\sin\left(\frac{\pi}{2n}\right)}\right)|\psi\rangle + \frac{1}{n} \\
&= \frac{1}{4n}\left(2n - 4 + \frac{2}{\sin\left(\frac{\pi}{2n}\right)}\right) + \frac{1}{n} \\
&= \frac{1}{2} + \frac{1}{2n\sin\left(\frac{\pi}{2n}\right)}.
\end{aligned}$$

□

Theorem 2.4.10. *The following hold*

1. $\lim_{n\to\infty} \nu(\mathcal{G}_n, \mathcal{S}_n) = 1/2 + 1/\pi$.
2. $\nu(\mathcal{G}_n, \mathcal{S}_n)$ *is a strictly decreasing function.*
3. *The games $\mathcal{G}_n$ exhibit quantum advantage, i.e., for $n > 1$*

$$\nu^*(\mathcal{G}_n) > 1/2 + 1/\pi > 3/4 = \nu(\mathcal{G}_n).$$

Proof. For the first statement, it suffices to see that

$$\lim_{x\to\infty} \frac{1}{2x\sin\left(\frac{\pi}{2x}\right)} = \lim_{x\to\infty} \frac{\frac{1}{2x}}{\sin\left(\frac{\pi}{2x}\right)} = \lim_{x\to\infty} \frac{\frac{-1}{2x^2}}{-\frac{\pi\cos\left(\frac{\pi}{2x}\right)}{2x^2}} = \frac{1}{\pi}.$$

For the second statement, we show that the function $f(x) = 2x\sin(\pi/2x)$ is strictly increasing for $x \geq 1$. We have $f'(x) = 2\sin(\pi/2x) - \pi\cos(\pi/2x)/x$. Then $f'(x) > 0$ is equivalent to $\tan(\pi/2x) \geq \pi/2x$. This latter statement is true for all $x \geq 1$. The third statement follows from the first two. □

Theorem 2.4.11. *States $|\psi_n\rangle$ have full Schmidt rank and the ratio of entanglement entropy to maximum entangled entropy, i.e., $S_{\psi_n}/\log(n)$ approaches 1 as $n \to \infty$.*

Proof. Recall that

$$|\psi_n\rangle = \frac{1}{\gamma_n}\sum_{i=0}^{n-1}\left(1 - z^{2i+n+1}\right)|\sigma^i(0), \sigma^{-i}(0)\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B.$$

Let $|i_A\rangle = \frac{1-z^{2i+n+1}}{\left\|1-z^{2i+n+1}\right\|}|\sigma^i(0)\rangle$ and $|i_B\rangle = |\sigma^{-i}(0)\rangle$. Clearly $\{i_A\}_i$ and $\{i_B\}_i$ are orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The Schmidt decomposition is now given by

$$|\psi_n\rangle = \frac{1}{\gamma_n}\sum_{i=0}^{n-1}\left\|1 - z^{2i+n+1}\right\||i_A i_B\rangle.$$

To calculate the limit of $S_{\psi_n}/\log(n)$ first note that

$$\begin{aligned}
\frac{S_{\psi_n}}{\log(n)} &= -\frac{\sum_{i=0}^{n-1}\left\|1 - z^{2i+n+1}\right\|^2 \log\frac{\left\|1-z^{2i+n+1}\right\|^2}{\gamma_n^2}}{\gamma_n^2\log(n)} \\
&= -\frac{\sum_{i=0}^{n-1}\left\|1 - z^{2i+n+1}\right\|^2\left(\log\left\|1 - z^{2i+n+1}\right\|^2 - \log\gamma_n^2\right)}{\gamma_n^2\log(n)} \\
&\geq -\frac{\log(4)\sum_{i=0}^{n-1}\left\|1 - z^{2i+n+1}\right\|^2}{\gamma_n^2\log(n)} + \frac{\log\gamma_n^2\sum_{i=0}^{n-1}\left\|1 - z^{2i+n+1}\right\|^2}{\gamma_n^2\log(n)} \\
&= -\frac{\log(4)}{\log(n)} + \frac{\log\gamma_n^2}{\log(n)}
\end{aligned}$$

where for the inequality we used the fact that $\left\|1 - z^{2i+n+1}\right\| \leq 2$, and for the last equality we used the identity $\gamma_n^2 = \sum_{i=0}^{n-1}\left\|1 - z^{2i+n+1}\right\|^2$. So it holds that

$$-\frac{\log(4)}{\log(n)} + \frac{\log\gamma_n^2}{\log(n)} \leq \frac{S_{\psi_n}}{\log(n)} \leq 1.$$

By simple calculus $\lim_{n\to\infty}\frac{\log\gamma_n^2}{\log(n)} - \frac{\log(4)}{\log(n)} = 1$. Therefore by squeeze theorem $\lim_{n\to\infty}\frac{S_{\psi_n}}{\log(n)} = 1$.

□

2.5 Group structure of $\mathcal{S}_n$

Let $H_n = \langle A_0, A_1 \rangle$ be the group generated by Alice's observables in $\mathcal{S}_n$. Note that since $(A_1 A_0^*)^2 = z_n^4 I$, we could equivalently define $H_n = \langle A_0, A_1, z_n^4 I \rangle$. Also let

$$G_n = \left\langle P_0, P_1, J \mid P_0^n, P_1^n, J^n, [J, P_0], [J, P_1], J^i \left(P_0^i P_1^{-i}\right)^2 \text{ for } i = 1, 2, \ldots, \lfloor n/2 \rfloor \right\rangle.$$

In this section we show that $H_n \cong G_n$. So it also holds that H_n is a representation of G_n. We conjecture that $\mathcal{G}_n$ is a self-test for G_n, in the sense that every optimal strategy of $\mathcal{G}_n$ is a $|\psi\rangle$-representation of G_n. In Section 2.7, we prove this for $n = 3$.

Remark 2.5.1. Note that the relations $J^i \left(P_0^i P_1^{-i}\right)^2$ holds in G_n for all i.

The following lemma helps us develop a normal form for elements of G_n.

Lemma 2.5.2. *For all i, j, the elements $P_0^i P_1^{-i}$ and $P_0^j P_1^{-j}$ commute.*

Proof.

$$\begin{aligned}
\left(P_0^i P_1^{-i}\right)\left(P_0^j P_1^{-j}\right) &= J^{-i} P_1^i P_0^{-i} P_0^j P_1^{-j} \\
&= J^{-i} P_1^i P_0^{j-i} P_1^{-j} \\
&= J^{-i} P_1^i \left(P_0^{j-i} P_1^{-(j-i)}\right) P_1^{-i} \\
&= J^{-i-(j-i)} P_1^i P_1^{j-i} P_0^{-(j-i)} P_1^{-i} \\
&= J^{-j} \left(P_1^j P_0^{-j}\right)\left(P_0^i P_1^{-i}\right) \\
&= J^{-j} \left(J^j P_0^j P_1^{-j}\right)\left(P_0^i P_1^{-i}\right) \\
&= \left(P_0^j P_1^{-j}\right)\left(P_0^i P_1^{-i}\right).
\end{aligned}$$

□

Lemma 2.5.3. *For every $g \in G_n$ there exist $i, j \in [n]$ and $q_k \in \{0, 1\}$ for $k = 1, 2, \ldots, n-1$ such that*

$$g = J^i P_0^j \left(P_0 P_1^{-1}\right)^{q_1} \left(P_0^2 P_1^{-2}\right)^{q_2} \cdots \left(P_0^{n-1} P_1^{-(n-1)}\right)^{q_{n-1}}.$$

Proof. First note that J is central, therefore we can write g in G_n as

$$g = J^i P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_k},$$

for some $k \in \mathbb{N}$, $i \in [n]$, $j_l \in [n]$ where $l = 1, 2, \ldots, k$. Without loss of generality, let k be even. We perform the following sequence of manipulations

$$\begin{aligned}
g &= J^i P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_{k-2}} P_0^{j_{k-1}} P_1^{j_k} \\
&= J^i P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_{k-2}} P_0^{j_{k-1}} P_0^{j_k} \left(P_0^{-j_k} P_1^{j_k}\right) \\
&= J^i P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_{k-2}} P_1^{j_{k-1}+j_k} \left(P_1^{-(j_{k-1}+j_k)} P_0^{j_{k-1}+j_k}\right)\left(P_0^{-j_k} P_1^{j_k}\right) \\
&= J^{i-(j_{k-1}+j_k)} P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_{k-2}+j_{k-1}+j_k} \left(P_0^{-(j_{k-1}+j_k)} P_1^{j_{k-1}+j_k}\right)\left(P_0^{-j_k} P_1^{j_k}\right) \\
&= \cdots \\
&= J^{i-s} P_0^{-s_1} \left(P_0^{s_2} P_1^{-s_2}\right) \cdots \left(P_0^{s_{k-1}} P_1^{-s_{k-1}}\right)\left(P_0^{s_k} P_1^{-s_k}\right),
\end{aligned}$$

where $s_l = -\sum_{t=l}^{k} j_t$ and $s = -\sum_{t=1}^{(k-2)/2} s_{2t+1}$. Then we use the commutation relationship from lemma 2.5.2 to group the terms with the same P_0 and P_1 exponents, and use the relation $J^i(P_0^i P_1^{-i})^2$ to reduce each term to have an exponent of less than 1, introducing extra J terms as needed. Finally after reducing the exponents of J and P_0, knowing that they are all order n, we arrive at the desired form. □

Corollary 2.5.4. $|G_n| \leq n^2 2^{n-1}$ *for all* $n \in \mathbb{N}$.

Proof. Follows from lemma 2.5.3. □

Lemma 2.5.5. $|H_n| \geq n^2 2^{n-1}$ *for all* $n \in \mathbb{N}$.

Proof. We lower bound the order of the group H_n by exhibiting $n^2 2^{n-1}$ distinct elements in the group. We divide the proof into cases depending on the parity of n.

First note that $z^2 D_i \in H_n$ for all $i \in [n]$ since

$$z^{-4i} A_1^i A_0^{-i} A_1^{i+1} A_0^{-(i+1)} = z^{-4i} z^{2i} D_{[i]} X^i X^{-i} z^{2(i+1)} D_{[i+1]} X^{i+1} X^{-(i+1)} = z^2 D_i,$$

where in the first equality we use Proposition 2.4.5. This allows us to generate $z^2 D_{i_0} D_{i_1} \cdots D_{i_{k-1}}$ if k is odd via

$$z^{-4(k-1)/2}(z^2 D_{i_0})(z^2 D_{i_1}) \cdots (z^2 D_{i_{k-1}}) = z^2 D_{i_0} D_{i_1} \cdots D_{i_{k-1}}, \tag{1}$$

and $D_{i_0} D_{i_1} \cdots D_{i_{k-1}}$ if k is even by

$$z^{-4(k/2)}(z^2 D_{i_0})(z^2 D_{i_1}) \cdots (z^2 D_{i_{k-1}}) = D_{i_0} D_{i_1} \cdots D_{i_{k-1}}. \tag{2}$$

Let n be odd. From (2) we will be able to generate elements of the form $z^{4i} D_0^{q_0} D_1^{q_1} \cdots D_{n-1}^{q_{n-1}} X^j$ where there are an even number of nonzero q_k for $i, j \in [n]$. It should be clear that the elements with $i \neq i' \in \{0, 1, \ldots, (n-1)/2\}$ will be distinct. For $i > (n-1)/2$, we simply note that we can factor out a $z^{2n} = -1$ and so we get elements of the form $z^{4i'+2} D_0^{q_0} D_1^{q_1} \cdots D_{n-1}^{q_{n-1}} X^j$, where there are an odd number of nonzero q_k for $i' \in \{0, 1, \ldots, (n-3)/2\}$, $j \in [n]$. Each of these will be distinct from each other as, again, the powers of the nth root of unity will be distinct, and distinct from the previous case by the parity of the sign matrices. Therefore we are able to lower-bound $|C_n|$ by $n^2 2^{n-1}$.

If n is even, we will still be able to generate elements of the form $z^{4i} D_0^{q_0} D_1^{q_1} \cdots D_{n-1}^{q_{n-1}} X^j$ where there are an even number of nonzero q_k for $i, j \in [n]$. However, note that for $i > (n-2)/2$, we begin to generate duplicates. So from (1) we can generate elements of the form $z^{4i+2} D_0^{q_0} D_1^{q_1} \cdots D_{n-1}^{q_{n-1}} X^j$ for $i, j \in [n]$ and an odd number of nonzero q_k. These will be distinct from the previous elements by the parity of the sign matrices but again will begin to generate duplicates after $i > (n-2)/2$. Therefore we have the lower-bound of $\frac{n}{2} n 2^{n-1} + \frac{n}{2} n 2^{n-1} = n^2 2^{n-1}$ elements. □

Lemma 2.5.6. *There exists a surjective homomorphism $f : G_n \to H_n$.*

Proof. Let us define $f : \{J, P_0, P_1\} \to H_n$ by $f(J) = z^4 I, f(P_0) = A_0, f(P_1) = A_1$. We show that f can be extended to a homomorphism from G_n to H_n. Consider the formal extension $\widetilde{f}$ of f to the free group generated by $\{J, P_0, P_1\}$. We know from the theory of group presentations that f can be extended to a homomorphism if and only if $\widetilde{f}(r) = I$ for all relation r in the presentation of

G_n.

It is clear that $\widetilde{f}$ respects the first five relations of G_n. Now we check the last family of relations:

$$\begin{aligned}\widetilde{f}(J^i(P_0^iP_1^{-i})^2) &= z^{4i}(A_0^iA_1^{-i})^2\\ &= z^{4i}(X^iz^{-2i}(D_0X)^{-i})^2\\ &= (X^iX^{-i}D_{[i]})^2\\ &= D_{[i]}^2\\ &= I.\end{aligned}$$

The homomorphism f is surjective because A_0, A_1 generate the group H_n. □

Theorem 2.5.7. *$H_n \cong G_n$ for all $n \in \mathbb{N}$.*

Proof. Since f is surjective, then $n^2 2^{n-1} \leq |H_n| \leq |G_n| \leq n^2 2^{n-1}$. Thus $|H_n| = |G_n|$, so the homomorphism is also injective. □

Remark 2.5.8. What about the group generated by Bob's operators in $\mathcal{S}_n$? We can define

$$G'_n = \left\langle Q_0, Q_1, J \mid Q_0^n, Q_1^n, J^n, [J, Q_0], [J, Q_1], J^i\left(Q_0^{-i}Q_1^{-i}\right)^2 \text{ for } i = 1, 2, \ldots, \lfloor n/2 \rfloor \right\rangle.$$

and with a similar argument as in Theorem 2.5.7 show that $\langle B_0, B_1, z_n^4 I\rangle \cong G'_n$. It is now easily verified that the mapping $P_0 \mapsto Q_0^{-1}, P_1 \mapsto Q_1, J \mapsto J$ is an isomorphism between G_n and G'_n. So Alice and Bob's operator generate the same group, that is $\langle A_0, A_1, z_n^4 I\rangle = \langle B_0, B_1, z_n^4 I\rangle$. The latter fact could also be verified directly.

2.6 Sum of squares framework

In this paper, the sum of squares (SOS) proofs are used to demonstrate that certain non-commutative polynomials are positive semidefinite. We use this approach to upper bound the quantum value of non-local games and to establish rigidity. This approach has been used previously in the literature, e.g., [81, 70]. We illustrate the basics of this framework by going over the proof of optimality and rigidity of CHSH. At the end of this section, we extend this method to deal with the complexities of $\mathcal{G}_n$ and similar games.

By Proposition 2.3.1, the probability of winning $\mathcal{G}_2$ using a strategy consisting of a state $|\psi\rangle$ and observables A_0, A_1 for Alice and B_0, B_1 for Bob is given by the expression

$$\frac{1}{2} + \frac{1}{8}\langle\psi|(A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1)|\psi\rangle.$$

To prove $v^*(\mathcal{G}_2) = \frac{1}{2} + \frac{\sqrt{2}}{4}$, we just need to show that

$$2\sqrt{2}I - (A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1) \geq 0,$$

for any observables A_0, A_1, B_0, B_1. This immediately follows from the following SOS decomposition

$$2\sqrt{2}I - (A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1) = \frac{\sqrt{2}}{4}(A_0 + A_1 - \sqrt{2}B_0)^2 + \frac{\sqrt{2}}{4}(A_0 - A_1 - \sqrt{2}B_1)^2. \tag{2.6.1}$$

Next we use this SOS and the Gowers-Hatami theorem to establish that CHSH is a self-test for the strategy $\mathcal{S}_2$ given in Example 2.4.1. We learned in Section 2.5 that $A_0 = B_0 = \sigma_x$ and $A_1 = B_1 = \sigma_y$ generate

$$G_2 = \left\langle P_0, P_1, J \mid P_0^2, P_1^2, J^2, [J, P_0], [J, P_1], J\,(P_0P_1)^2 \right\rangle,$$

which is in fact the dihedral group D_4 (also known as the Weyl-Heisenberg group).

The strategy $\mathcal{S}_2$ gives a representation of D_4 as seen by the homomorphism $J \mapsto -I, P_0 \mapsto A_0$, and $P_1 \mapsto A_1$. Our first step in proving rigidity is to show that a weaker statement holds for any optimal strategy $(\{\widetilde{A}_0, \widetilde{A}_1\}, \{\widetilde{B}_0, \widetilde{B}_1\}, |\widetilde{\psi}\rangle)$ where $|\widetilde{\psi}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{H}_A = \mathbb{C}^{d_A}, \mathcal{H}_B = \mathbb{C}^{d_B}$. More precisely, we show that any optimal strategy gives rise to a $|\widetilde{\psi}\rangle$-representation. By optimality

$$\langle\widetilde{\psi}|(2\sqrt{2}I - (\widetilde{A}_0\widetilde{B}_0 + \widetilde{A}_0\widetilde{B}_1 + \widetilde{A}_1\widetilde{B}_0 - \widetilde{A}_1\widetilde{B}_1))|\widetilde{\psi}\rangle = 0.$$

Then by (2.6.1)

$$\begin{aligned}\widetilde{B}_0|\widetilde{\psi}\rangle &= \frac{1}{\sqrt{2}}(\widetilde{A}_0 + \widetilde{A}_1)|\widetilde{\psi}\rangle,\\ \widetilde{B}_1|\widetilde{\psi}\rangle &= \frac{1}{\sqrt{2}}(\widetilde{A}_0 - \widetilde{A}_1)|\widetilde{\psi}\rangle.\end{aligned}$$

These then let us derive the state-dependent anti-commutation relation

$$\begin{aligned}(\widetilde{B}_0\widetilde{B}_1 + \widetilde{B}_1\widetilde{B}_0)|\widetilde{\psi}\rangle &= \frac{1}{\sqrt{2}}(\widetilde{B}_0(\widetilde{A}_0 - \widetilde{A}_1) + \widetilde{B}_1(\widetilde{A}_0 + \widetilde{A}_1))|\widetilde{\psi}\rangle\\ &= \frac{1}{\sqrt{2}}((\widetilde{A}_0 - \widetilde{A}_1)\widetilde{B}_0 + (\widetilde{A}_0 + \widetilde{A}_1)\widetilde{B}_1)|\widetilde{\psi}\rangle\\ &= \frac{1}{2}((\widetilde{A}_0 - \widetilde{A}_1)(\widetilde{A}_0 + \widetilde{A}_1) + (\widetilde{A}_0 + \widetilde{A}_1)(\widetilde{A}_0 - \widetilde{A}_1))|\widetilde{\psi}\rangle\\ &= 0,\end{aligned}$$

where in the second equality we used the fact that Alice and Bob's operators commute. Similarly we have that

$$(\widetilde{A}_0\widetilde{A}_1 + \widetilde{A}_1\widetilde{A}_0)|\widetilde{\psi}\rangle = 0.$$

Define the functions $f_A : D_4 \to \mathrm{U}_{d_A}(\mathbb{C})$, $f_B : D_4 \to \mathrm{U}_{d_B}$ by

$$\begin{aligned}f_A(J^iP_0^jP_1^k) &= (-1)^i\widetilde{A}_0^j\widetilde{A}_1^k,\\ f_B(J^iP_0^jP_1^k) &= (-1)^i\widetilde{B}_0^j\widetilde{B}_1^k,\end{aligned}$$

for all $i, j, k \in [2]$. This is well-defined because every element of D_4 can be written uniquely as

$J^i P_0^j P_1^k$ (See Section 2.5). Next we show that f_A is a $|\widetilde{\psi}\rangle$-representation, and a similar argument holds for f_B. We show that for all $i_1, j_1, k_1, i_2, j_2, k_2 \in [2]$

$$\begin{aligned} f_A(J^{i_1} P_0^{j_1} P_1^{k_1}) f_A(J^{i_2} P_0^{j_2} P_1^{k_2})|\psi\rangle &= f_A((J^{i_1} P_0^{j_1} P_1^{k_1})(J^{i_2} P_0^{j_2} P_1^{k_2}))|\psi\rangle \\ &= f_A(J^{i_1+i_2+k_1 j_2} P_0^{j_1+j_2} P_1^{k_1+k_2})|\psi\rangle. \end{aligned}$$

We prove this as follows

$$\begin{aligned} f_A(J^{i_1} P_0^{j_1} P_1^{k_1}) f_A(J^{i_2} P_0^{j_2} P_1^{k_2})|\psi\rangle &= ((-1)^{i_1} \widetilde{A}_0^{j_1} \widetilde{A}_1^{k_1})((-1)^{i_2} \widetilde{A}_0^{j_2} \widetilde{A}_1^{k_2})|\psi\rangle \\ &= (-1)^{i_1+i_2+k_2 j_2} \widetilde{A}_0^{j_1} \widetilde{A}_1^{k_1+k_2} \widetilde{A}_0^{j_2}|\psi\rangle \\ &= (-1)^{i_1+i_2+k_1 j_2} \widetilde{A}_0^{j_1+j_2} \widetilde{A}_1^{k_1+k_2}|\psi\rangle \\ &= f_A(J^{i_1+i_2+k_1 j_2} P_0^{j_1+j_2} P_1^{k_1+k_2})|\psi\rangle, \end{aligned}$$

where in lines 2 and 3, we make essential use of the fact that the exponents are modulo 2.

The representation theory of D_4 is simple. There are four irreducible representations of dimension one: These are given by $P_0 \mapsto (-1)^i, P_1 \mapsto (-1)^j, J \mapsto 1$ for $i, j \in [2]$. The only irreducible representation of dimension larger than one is given by

$$\rho(P_0) = \sigma_x, \ \rho(P_1) = \sigma_y, \ \rho(J) = -I.$$

Among these, ρ is the only irreducible representation that gives rise to an optimal strategy for CHSH. In addition $|\psi_2\rangle$ is the unique state that maximizes $\nu(\text{CHSH}, \mathcal{S}_{\rho,\rho,|\psi\rangle})$. This follows since $|\psi_2\rangle$ is the unique eigenvector associated with the largest eigenvalue of $\mathcal{B}_2(\sigma_x, \sigma_y, \sigma_x, \sigma_y)$. The rigidity of CHSH follows from Corollary 2.2.5.

Now we propose a general framework for proving rigidity of $\mathcal{G}_n$ and similar games. This framework extends the methods demonstrated in the CHSH example to deal with more complex games. For concreteness, we focus on $\mathcal{G}_n$. We use Corollary 2.2.5 to prove rigidity. This requires us to ascertain two facts about the game $\mathcal{G}$:

1. Every optimal strategy induces $|\psi\rangle$-representations of some groups G_A and G_B.

2. There is a unique pair of irreducible representations ρ, σ of G_A, G_B, respectively, such that $\nu(\mathcal{G}, \rho, \sigma) = \nu^*(\mathcal{G})$.

The first step is to obtain algebraic relations (i.e., groups G_A and G_B) between the observables of optimal strategies. Suppose we found some SOS decomposition

$$\lambda_n I - \mathcal{B}_n(a_0, a_1, b_0, b_1) = \sum_k T_k(a_0, a_1, b_0, b_1)^* T_k(a_0, a_1, b_0, b_1),$$

where $\mathcal{B}_n$ is the bias polynomial for $\mathcal{G}_n$ and $\lambda_n = 4n\nu^*(\mathcal{G}_n) - 4$. This equality is over

$$\mathbb{C}^*\langle a_0, a_1, b_0, b_1\rangle / \langle a_i^n - 1, b_j^n - 1, a_i b_j - a_j b_i : \forall i, j \in \{0, 1\}\rangle$$

where $\mathbb{C}^*\langle a_0, a_1, b_0, b_1\rangle$ is the ring of noncommutative polynomials equipped with adjoint, and $\langle a_i^n - 1, b_j^n - 1, a_i b_j - a_j b_i : \forall i, j \in \{0, 1\}\rangle$ is the ideal that forces Alice and Bob's operators to form a valid strategy.

For any optimal strategy $(\{A_0, A_1\}, \{B_0, B_1\}, |\psi\rangle)$, it holds that

$$\big(\lambda_n I - \mathcal{B}_n(A_0, A_1, B_0, B_1)\big)|\psi\rangle = 0.$$

So it must also hold that $T_k(A_0, A_1, B_0, B_1)|\psi\rangle = 0$. Let $(M_j(A_0, A_1) - I)|\psi\rangle = 0$ be all the relations derived from T_k such that M_i are monomials only in Alice's operators. Similarly let $(N_j(A_0, A_1) - I)|\psi\rangle = 0$ be all the monomial relations involving only Bob's operators. We call M_i, N_j the *group relations*. Define groups

$$G_A = \langle P_0, P_1 : M_i(P_0, P_1)\rangle, \quad G_B = \langle Q_0, Q_1 : N_j(Q_0, Q_1)\rangle.$$

In the case of $\mathcal{G}_n$, we in fact have $G_A = G_B = G_n$.[1] Next, prove that, for all optimal strategies,

[1] In Section 2.5, we gave a presentation for G_n using three generators, but in fact one could obtain a presentation using only two generators.

the functions f_A, f_B defined by $f_A(P_i) = A_i$ and $f_B(Q_j) = B_j$ (as in the preliminaries) are $|\psi\rangle$-representations of G_A, G_B, respectively.

To prove the second assumption, one approach is the brute force enumeration of irreducible representation pairs. A more practical approach, when dealing with families of games, is to demonstrate uniqueness of the pair of optimal irreducible representations using *ring relations*. Let $R_i(A_0, A_1)|\psi\rangle = 0$ be all the relations derived from T_k. We call $R_i(A_0, A_1)|\psi\rangle = 0$ ring relations. They are allowed to be arbitrary polynomials (as opposed to monomials in the case of group relations). Similarly let $S_j(B_0, B_1)|\psi\rangle = 0$ be all the relations derived from T_k involving only Bob's operators. Then show that there is a unique irreducible representation ρ of G_A (resp. σ of G_B) satisfying the ring relations, i.e., $R_i(\rho(P_0), \rho(P_1)) = 0$ (resp. $S_i(\sigma(Q_0), \sigma(Q_1)) = 0$). Note that here we require the stronger constraint $R_i(\rho(P_0), \rho(P_1)) = 0$ as opposed to $R_i(\rho(P_0), \rho(P_1))|\psi\rangle = 0$.[2]

In some special cases, e.g., games $\mathcal{G}_n$, there is one ring relation that rules them all. For $\mathcal{G}_n$ there is a unique irreducible representation of G_n satisfying the ring relation $(H_n+(n-2)I)|\psi\rangle = 0$ where

$$H_n = H_n(A_0, A_1) = \omega \sum_{i=0}^{n-1} A_0^i A_1 A_0^{(n-i-1)}. \tag{2.6.2}$$

For example in the case of G_5, there are 25 degree one irreducible representations given by $P_0 \mapsto \omega_5^i, P_1 \mapsto \omega_5^j, J \mapsto \omega^{2(j-i)}$ for all $i, j \in [5]$. There are also 15 irreducible representations of degree five: For each $i \in [5]$, there are three irreducible representations sending $J \to \omega_5^i I_5$. Among these 40 irreducible representations only one satisfies the ring relation $(H_5 + 3I)|\psi\rangle = 0$. This unique irreducible representation is one of the three irreducible representations mapping $J \mapsto \omega_5 I_5$.[3]

In section 2.8, we show that in the special case of pseudo-telepathic games, this framework reduces to the solution group formalism of Cleve, Liu, and Slofstra [6]. The group derived from

[2] The intuition behind this step is the one-to-one correspondence between the group representations of G_A and the ring representations of the group ring $\mathbb{C}[G_A]$. The optimal pair of irreducible representations are in fact irreducible representations of rings $\mathbb{C}[G_A]/\langle R_i(P_0, P_1)\rangle$ and $\mathbb{C}[G_B]/\langle S_j(Q_0, Q_1)\rangle$.

[3] Interestingly, cousin games of $\mathcal{G}_5$, defined using systems of equation $x_0x_1 = 1, x_0, x_1 = \omega^i$ for $i \in [5]$, generate the same group G_5. For every i, the unique optimal irreducible representation strategy is one of the three irreducible representations mapping $J \mapsto \omega_5^i I_5$.

the SOS is the solution group, and the analogue of the ring relation that hones in on the optimal irreducible representation ρ is the requirement that $\rho(J) \neq I$.

In the next section, we use the SOS framework to give a full proof of the rigidity of $\mathcal{G}_3$. While omitted, the cases of $\mathcal{G}_4, \mathcal{G}_5$ follow similarly. The SOS decompositions of $\mathcal{B}_4, \mathcal{B}_5$ are comparatively long and tedious.

2.7 Optimality and rigidity for $\mathcal{G}_3$

In this section, we show that $\mathcal{S}_3$ is optimal, and therefore $\nu^*(\mathcal{G}_3) = 5/6$. We also show that $\mathcal{G}_3$ is a self-test for the strategy $\mathcal{S}_3$. We obtain these results by obtaining algebraic relations between operators in any optimal strategy using an SOS decomposition for $\mathcal{B}_3$.

2.7.1 Optimality of $\mathcal{S}_3$

For every operator A_i, B_j for which $A_i^3 = B_j^3 = I$ and $[A_i, B_j] = 0$, we have the following SOS decomposition:

$$\begin{aligned} &6I - A_0B_0^* - A_0^*B_0 - A_0B_1 - A_0^*B_1^* - A_1B_0^* - A_1^*B_0 - \omega^*A_1B_1 - \omega A_1^*B_1^* \\ &\quad = \lambda_1(S_1^*S_1 + S_2^*S_2) + \lambda_2(T_1^*T_1 + T_2^*T_2) + \lambda_3(T_3^*T_3 + T_4^*T_4) + \lambda_4(T_5^*T_5 + T_6^*T_6), \end{aligned} \tag{2.7.1}$$

where

$$
\begin{aligned}
S_1 &= A_0 + \omega A_1 + \omega^* B_0 + \omega B_1^*, \\
S_2 &= A_0^* + \omega^* A_1^* + \omega B_0^* + \omega^* B_1, \\
T_1 &= A_0 B_0^* + ai A_0^* B_0 - a A_0 B_1 + i A_0^* B_1^* + a A_1 B_0^* - i A_1^* B_0 - \omega^* A_1 B_1 - ai\omega A_1^* B_1^*, \\
T_2 &= A_0 B_0^* + ai A_0^* B_0 + a A_0 B_1 - i A_0^* B_1^* - a A_1 B_0^* + i A_1^* B_0 - \omega^* A_1 B_1 - ai\omega A_1^* B_1^*, \\
T_3 &= A_0 B_0^* - ai A_0^* B_0 - a A_0 B_1 - i A_0^* B_1^* + a A_1 B_0^* + i A_1^* B_0 - \omega^* A_1 B_1 + ai\omega A_1^* B_1^*, \\
T_4 &= A_0 B_0^* - ai A_0^* B_0 + a A_0 B_1 + i A_0^* B_1^* - a A_1 B_0^* - i A_1^* B_0 - \omega^* A_1 B_1 + ai\omega A_1^* B_1^*, \\
T_5 &= A_0 B_0^* + b A_0^* B_0 - b A_0 B_1 - A_0^* B_1^* - b A_1 B_0^* - A_1^* B_0 + \omega^* A_1 B_1 + b\omega A_1^* B_1^*, \\
T_6 &= 6I - A_0 B_0^* - A_0^* B_0 - A_0 B_1 - A_0^* B_1^* - A_1 B_0^* - A_1^* B_0 - \omega^* A_1 B_1 - \omega A_1^* B_1^*,
\end{aligned}
$$

and

$$
\lambda_1 = \frac{5}{86},\ \lambda_2 = \frac{14+\sqrt{21}}{4\cdot 86},\ \lambda_3 = \frac{14-\sqrt{21}}{4\cdot 86},\ \lambda_4 = \frac{7}{86},
$$
$$
a = \frac{2\omega + 3\omega^*}{\sqrt{7}},\ b = \frac{3\omega + 8\omega^*}{7}, \omega = \omega_3.
$$

This SOS decomposition tells us that $\mathcal{B}_3 \le 6I$ in positive semidefinite order. So from Theorem 2.3.1, it holds that $\nu^*(\mathcal{G}_3) \le 5/6$. Combined with Theorem 2.4.9, we have $\nu^*(\mathcal{G}_3) = 5/6$.

This SOS is obtained from the dual semidefinite program associated with the second level of the NPA hierarchy. Surprisingly, the first level of NPA is not enough to obtain this upper bound, as was the case with CHSH.

2.7.2 Algebraic relations

As in Section 2.6, we derive group and ring relations for optimal strategies of $\mathcal{G}_3$ from the SOS (2.7.1). For the rest of this section, let $(A_0, A_1, B_0, B_1, |\psi\rangle)$ be an optimal strategy. Then $\langle\psi|(6I - \mathcal{B}_3)|\psi\rangle = 0$. So it also holds that $S_i|\psi\rangle = 0$ and $T_j|\psi\rangle = 0$ for all $i \in [2]$ and $j \in [6]$.

Therefore

$$(T_1 + T_2 + T_3 + T_4)|\psi\rangle = 0, \quad (T_1 + T_2 - T_3 - T_4)|\psi\rangle = 0,$$
$$(T_1 - T_2 + T_3 - T_4)|\psi\rangle = 0, \quad (T_1 - T_2 - T_3 + T_4)|\psi\rangle = 0.$$

From which by simplification we obtain the four relations

$$\begin{aligned} &A_0 B_0^* |\psi\rangle = \omega^* A_1 B_1 |\psi\rangle, \quad &&A_0^* B_0 |\psi\rangle = \omega A_1^* B_1^* |\psi\rangle, \\ &A_0 B_1 |\psi\rangle = A_1 B_0^* |\psi\rangle, &&A_0^* B_1^* |\psi\rangle = A_1^* B_0 |\psi\rangle. \end{aligned} \tag{2.7.2}$$

Now from these four relations and the fact that A_i, B_j are generalized observables satisfying $[A_i, B_j] = 0$, we obtain

$$\omega^* A_0^* A_1 |\psi\rangle = B_1^* B_0^* |\psi\rangle \tag{2.7.3}$$

$$\omega A_0 A_1^* |\psi\rangle = B_1 B_0 |\psi\rangle \tag{2.7.4}$$

$$A_0^* A_1 |\psi\rangle = B_0 B_1 |\psi\rangle \tag{2.7.5}$$

$$A_0 A_1^* |\psi\rangle = B_0^* B_1^* |\psi\rangle \tag{2.7.6}$$

$$A_1^* A_0 |\psi\rangle = \omega^* B_0 B_1 |\psi\rangle \tag{2.7.7}$$

$$A_1 A_0^* |\psi\rangle = \omega B_0^* B_1^* |\psi\rangle \tag{2.7.8}$$

$$A_1^* A_0 |\psi\rangle = B_1^* B_0^* |\psi\rangle \tag{2.7.9}$$

$$A_1 A_0^* |\psi\rangle = B_1 B_0 |\psi\rangle. \tag{2.7.10}$$

From the pair of relations (2.7.3) and (2.7.9) as well as the pair of relations (2.7.4) and (2.7.10), we obtain the following relations between Alice's observables acting on the state $|\psi\rangle$:

$$A_0^* A_1 |\psi\rangle = \omega A_1^* A_0 |\psi\rangle, \tag{2.7.11}$$

$$A_1 A_0^* |\psi\rangle = \omega A_0 A_1^* |\psi\rangle. \tag{2.7.12}$$

Next we prove two propositions regarding $H = H_3 = \omega A_0 A_1 A_0 + \omega A_0^* A_1 + \omega A_1 A_0^*$ defined in (2.6.2).

Proposition 2.7.1. $(H + H^*)|\psi\rangle = -2|\psi\rangle$

Proof. We start by writing

$$\begin{aligned}
(\omega B_0^* + \omega^* B_1 + B_0 B_1^* + B_1^* B_0)|\psi\rangle &= (\omega^* B_0 + \omega B_1^*)(\omega^* B_0 + \omega B_1^*)|\psi\rangle \\
&= -(\omega^* B_0 + \omega B_1^*)(A_0 + \omega A_1)|\psi\rangle \\
&= -(A_0 + \omega A_1)(\omega^* B_0 + \omega B_1^*)|\psi\rangle \\
&= (A_0 + \omega A_1)(A_0 + \omega A_1)|\psi\rangle \\
&= (A_0^* + \omega^* A_1^* + \omega A_0 A_1 + \omega A_1 A_0)|\psi\rangle,
\end{aligned}$$

where for the second and fourth equality, we used the relation $S_1|\psi\rangle = 0$, and for the third equality we used the fact that Alice and Bob's operators commute. Now using $S_2|\psi\rangle = 0$, we obtain

$$(B_0 B_1^* + B_1^* B_0)|\psi\rangle = (2A_0^* + 2\omega^* A_1^* + \omega A_0 A_1 + \omega A_1 A_0)|\psi\rangle. \tag{2.7.13}$$

Similarly we have

$$(B_1 B_0^* + B_0^* B_1)|\psi\rangle = (2A_0 + 2\omega A_1 + \omega^* A_0^* A_1^* + \omega^* A_1^* A_0^*)|\psi\rangle. \tag{2.7.14}$$

We proceed by simplifying $T_6|\psi\rangle = 0$ using relations (2.7.2) to obtain

$$(3I - A_0 B_0^* - A_0^* B_0 - A_0 B_1 - A_0^* B_1^*)|\psi\rangle = 0.$$

Let $P = A_0B_0^* + A_0^*B_0 + A_0B_1 + A_0^*B_1^*$, and write

$$\begin{aligned}
0 &= \big(3I - A_0B_0^* - A_0^*B_0 - A_0B_1 - A_0^*B_1^*\big)^*\big(3I - A_0B_0^* - A_0^*B_0 - A_0B_1 - A_0^*B_1^*\big)|\psi\rangle \\
&= \big(13I - 5P + A_0^*(B_1B_0^* + B_0^*B_1) + A_0(B_0B_1^* + B_1^*B_0) + B_0^*B_1^* + B_0B_1 + B_1B_0 + B_1^*B_0^*\big)|\psi\rangle \\
&= (-2I + A_0^*(B_1B_0^* + B_0^*B_1) + A_0(B_0B_1^* + B_1^*B_0) + B_0^*B_1^* + B_0B_1 + B_1B_0 + B_1^*B_0^*)|\psi\rangle, \quad (2.7.15)
\end{aligned}$$

where in the last line, we used $(3I - P)|\psi\rangle = 0$. Using identities (2.7.13) and (2.7.14)

$$\begin{aligned}
&\big(A_0^*(B_1B_0^* + B_0^*B_1) + A_0(B_0B_1^* + B_1^*B_0)\big)|\psi\rangle \\
&\quad = \big(4I + \omega A_0A_1A_0 + \omega^*A_0^*A_1^*A_0^* + 2\omega A_0^*A_1 + \omega^*A_0A_1^* + 2\omega^*A_0A_1^* + \omega A_0^*A_1\big)|\psi\rangle.
\end{aligned}$$

Transferring Bob's operators to Alice using identities (2.7.3-2.7.6)

$$\big(B_0^*B_1^* + B_0B_1 + B_1B_0 + B_1^*B_0^*\big)|\psi\rangle = \big(A_0A_1^* + A_0^*A_1 + \omega A_0A_1^* + \omega^*A_0^*A_1\big)|\psi\rangle.$$

Plugging these back in (2.7.15)

$$\begin{aligned}
0 &= (2I + \omega A_0A_1A_0 + \omega^*A_0^*A_1^*A_0^* + (3\omega + \omega^* + 1)A_0^*A_1 + (3\omega^* + \omega + 1)A_0A_1^*)|\psi\rangle \\
&= (2I + \omega A_0A_1A_0 + \omega^*A_0^*A_1^*A_0^* + 2\omega A_0^*A_1 + 2\omega^*A_0A_1^*)|\psi\rangle \\
&= (2I + \omega A_0A_1A_0 + \omega^*A_0^*A_1^*A_0^* + \omega A_0^*A_1 + \omega^*A_1^*A_0 + \omega^*A_0A_1^* + \omega A_1A_0^*)|\psi\rangle. \\
&= (2I + H + H^*)|\psi\rangle,
\end{aligned}$$

where in the first line we used $1 + \omega + \omega^* = 0$, and in the second line we used identities (2.7.11) and (2.7.12). □

Proposition 2.7.2. $(H + I)|\psi\rangle = (H^* + I)|\psi\rangle = 0$.

Proof. First note

$$\begin{aligned}\langle\psi|H^*H|\psi\rangle = \langle\psi|(3I + A_0^*A_1^*A_0A_1 + A_1^*A_0^*A_1A_0 + A_1^*A_0A_1A_0^* + A_0A_1^*A_0^*A_1 \\ + A_0^*A_1^*A_0^*A_1A_0^* + A_0A_1^*A_0A_1A_0)|\psi\rangle.\end{aligned} \tag{2.7.16}$$

Using (2.7.11) and (2.7.12), we have

$$\langle\psi|A_0A_1^*A_0^*A_1|\psi\rangle = \omega\langle\psi|A_0A_1^*A_1^*A_0|\psi\rangle = \omega\langle\psi|A_0A_1A_0|\psi\rangle,$$

$$\langle\psi|A_0^*A_1^*A_0^*A_1A_0^*|\psi\rangle = \omega\langle\psi|A_0^*A_1^*A_0^*A_0A_1^*|\psi\rangle = \omega\langle\psi|A_0^*A_1|\psi\rangle,$$

and using (2.7.5) and (2.7.7)

$$\langle\psi|A_0^*A_1^*A_0A_1|\psi\rangle = \langle\psi|A_0^*A_1A_1A_0^*A_0^*A_1|\psi\rangle = \omega\langle\psi|B_1^*B_0^*A_1A_0^*B_0B_1|\psi\rangle = \omega\langle\psi|A_1A_0^*|\psi\rangle,$$

and taking conjugate transpose of these three we obtain

$$\langle\psi|A_1^*A_0A_1A_0^*|\psi\rangle = \omega^*\langle\psi|A_0^*A_1^*A_0^*|\psi\rangle,$$

$$\langle\psi|A_0A_1^*A_0A_1A_0|\psi\rangle = \omega^*\langle\psi|A_1^*A_0|\psi\rangle,$$

$$\langle\psi|A_1^*A_0^*A_1A_0|\psi\rangle = \omega^*\langle\psi|A_0A_1^*|\psi\rangle.$$

Plugging these back in (2.7.16), we obtain

$$\begin{aligned}\|H|\psi\rangle\|^2 &= \langle\psi|H^*H|\psi\rangle \\ &= \langle\psi|(3I + \omega A_0A_1A_0 + \omega A_0^*A_1 + \omega A_1A_0^* + \omega^*A_0^*A_1^*A_0^* + \omega^*A_1^*A_0 + \omega^*A_0A_1^*)|\psi\rangle \\ &= \langle\psi|(3I + H + H^*)|\psi\rangle \\ &= \langle\psi|I|\psi\rangle \\ &= 1,\end{aligned}$$

where in fourth equality we used Proposition 2.7.1. Similarly $\|H^*|\psi\rangle\| = 1$. From $(H + H^*)|\psi\rangle = -2|\psi\rangle$ and the fact that $H|\psi\rangle$ and $H^*|\psi\rangle$ are unit vectors, we get that $H|\psi\rangle = H^*|\psi\rangle = -|\psi\rangle$. □

Proposition 2.7.3. $A_0 A_1 A_0|\psi\rangle = \omega A_0^* A_1^* A_0^*|\psi\rangle$.

Proof. By Proposition 2.7.2, $H|\psi\rangle = H^*|\psi\rangle$, and by identities (2.7.11), (2.7.12), $(\omega A_0^* A_1 + \omega A_1 A_0^*)|\psi\rangle = (\omega^* A_1^* A_0 + \omega^* A_0 A_1^*)|\psi\rangle$. Putting these together, we obtain $A_0 A_1 A_0|\psi\rangle = \omega A_0^* A_1^* A_0^*|\psi\rangle$.

□

Proposition 2.7.4. $A_0 A_1^* A_0^* A_1|\psi\rangle = A_0^* A_1 A_0 A_1^*|\psi\rangle$ *in other words* $A_0 A_1^*$ *and* $A_0^* A_1$ *commute on* $|\psi\rangle$

Proof. To see this write

$$\begin{aligned}
A_0 A_1^* A_0^* A_1|\psi\rangle &= \omega A_0 A_1^* A_1^* A_0|\psi\rangle \\
&= \omega A_0 A_1 A_0|\psi\rangle \\
&= \omega^* A_0^* A_1^* A_0^*|\psi\rangle \\
&= \omega^* A_0^* A_1 A_1 A_0^*|\psi\rangle \\
&= A_0^* A_1 A_0 A_1^*|\psi\rangle,
\end{aligned}$$

where in the first line we used 2.7.11, in the third line we used 2.7.3, and in the fifth line we used 2.7.12.

□

2.7.3 Rigidity of $\mathcal{G}_3$

Suppose $(\{A_0, A_1\}, \{B_0, B_1\}, |\psi\rangle)$ is an optimal strategy for $\mathcal{G}_3$. By Theorem 2.5.7, we know that the optimal operators of Alice defined in section 2.4.1 generate the group

$$G_3 = \left\langle J, P_0, P_1 : J^3, P_0^3, P_1^3, [J, P_0], [J, P_1], J(P_0 P_1^{-1})^2 \right\rangle,$$

The same group is generated by Bob's operators as in Remark 2.5.8. We apply Corollary 2.2.5 with $G_A = G_B = G_3$. In order to do this, we first prove the following lemma stating that every optimal strategy is a $|\psi\rangle$-representation of G.

Lemma 2.7.5. *Let $(\{A_0, A_1\}, \{B_0, B_1\}, |\psi\rangle)$ be an optimal strategy for $\mathcal{G}_3$. Define maps $f_A, f_B : G_3 \to \mathrm{U}_d(\mathbb{C})$ by*

$$f_A(J) = \omega_3 I,\ f_A(P_0) = A_0,\ f_A(P_0P_1^{-1}) = A_0A_1^*,\ f_A(P_0^{-1}P_1) = A_0^*A_1$$
$$f_B(J) = \omega_3 I,\ f_B(P_0) = B_0^*,\ f_B(P_0P_1^{-1}) = B_0^*B_1^*,\ f_B(P_0^{-1}P_1) = B_0B_1$$

and extend it to all of G_3 using the normal form from Lemma 2.5.3. Then f_A, f_B are $|\psi\rangle$-representations of G_3.

Proof. These maps are well defined since every element of G_3 can be written uniqly as

$$J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2}$$

for $i, j \in [3], q_1, q_2 \in [2]$. All we need is that $f_A(g)f_A(g')|\psi\rangle = f_A(gg')|\psi\rangle$ for all $g, g' \in G_3$. The proof is reminiscent of the proof that gg' can be written in normal form for every $g, g' \in G_3$. Except that we need to be more careful here, since we are dealing with Alice's operators A_0, A_1, and not the abstract group elements P_0, P_1. Therefore we can only use the state-dependent relations derived in the previous section. We must show that

$$\begin{aligned} &f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})f_A(J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'})|\psi\rangle \\ &\quad = f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2}J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'})|\psi\rangle \end{aligned} \tag{2.7.17}$$

for all $i, j, i', j' \in [3]$ and $q_1, q_2, q_1', q_2' \in [2]$.

Claim 2. *Without loss of generality, we can assume $i = j = i' = q_1' = q_2' = 0$.*

Proof. Fix $i, j, q_1, q_2, i', j', q_1', q_2'$. We first show that without loss of generality we can assume

$q_1' = q_2' = 0$. By Lemma 2.5.3, there exist $i'', j'' \in [3], q_1'', q_2'' \in [2]$ such that

$$\big(J^i P_0^j (P_0 P_1^{-1})^{q_1} (P_0^{-1} P_1)^{q_2}\big)\big(J^{i'} P_0^{j'}\big) = J^{i''} P_0^{j''} (P_0 P_1^{-1})^{q_1''} (P_0^{-1} P_1)^{q_2''}.$$

So it also holds that

$$\big(J^i P_0^j (P_0 P_1^{-1})^{q_1} (P_0^{-1} P_1)^{q_2}\big)\big(J^{i'} P_0^{j'} (P_0 P_1^{-1})^{q_1'} (P_0^{-1} P_1)^{q_2'}\big) = J^{i''} P_0^{j''} (P_0 P_1^{-1})^{q_1''+q_1'} (P_0^{-1} P_1)^{q_2''+q_2'}$$

since by Lemma 2.5.2, $P_0 P_1^{-1}$ and $P_0^{-1} P_1$ commute. So the right-hand-side of (2.7.17) can be written

$$\begin{aligned}
&f_A(J^i P_0^j (P_0 P_1^{-1})^{q_1} (P_0^{-1} P_1)^{q_2} J^{i'} P_0^{j'} (P_0 P_1^{-1})^{q_1'} (P_0^{-1} P_1)^{q_2'})|\psi\rangle \\
&\quad = f_A(J^{i''} P_0^{j''} (P_0 P_1^{-1})^{q_1''+q_1'} (P_0^{-1} P_1)^{q_2''+q_2'})|\psi\rangle \\
&\quad = \omega^{i''} A_0^{j''} (A_0 A_1^{-1})^{q_1''+q_1'} (A_0^{-1} A_1)^{q_2''+q_2'} |\psi\rangle \\
&\quad = (B_0 B_1)^{q_2'} (B_0^* B_1^*)^{q_1'} \omega^{i''} A_0^{j''} (A_0 A_1^{-1})^{q_1''} (A_0^{-1} A_1)^{q_2''} |\psi\rangle \\
&\quad = (B_0 B_1)^{q_2'} (B_0^* B_1^*)^{q_1'} f_A(J^{i''} P_0^{j''} (P_0 P_1^{-1})^{q_1''} (P_0^{-1} P_1)^{q_2''})|\psi\rangle \\
&\quad = (B_0 B_1)^{q_2'} (B_0^* B_1^*)^{q_1'} f_A((J^i P_0^j (P_0 P_1^{-1})^{q_1} (P_0^{-1} P_1)^{q_2})(J^{i'} P_0^{j'}))|\psi\rangle,
\end{aligned}$$

where in the fourth equality, we used (2.7.5) and (2.7.6) and the fact that Alice and Bob's operators commute.

Also since Alice and Bob's operators commute

$$\begin{aligned}
f_A(J^{i'} P_0^{j'} (P_0 P_1^{-1})^{q_1'} (P_0^{-1} P_1)^{q_2'})|\psi\rangle &= \omega^{i'} A_0^{j'} (A_0 A_1^*)^{q_1'} (A_0^* A_1)^{q_2'} |\psi\rangle \\
&= (B_0 B_1)^{q_2'} \omega^{i'} A_0^{j'} (A_0 A_1^*)^{q_1'} |\psi\rangle \\
&= (B_0 B_1)^{q_2'} (B_0^* B_1^*)^{q_1'} \omega^{i'} A_0^{j'} |\psi\rangle \\
&= (B_0 B_1)^{q_2'} (B_0^* B_1^*)^{q_1'} f_A(J^{i'} P_0^{j'})|\psi\rangle.
\end{aligned}$$

Therefore the left-hand-side of (2.7.17) can be written as

$$f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})f_A(J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'})|\psi\rangle$$
$$= (B_0B_1)^{q_2'}(B_0^*B_1^*)^{q_1'}f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})f_A(J^{i'}P_0^{j'})|\psi\rangle$$

Since B_0, B_1 are unitaries, (2.7.17) is equivalent to the following identity

$$f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})f_A(J^{i'}P_0^{j'})|\psi\rangle = f_A((J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})(J^{i'}P_0^{j'}))|\psi\rangle,$$

in other words we can assume without loss of generality $q_1' = q_2' = 0$. The case of $i = j = 0$ is handled similarly. Also since J and $f(J)$ are both central, we can assume $i' = 0$. □

By this claim, we just need to verify

$$f_A((P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})f_A(P_0^{j'})|\psi\rangle = f_A((P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2}P_0^{j'})|\psi\rangle \tag{2.7.18}$$

There are 12 cases to consider: $q_1, q_2 \in [2], j' \in [3]$. The case of $j' = 0$ is trivial, and the case of $j' = 2$ is handled similar to the case of $j' = 1$. So we only consider the case of $j' = 1$. The case of $q_1 = q_2 = 0$ is trivial. We analyse the remaining three cases one-by-one:

- $q_1 = 0, q_2 = 1$: First note that

$$(P_0^{-1}P_1)P_0 = P_0P_0P_1^{-1}P_1^{-1}P_0 = J^2P_0(P_0P_1^{-1})(P_0^{-1}P_1),$$

which allows us to write

$$\begin{aligned} f_A((P_0^{-1}P_1))f_A(P_0)|\psi\rangle &= A_0^*A_1A_0|\psi\rangle \\ &= A_0^*A_1^*A_1^*A_0|\psi\rangle \\ &= \omega^*A_0^*A_1^*A_0^*A_1|\psi\rangle \\ &= \omega^*A_0(A_0A_1^*)(A_0^*A_1)|\psi\rangle \\ &= f_A(J^2P_0(P_0P_1^{-1})(P_0^{-1}P_1))|\psi\rangle \\ &= f_A((P_0^{-1}P_1)P_0)|\psi\rangle, \end{aligned}$$

where in the third line we used (2.7.11).

- $q_1 = 1, q_2 = 0$:

$$(P_0P_1^{-1})P_0 = J^2P_0(P_0^{-1}P_1)$$

which allows us to write

$$\begin{aligned} f_A(P_0P_1^{-1})f_A(P_0)|\psi\rangle &= (A_0A_1^*)A_0|\psi\rangle \\ &= A_0(A_1^*A_0)|\psi\rangle \\ &= \omega^*A_0(A_0^*A_1)|\psi\rangle \\ &= f_A(J^2P_0(P_0^{-1}P_1))|\psi\rangle \\ &= f_A((P_0P_1^{-1})P_0)|\psi\rangle, \end{aligned}$$

where in the third line we used (2.7.11).

- $q_1 = q_2 = 1$:

$$(P_0P_1^{-1})(P_0^{-1}P_1)P_0 = J(P_0P_1^{-1})(P_1^{-1}P_0)P_0 = JP_0(P_1P_0^{-1}) = J^2P_0(P_0P_1^{-1}).$$

Now write

$$\begin{aligned}
f_A((P_0P_1^{-1})(P_0^{-1}P_1))f_A(P_0)|\psi\rangle &= A_0A_1^*A_0^*A_1A_0|\psi\rangle \\
&= A_0A_1^*A_0A_0A_1A_0|\psi\rangle \\
&= \omega A_0A_1^*A_0A_0^*A_1^*A_0^*|\psi\rangle \\
&= \omega A_0(A_1A_0^*)|\psi\rangle \\
&= \omega^* A_0(A_0A_1^*)|\psi\rangle \\
&= f_A(J^2P_0(P_0P_1^{-1}))|\psi\rangle \\
&= f_A((P_0P_1^{-1})(P_0^{-1}P_1)P_0)|\psi\rangle,
\end{aligned}$$

where in the third line we used Proposition 2.7.3 and in the second last line we used (2.7.12). The proof that f_B is a $|\psi\rangle$-representation follows similarly. □

Theorem 2.7.6. *$\mathcal{G}_3$ is rigid.*

Proof. The representation theory of G_3 is simple. There are nine irreducible representation of dimension one: These are given by $P_0 \mapsto \omega^i, P_1 \mapsto \omega^j, J \mapsto \omega^{2(j-i)}$ for $i, j \in [3]$. It also has three irreducible representations g_1, g_2, g_3 of dimension three defined by

$$g_1(P_0) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},\ g_1(P_1) = \begin{pmatrix} 0 & 0 & \omega^* \\ -\omega^* & 0 & 0 \\ 0 & -\omega^* & 0 \end{pmatrix},\ g_1(J) = \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{pmatrix},$$

$$g_2(P_0) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},\ g_2(P_1) = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},\ g_2(J) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$g_3(P_0) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},\ g_3(P_1) = \begin{pmatrix} 0 & \omega & 0 \\ 0 & 0 & -\omega \\ -\omega & 0 & 0 \end{pmatrix},\ g_3(J) = \begin{pmatrix} \omega^* & 0 & 0 \\ 0 & \omega^* & 0 \\ 0 & 0 & \omega^* \end{pmatrix}.$$

Among these g_1, is the only representation that gives rise to an optimal strategy. This follows from a simple enumeration of these 12 irreducible representations. However we could also immediately see this, since g_1 is the only irreducible representation that satisfies the ring relation $H_3 + I = 0$.

Define a unitarily equivalent irreducible representation $g_1' = U g_1 U^*$ where $U = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Now $\widetilde{A}_0 = g_1(P_0), \widetilde{A}_1 = g_1(P_1), \widetilde{B}_0 = g_1'(P_0)^*, \widetilde{B}_1 := g_1'(P_1)$ is the same strategy defined in example 2.4.2.

In addition

$$|\psi_3\rangle = \frac{1}{\sqrt{10}} \Big((1 - z^4)|00\rangle + 2|12\rangle + (1 + z^2)|21\rangle \Big)$$

is the unique state that maximizes $v(\mathcal{G}_3, \mathcal{S}_{g_1, g_1', |\psi\rangle})$. This follows since $|\psi_3\rangle$ is the unique eigenvector associated with the largest eigenvalue of $\mathcal{B}_3(\widetilde{A}_0, \widetilde{A}_1, \widetilde{B}_0, \widetilde{B}_1)$. The rigidity of $\mathcal{G}_3$ follows from Corollary 2.2.5.

□

Remark 2.7.7. The game $\mathcal{G}_3$ is in fact a robust self-test. We omit the proof, but at a high-level, if a strategy $(\{A_0, A_1\}, \{B_0, B_1\}, |\psi\rangle)$ is ε-optimal for $\mathcal{G}_3$, then

$$\langle \psi | (6I - \mathcal{B}_3) | \psi \rangle \leq O(\varepsilon).$$

Consequently, $\|S_i|\psi\rangle\| \leq O(\sqrt{\varepsilon}), \|T_j|\psi\rangle\| \leq O(\sqrt{\varepsilon})$ for all $i \in [2], j \in [6]$. From which one obtains a robust version of every relation in this section.

2.8 SOS approach to solution group

In this section we show that the connection between an LCS game over $\mathbb{Z}_2$ and its solution group shown in [6] can be determined using sum of squares techniques.

We will suppress the tensor product notation and simply represent a strategy for an LCS game

$\mathcal{G}_{A,b}$ by a state $|\psi\rangle \in \mathcal{H}$ and a collection of commuting measurement systems $\{E_{i,x}\}$ and $\{F_{j,y}\}$. Using the notation outlined in section 2.2.3 we define the following sets of observables

- Alice's Observables: $A_j^{(i)} = \sum_{x:x_j=1} E_{i,x} - \sum_{x:x_j=-1} E_{i,x}$, for each $i \in [r]$ and $j \in V_i$
- Bob's Observables: $B_j = F_{j,1} - F_{j,-1}$ for each $j \in [s]$.

Note $A_j^{(i)}$ commutes with $A_{j'}^{(i)}$ for all $i \in [r]$ and $j, j' \in V_i$ and B_j commutes with $A_j^{(i)}$ for all i, j. These observables will satisfy the following identities:

$$\sum_{x:x\in S_i} E_{i,x} = \frac{1}{2}\left(I + (-1)^{b_i} \prod_{k\in V_i} A_k^{(i)}\right) \tag{2.8.1}$$

$$\sum_{x:y=x_j} E_{i,x} = \frac{1}{2}\left(I + yA_j^{(i)}\right) \tag{2.8.2}$$

The probability of Alice and Bob winning the game is given by evaluating $\langle\psi|v|\psi\rangle$ where

$$\begin{aligned} v &= \sum_{\substack{i\in[r]\\ j\in V_i}} \frac{1}{r|V_i|}\left(\sum_{\substack{x,y:\\ x\in S_i\\ y=x_j}} E_{i,x}F_{j,y}\right) \\ &= \sum_{i,j} \frac{1}{2r|V_i|}\left(1 - \sum_{\substack{x,y:\\ x\in S_i\\ y=x_j}} E_{i,x}F_{j,y}\right)^2 . \end{aligned}$$

Observe using identities 2.8.1 and 2.8.2 we have

$$\begin{aligned}
\left(1 - \sum_{\substack{x,y: \\ x\in S_i \\ y=x_j}} E_{i,x}F_{j,y}\right) &= I - \sum_{y} F_{j,y} \sum_{\substack{x: \\ x\in S_i \\ y=x_j}} E_{i,x} \\
&= I - \frac{1}{4}\sum_{y} F_{j,y}\left((I + yA_j^{(i)})(I + (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)})\right) \\
&= I - \frac{1}{4}\sum_{y} F_{j,y}\left(I + yA_j^{(i)} + (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)} + y(-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)}\right) \\
&= I - \frac{1}{4}F_{j,1}\left(I + A_j^{(i)} + (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)} + (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)}\right) \\
&\qquad - \frac{1}{4}F_{j,-1}\left(I - A_j^{(i)} + (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)} + -(-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)}\right) \\
&= I - \frac{1}{4}I - \frac{1}{4}B_jA_j^{(i)} - \frac{1}{4}(-1)^{b_i}\prod_{k\in v_i} A_k^{(i)} - \frac{1}{4}B_j(-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)} \\
&= \frac{1}{8}\left((I - B_jA_j^{(i)})^2 + (I - (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)})^2 + (I - (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)}B_j)^2\right).
\end{aligned}$$

Thus Alice and Bob are using a perfect strategy if and only if

$$0 = (I - B_jA_j^{(i)})|\psi\rangle = (I - (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)})|\psi\rangle = (I - (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)}B_j)|\psi\rangle.$$

The above equalities will hold exactly when the following two identities hold for all i and $j \in V_i$,

$$B_j|\psi\rangle = A_j^{(i)}|\psi\rangle \tag{2.8.3}$$

$$|\psi\rangle = (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}|\psi\rangle \tag{2.8.4}$$

Using identities 2.8.3 and 2.8.4 it is possible to define a $|\psi\rangle$-representation for the solution group $G_{A,b}$.

2.9 A non-rigid pseudo-telepathic LCS game

The canonical example of a pseudo-telepathic LCS games is the Mermin-Peres magic square game [68] defined in the following figure.

$$\begin{array}{ccccc} e_1 & — & e_2 & — & e_3 \\ | & & | & & \| \\ e_4 & — & e_5 & — & e_6 \\ | & & | & & \| \\ e_7 & — & e_8 & — & e_9 \end{array}$$

Figure 2.3: This describes the Mermin-Peres magic square game. Each single-line indicates that the variables along the line multiply to 1, and the double-line indicates that the variables along the line multiply to -1.

It is well-known that the Mermin-Peres magic square game has the following operator solution for which the corresponding quantum strategy is rigid [91].

$$\begin{array}{lll} A_1 = I \otimes \sigma_Z, & A_2 = \sigma_Z \otimes I, & A_3 = \sigma_Z \otimes \sigma_Z \\ A_4 = \sigma_X \otimes I, & A_5 = I \otimes \sigma_X, & A_6 = \sigma_X \otimes \sigma_X \\ A_7 = \sigma_X \otimes \sigma_Z, & A_8 = \sigma_Z \otimes \sigma_X, & A_9 = \sigma_Y \otimes \sigma_Y, \end{array}$$

In this section, we provide an example of a non-local game whose perfect solutions must obey particular group relations but is not a self-test. This game, *glued magic square*, is described in Figure 2.4.

$$\begin{array}{ccccccccc}
e_1 & — & e_2 & — & e_3 & & & & \\
| & & | & & || & & & & \\
e_4 & — & e_5 & — & e_6 & & & & \\
| & & | & & || & & & & \\
e_7 & — & e_8 & — & e_9 & & & & \\
 & & & & || & & & & \\
 & & & & e_{10} & — & e_{11} & — & e_{12} \\
 & & & & || & & | & & | \\
 & & & & e_{13} & — & e_{14} & — & e_{15} \\
 & & & & || & & | & & | \\
 & & & & e_{16} & — & e_{17} & — & e_{18}
\end{array}$$

Figure 2.4: This describes a LCS game with 18 variables $e_1, e_2, \ldots, e_{18}$. Each single-line indicates that the variables along the line multiply to 1, and the double-line indicates that the variables along the line multiply to -1.

In order to show that this game is not a self-test, we first define two operator solutions, that give rise to perfect strategies. Let $\mathcal{E} = \{E_1, E_2, \ldots, E_{18}\}$ be defined as

$$E_i = \begin{cases} \begin{pmatrix} I_4 & 0 \\ 0 & A_i \end{pmatrix} & \text{for } i = 1, 2, \ldots, 9 \\ \begin{pmatrix} A_{i-9} & 0 \\ 0 & I_4 \end{pmatrix} & \text{for } i = 10, 11, \ldots, 18 \end{cases}$$

and $\mathcal{F} = \{F_1, F_2, \ldots, F_{18}\}$ as

$$F_i = \begin{cases} A_i & \text{for } i = 1, 2 \ldots, 9 \\ I_4 & \text{for } i = 10, 11 \ldots, 18 \end{cases}$$

These two operators solutions $\mathcal{E}$ and $\mathcal{F}$ give rise to two quantum strategies with the entangled states $|\psi_1\rangle = \frac{1}{\sqrt{8}} \sum_{i=0}^{7} |i\rangle|i\rangle$ and $|\psi_2\rangle = \frac{1}{2} \sum_{i=0}^{3} |i\rangle|i\rangle$.

Theorem 2.9.1. *The glued magic square game is not a self-test for any quantum strategy.*

Proof. Suppose, for the sake of contradiction, there is a quantum strategy $\big(\{A_i\}_i, \{B_j\}_j |\psi\rangle\big)$ that is rigid. Then there exist local isometries U_A, U_B and V_A, V_B such that

$$(U_A E_1 \otimes U_B)|\psi_1\rangle = ((A_1 \otimes I)|\psi\rangle)|\text{junk}_1\rangle \tag{2.9.1}$$

$$(U_A E_5 \otimes U_B)|\psi_1\rangle = ((A_5 \otimes I)|\psi\rangle)|\text{junk}_1\rangle \tag{2.9.2}$$

$$(V_A F_1 \otimes V_B)|\psi_2\rangle = ((A_1 \otimes I)|\psi\rangle)|\text{junk}_2\rangle \tag{2.9.3}$$

$$(V_A F_5 \otimes V_B)|\psi_2\rangle = ((A_5 \otimes I)|\psi\rangle)|\text{junk}_2\rangle. \tag{2.9.4}$$

From relation (2.9.2), we obtain

$$\langle\psi_1|(E_5 U_A^* \otimes U_B^*) = \langle\text{junk}_1|(\langle\psi|(A_5^* \otimes I)),$$

and hence together with relation (2.9.1), we obtain the following relation between E_5E_1 and $A_5^*A_1$

$$\langle\psi_1|(E_5E_1 \otimes I)|\psi_1\rangle = \langle\psi|(A_5^*A_1 \otimes I)|\psi\rangle.$$

Similarly, we also obtain

$$\langle\psi_2|(F_5F_1 \otimes I)|\psi_2\rangle = \langle\psi|(A_5^*A_1 \otimes I)|\psi\rangle,$$

and hence

$$\langle\psi_1|(E_5E_1 \otimes I)|\psi_1\rangle = \langle\psi_2|(F_5F_1 \otimes I)|\psi_2\rangle.$$

By first applying the adjoint to relation (2.9.1) and (2.9.3), we obtain

$$\langle\psi_1|(E_1E_5\otimes I)|\psi_1\rangle = \langle\psi_2|(F_1F_5\otimes I)|\psi_2\rangle.$$

Now, since F_1 and F_5 anti-commute, we get the following relation between E_5E_1 and E_1E_5

$$\langle\psi_1|(E_5E_1\otimes I)|\psi_1\rangle = -\langle\psi_1|(E_1E_5\otimes I)|\psi_1\rangle.$$

However, a direct computation of $\langle\psi_1|(E_5E_1\otimes I)|\psi_1\rangle$ shows that

$$\langle\psi_1|(E_5E_1\otimes I)|\psi_1\rangle = \frac{1}{8}\sum_{i=0}^{7}\langle i|E_5E_1|i\rangle = \frac{1}{8}\mathrm{TR}(E_5E_1) = \frac{1}{8}\mathrm{TR}(E_1E_5) = \langle\psi_1|(E_1E_5\otimes I)|\psi_1\rangle,$$

and $\mathrm{TR}(E_1E_5) = \mathrm{TR}(I_4) + \mathrm{TR}(I\otimes\sigma_Z\sigma_X) = 4 \neq 0$. Hence, the glued magic square game is not rigid. □

Although this game is not a self-test, we know from Section 2.8 Alice's operators must provide a $|\psi\rangle$-representation for the solution group of glued magic square, and thus must satisfy particular group relations.

Chapter 3: Noncommutativity and constraint satisfaction problems

A general recipe for designing approximation algorithms for CSPs is to relax variables in the CSP so that they can take vector values rather than scalars. Then solve the vector problem which is often efficiently solvable. Finally round back the vector solution to a good solution of the original CSP. We introduce noncommutative CSPs in this chapter. When trying to come up with a framework for designing approximation algorithms for noncommutative CSPs, such as the one above, we immediately face a few choices. First, one has to make a decision about the underlying algebraic structure of the solutions. There could be multiple choices of algebras here. This choice will then determine the best overall strategy for a rounding scheme (which also involves multiple choices). This is very different from the world of classical CSPs where we already know the best approximation algorithm (assuming unique games conjecture). We explore our proposed framework in the first section. We then design deterministic and randomized approximation algorithms for a famous class of noncommutative CSPs.

In the second section, we shift the focus back to commutative CSPs and ask whether we could extract a good commutative solution from a given noncommutative solution. We propose a general rounding scheme that takes any noncommutative solution and produces a commutative solution. We introduce noncommutative Goemans-Williamson constants that describe how good this extracted commutative solution is. We state a conjecture regarding these constants, that if resolved, establishes that for a number of CSPs, one can always extract a good classical solution from any given noncommutative solution. The quality of this solution will be better than then the ones obtained by the best approximation algorithms in the literature. However, at this stage, we make no claims that the operator rounding technique can be executed efficiently. In particular, this does not refute the unique games conjecture.

3.1 Approximation algorithms for noncommutative CSPs

3.1.1 Noncommutative CSPs

Our goal in this section is to study a noncommutative variant of classical constraint satisfaction problems where we allow variables to take values in the ring of operators rather than the original commutative ring the classical CSP was defined over. This noncommutative analogue is of interest in quantum information as becomes clear shortly, but for now let us justify study of noncommutative CSPs quickly by recalling the example of the Magic-Square game that we saw in the earlier sections of this thesis. Magic-Square is a constraint satisfaction problem with nine variables taking values in the set $\{\pm 1\}$ and six equations as constraints. We saw that over this commutative domain these set of equations were inconsistent (we could not satisfy them all at the same time). However these set of equations are perfectly satisfiable when we considered instead of classical domain $\{\pm 1\}$ the set of unitaries with eigenvalues that are $\{\pm 1\}$. We saw that Magic-Square has important applications in the field of quantum information and this change of domain was not a mere mathematical curiosity.

In the classical theory of combinatorial optimization, we are often interested in constraint satisfaction problems in which we are given a number of variables $x_1, x_2, \ldots, x_n$ taking values in a finite commutative ring (usually the ring of integers modulo m) and a number of linear equations

$$a_1 x_1 + \cdots + a_n x_n = b$$

or inequations

$$a_1 x_1 + \cdots + a_n x_n \neq b$$

and our goal is to find the largest number of these constraints that can be satisfied simultaneously. In our discussion here we limit ourselves to the simplest class of these CSPs known as Max-2-Lin. These are CSPs where each equation or inequation involves exactly two variables. This class of CSPs include many interesting problems such as Max-k-Cuts and linear unique games. Max-

k-Cuts are those instances where we only have inequations as our constraints and linear unique games are those instances where we only have equations as our constraints.

In this section our focus is on CSPs with variables $x_1, \ldots, x_n$ taking values in the ring of integers mod m with constraints of the form

$$x_i - x_j = c_{ij},$$

or

$$x_i - x_j \neq c_{ij},$$

for all $i > j$. Let us also further imagine that each constraint (i, j) has a weight $w_{ij} \geq 0$ associated to it. Let us refer to the problem of maximizing the sum of weights of satisfied constraints as Max-2-Lin-m. We let $\mathcal{E}$ be the set of all pairs (i, j) such that the associated constraint is an equality constraint $x_i - x_j = c_{ij}$, and let $\mathcal{E}^c$ denote the complement, i.e, all pairs (i, j) such that the associated constraint is an inequation constraint $x_i - x_j \neq c_{ij}$.

In order to make the transition to a noncommutative analogue a bit easier to state let us rewrite the constraints multiplicatively. With a transformation $x_i \leftarrow \omega^{x_i}$ where $\omega = \exp(2\pi i/m)$ is an mth root of unity, we can rewrite the constraints multiplicatively as

$$x_i x_j^* = \omega^{c_{ij}},$$

if $(i, j) \in \mathcal{E}$ or otherwise

$$x_i x_j^* \neq \omega^{c_{ij}},$$

where * denotes complex conjugate.

Now a moment's thought shows that Max-2-Lin-m can be equivalently formulated as a polynomial optimization problem

$$\begin{aligned}\text{maximize:}\quad & \frac{1}{m}\sum_{(i,j)\in\mathcal{E}} w_{ij}\sum_{k=0}^{m-1}\omega^{-c_{ij}k}x_i^k x_j^{-k} + \frac{1}{m}\sum_{(i,j)\in\mathcal{E}^c} w_{ij}\sum_{k=1}^{m-1} 1-\omega^{-c_{ij}k}x_i^k x_j^{-k} \qquad (3.1.1)\\ \text{subject to:}\quad & x_i\in\{1,\omega,\dots,\omega^{m-1}\}.\end{aligned}$$

We are now ready to introduce the noncommutative analogue very easily. This is the problem of optimizing the above polynomial after relaxing the constraint that variables x_is must commute. Just like in the case of Magic-Square, the noncommutative analogue of the above CSP changes the domain of variables from mth roots of unity to unitary operators with eigenvalues that are mth roots of unity. To be precise, NC-Max-2-Lin-m asks what is the largest trace of all operators obtained by plugging in for x_is in the polynomial above, unitary operators with eigenvalues that are in the set $\{1,\omega,\dots,\omega^{m-1}\}$:

$$\begin{aligned}\text{maximize:}\quad & \frac{1}{m}\operatorname{tr}\sum_{(i,j)\in\mathcal{E}} w_{ij}\sum_{k=0}^{m-1}\omega^{-c_{ij}k}X_i^k X_j^{-k} + \frac{1}{m}\operatorname{tr}\sum_{(i,j)\in\mathcal{E}^c} w_{ij}\sum_{k=1}^{m-1} 1-\omega^{-c_{ij}k}X_i^k X_j^{-k} \qquad (3.1.2)\\ \text{subject to:}\quad & X_i^m = X_i^*X_i = 1.\end{aligned}$$

Everywhere in this section tr denotes the dimension-normalized trace.

Connection with nonlocal games

In the earlier parts of the thesis, we studied two-player nonlocal games extensively. Max-2-Lin problems can easily be formulated as a 2-player nonlocal game. In the game formulation, the referee samples two variables and sends one to Alice and the other to Bob. The winning condition is that Alice and Bob must be consistent if they received the same variable. Otherwise, if they received distinct variables their assignments must satisfy the corresponding constraint involving the two variables. It is very easy to see that the synchronous value of this game is proportional to the value of the Max-2-Lin instance, i.e., the largest number of constraints that can be satisfied simultaneously. Similarly, the synchronous quantum value is proportional to the value of the NC-

Max-2-Lin instance.[1]

3.1.2 A framework for designing approximation algorithms for noncommutative CSPs

We understand the theory of approximation algorithms for classical CSPs very well. In this section, we take the first step in developing a theory of approximation algorithms for NC-Max-2-Lin-m.

What is special about Max-2-Lin?

First, we explain why we are focusing on NC-Max-2-Lin CSPs. The general noncommutative CSPs reduce to general noncommutative polynomial optimization and as we elaborated in the previous sections this is a very hard undecidable problem. However, there is some evidence that NC-Max-2-Lin CSPs are easy, even easier than their classical counterpart. This phenomenon is extremely interesting and these last sections of the thesis are our attempts in trying to understand the phenomenon better.

Let us recount some of the evidence for this phenomenon. One piece of evidence is of course the fact that Max-Cut is NP-hard but NC-Max-Cut is in polynomial-time as we will see in a moment.

A second piece of evidence is that the UGC states that for every $\varepsilon, \delta > 0$ it is NP-hard to distinguish if the value of a unique game is larger than $1 - \varepsilon$ or at most δ. On the other hand

[1] We chose to work in the synchronous framework in this section because of the ease of exposition. Everything we develop here can be translated into the non-synchronous regime. There the form of the noncommutative polynomial that is being optimized is as follows: we have two sets of variables X_i (for Alice) and Y_j (for Bob). There is a commutation relation that must hold between Alice's variables and Bob's variables. Furthermore, in the non-synchronous regime, the optimization is over all states rather than tracial states. Putting all these together the non-synchronous version of (3.1.2) is

$$\begin{aligned}
\text{maximize:} \quad & \phi^*(\frac{1}{m} \sum_{(i,j)\in\mathcal{E}} w_{ij} \sum_{k=0}^{m-1} \omega^{-c_{ij}k} X_i^k Y_j^{-k} + \frac{1}{m} \operatorname{tr} \sum_{(i,j)\in\mathcal{E}^c} w_{ij} \sum_{k=1}^{m-1} 1 - \omega^{-c_{ij}k} X_i^k Y_j^{-k})\phi \\
\text{subject to:} \quad & X_i^m = X_i^* X_i = 1, \\
& Y_j^m = Y_j^* Y_j = 1, \\
& X_i Y_j = Y_j X_i.
\end{aligned}$$

where the optimization is over all Hilbert spaces $\mathcal{H}$, and operators X_i, Y_j and states ϕ over $\mathcal{H}$.

[92] gave an approximation algorithm for noncommutative unique games that flies in the face of UGC. Their algorithm guarantees that if the optimal solution of a noncommutative unique game has value $1 - \varepsilon$ then their algorithm produces a solution with value $1 - 4\varepsilon$.

What kind of approximation algorithm?

The rest of this section outlines the first steps towards developing a theory of approximation algorithms for NC-Max-2-Lin. In particular, we are interested in knowing the best approximation ratio of any approximation algorithm based on the basic SDP for NC-Max-2-Lin problems. This is in contrast with the approximation algorithm of [92] for noncommutative unique games because it does not yield an approximation ratio (although it is still based on the basic SDP). For example, one drawback of [92] is that in the regime where the value of the unique game is $1 - \varepsilon$ for $\varepsilon \geq 1/4$ their algorithm may not produce any interesting solution.

Review of Max-Cut

The simplest of all Max-2-Lin problems is the famous Max-Cut problem where an instance is a simple graph $G = (V, E)$ with variables x_i associated to every vertex $i \in V$. These variables are taking values in the set $\{\pm 1\}$. Our goal is to find an assignment such that the inequations $x_i \neq x_j$ are satisfied for as many edges (i, j) as possible. When additionally considering weighted graphs with weights $w_{ij} \geq 0$ over the edges, Max-Cut can be phrased as the following polynomial optimization problem

$$\begin{aligned} \text{maximize:} \quad & \sum_{(i,j)\in E} w_{ij} \frac{1 - x_i x_j}{2} \qquad (3.1.3) \\ \text{subject to:} \quad & x_i \in \{\pm 1\}. \end{aligned}$$

We observe that $\frac{1-x_ix_j}{2} = 1$ if $x_i \neq x_j$ and $\frac{1-x_ix_j}{2} = 0$ otherwise. Therefore $\sum_{(i,j) \text{ an edge}} w_{ij} \frac{1-x_ix_j}{2}$ is the sum of weights of all edges that cross the cut $(C, V \setminus C)$ where $C = \{i : x_i = 1\}$.

Approximation algorithms for classical CSPs and review of Goemans-Williamson

There is a framework of approximation algorithms for classical constraint satisfaction problems that involves first relaxing the domain of variables from the finite ring to a finite-dimensional vector space. The problem over this domain is now a semidefinite program and hence can be solved efficiently. The second step is then to round the vectors back to the true labels in the finite ring. There is a very beautiful theory that explains the effectiveness of this framework. For example by a celebrated result of Raghavendra [93], we know that for any CSP, the basic SDP (which we introduce shortly) achieves the best approximation ratio of any approximation algorithm as long as the unique games conjecture (UGC) holds.

For example the basic SDP for (3.1.3) is

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} \frac{1 - X_{ij}}{2} \\ \text{subject to:} \quad & X_{ii} = 1, \text{ for all } i, \\ & X \geq 0. \end{aligned} \tag{3.1.4}$$

Let us refer to this as the SDP-Max-Cut. This program can equivalently be written as

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} \frac{1 - \langle v_i, v_j \rangle}{2} \\ \text{subject to:} \quad & \|v_i\|_2 = 1, \text{ for all } i, \end{aligned} \tag{3.1.5}$$

where v_i's are vectors in $\mathbb{R}^n$ (where n is the number of vertices). Let us call this the vector-MAX-CUT problem. It should be clear that these two programs are the same and it should also be clear that they provide an upper-bound on (3.1.3). The celebrated Goemans-Williamson algorithm for Max-Cut starts by solving this SDP and obtaining vectors v_i. To round these vectors back to true binary labels x_i, they proposed the hyperplane rounding algorithm: Sample a unit vector r from the Haar measure and let $x_i = \text{sign}\langle r, x_i \rangle$. They then showed that random variables x_i have the property that

$$\mathbb{E}\frac{1 - x_i x_j}{2} = \Pr(x_i \neq x_j) = \frac{\arccos\langle x_i, x_j\rangle}{\pi} \geq 0.878\frac{1 - \langle v_i, v_j\rangle}{2}. \tag{3.1.6}$$

Therefore x_i's in (3.1.3) achieve a value that, in expectation, is at least 0.878 times the SDP value.

Noncommutative Max-Cut

Now let us switch the noncommutative analogue. The NC-Max-Cut is the problem

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij}\frac{1 - \langle X_i, X_j\rangle}{2} \\ \text{subject to:} \quad & X_i^* X_i = X_i^2 = 1, \end{aligned} \tag{3.1.7}$$

where the variables, instead of taking binary values $\{\pm 1\}$ in the original Max-Cut, are now taking values in the set of all unitaries with eigenvalues $\{\pm 1\}$ and in the objective function we replaced quadratic terms $x_i x_j$ with the dimension-normalized Hilbert-Schmidt inner products $\langle X_i, X_j\rangle = \mathrm{tr}(X_i^* X_j)$. Everywhere in this note * denotes Hermitian conjugate when on an operator.[2]

Review of Tsirelson's theorem

We know a lot about NC-Max-Cut in the quantum information literature, since they are essentially equivalent to XOR nonlocal games. Tsirleson [94] showed that this problem can be solved efficiently by just solving the basic SDP (3.1.4) which was also the SDP used in the Goemans-Williamson algorithm for solving Max-Cut. It should be clear that the basic SDP (3.1.4) is still a relaxation of the NC-Max-Cut. Tsirelson showed that in fact SDP-Max-Cut has the same value as NC-Max-Cut. Next we quickly review the theorem of Tsirelson.

Suppose we obtained optimal solution $v_1, \ldots, v_n$ for the vector-Max-Cut. We want to construct order-2 unitary operators X_i that achieve an objective value equal to the optimal value of the vector-

[2] NC-Max-Cut should not be confused with its cousin quantum-Max-Cut which is an instance of the local Hamiltonian problem.

Max-Cut. For this we first need to introduce Weyl-Brauer operators which generate what is known as Clifford algebras. This is the algebra with generators $\sigma_1, \ldots, \sigma_n$ and relations $\sigma_i^2 = 1$ and $\sigma_i\sigma_j = -\sigma_j\sigma_i$ for $i \neq j$. Now we construct operators $X_i = \sum_{j=1}^n v_{ij}\sigma_j$. Following the properties of Clifford algebra, it is easy to verify that X_i are a feasible solution of (3.1.7), i.e., X_i are unitary and are of order 2 (i.e., $X_i^* X_i = 1$ and $X_i^2 = 1$). Furthermore the objective value of this solution in (3.1.7) is the same as the optimal value of (3.1.4), since $\langle X_i, X_j \rangle = \langle v_i, v_j \rangle = X_{ij}$.

The algebraic framework for designing approximation algorithms for noncommutative CSPs

Unfortunately the moment we move on to Max-2-Lin problems with nonbinary variables this argument no longer goes through fully intact. The main reason for this unlucky situation is that there does not exist a proper generalization of the Clifford algebra to the nonbinary setting that has all the properties that we need. So all our attempts here would center around generalizing Clifford algebras to keep some desired properties and sacrifice some others. The less we sacrifice the better approximation ratio we recover in the end. Let us make this more clear.

Max-3-Cut To be concrete we first introduce the ternary analogue of Max-Cut called Max-3-Cut. Here the goal is to partition the vertices of the graph into at most three sets such that the number of edges crossing between partitions is maximized. So just like Max-Cut the instance is a graph with variable x_i associated to vertex i. Variables take value in the ternary set $\{1, \omega, \omega^2\}$, where $\omega = exp(2\pi i/3)$ is a third root of unity. The constraints are $x_i \neq x_j$ for every edge (i, j). It is easily seen that Max-3-Cut is equivalent to the polynomial optimization

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} \frac{2 - x_i^* x_j - x_j^* x_i}{3} \qquad (3.1.8) \\ \text{subject to:} \quad & x_i \in \{1, \omega, \omega^2\}. \end{aligned}$$

The NC-Max-3-Cut is similarly defined to be

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} \frac{2 - \langle X_i, X_j \rangle - \langle X_j, X_i \rangle}{3} \\ \text{subject to:} \quad & X_i^* X_i = X_i^3 = 1, \end{aligned} \tag{3.1.9}$$

and where the domain is the set of unitaries with eigenvalues that are $\{1, \omega, \omega^2\}$.

The reason we had success in the case of binary Max-Cut was the existence of the Weyl-Brauer operators $\sigma_1, \ldots, \sigma_n$ that allowed us to construct feasible solution of the noncommutative problem from the vectors feasible in the SDP problem. The properties of these operators gave us

1. that $A = \sum_i a_i \sigma_i$ is an order-2 unitary whenever $a \in \mathbb{R}^n$ and $\|a\|_2 = 1$,
2. and that the inner product of two operators $A = \sum_i a_i \sigma_i$ and $B = \sum_j b_j \sigma_j$ is exactly the inner product $\langle a, b \rangle$ of the vectors of coefficients.

Generalized Weyl-Brauer Now for this program to carry over to the case of NC-Max-3-Cut, we must seek out a number of generalized Weyl-Brauer operators $\sigma_1, \sigma_2, \ldots, \sigma_n$ such that $A = \sum_i a_i \sigma_i$ is an order-3 unitary whenever some simple criterion on $a \in \mathbb{R}^n$ with $\|a\|_2 = 1$ is satisfied. First one immediately observes that σ_i's themselves must be order-3 unitaries (consider the case where the vector a is 1 at entry i and 0 everywhere else). Now for A to be a unitary we need

$$\sigma_i^* \sigma_j = -\sigma_j^* \sigma_i \tag{3.1.10}$$

for all $i \neq j$. For A to be order 3 we need

$$\sigma_i \sigma_j = \omega \sigma_j \sigma_i \tag{3.1.11}$$

for all $j > i$ and that $\|a\|_3 = 1$. The exotic anticommutation relations (3.1.10) and (3.1.11) each can be satisfied separately but not simultaneously. Even when $n = 2$, imposing these sets of relations results in an algebra where $1 = 0$, i.e., the 0-algebra (the algebra consisting only of 0). Therefore the criteria for unitariness $A^*A = 1$ and order-3-ness $A^3 = 1$ are not compatible with one another.[3]

So at the stage of relaxation, there are two possibilities for designing an approximation algorithm for NC-Max-3-Cut. If we sacrifice order-3-ness of $A = \sum_i a_i \sigma_i$ we get the algebra with relations

$$\sigma_i^3 = \sigma_i^* \sigma_i = 1, \sigma_i^* \sigma_j = -\sigma_j^* \sigma_i \text{ for } i \neq j \tag{3.1.12}$$

in which case $A = \sum_i a_i \sigma_i$ is a unitary for free whenever $a \in \mathbb{R}^n$ and $\|a\|_2 = 1$. If we proceed with this choice then the rounding scheme involves obtaining an operator $\widetilde{A}$ from A that is unitary and order-3. For example, from linear algebra we know that for any unitary A with spectral decomposition UDU^*, the closest order-3 unitary to A in Frobenious norm is $\widetilde{A} = U\widetilde{D}U^*$ where $\widetilde{D}$ is obtained from D by replacing each diagonal entry λ with the closest third root of unity $\widetilde{\lambda}$ to λ. This is one possible rounding scheme. However, in this section, we propose a better rounding scheme.

Alternatively we could sacrifice unitariness of $A = \sum_i a_i \sigma_i$, and get the algebra with relations

$$\sigma_i^3 = \sigma_i^* \sigma_i = 1, \sigma_i \sigma_j = \omega \sigma_j \sigma_i \text{ for } i \neq j \tag{3.1.13}$$

in which case $A = \sum_i a_i \sigma_i$ is such that A^3 is a scalar operator whenever $a \in \mathbb{R}^n$ and $\|a\|_2 = 1$. If we proceed with this choice then the rounding scheme involves obtaining an operator $\widetilde{A}$ from A that is unitary and order-3. For example, from linear algebra, we know that for any operator A with singular value decomposition UDV^* the closest unitary to A in Frobenius norm is $\widetilde{A} = UV^*$.

Each of these two relaxation and rounding schemes leads to qualitatively different approximation algorithm with different approximation ratios. This makes the task of designing approximation algorithms for NC CSPs so much more flavourful and interesting. Here we only considered the extreme case of choosing one property over another property. One could also imagine relaxation to algebras that preserves both properties (of unitariness and order-3-ness) to some degree.

It turns out that sacrificing any of the two properties of unitary or order-3, the operator A we

[3] The exotic anticommutation (3.1.11) is a sufficient condition for A to be order-3. The necessary condition is the more general relation of $\sigma_i^2 \sigma_j + \sigma_i \sigma_j \sigma_i + \sigma_j * \sigma_i^2 = \lambda I$ where λ could be any complex number and I is the identity matrix. One can also show that the only algebra with this relation and (3.1.10) is the 0-algebra.

obtain at the end is going to satisfy the sacrificed property almost exactly. Therefore each of these approaches would lead to good approximation algorithms. Let us see an example now.

Representations of generalized Weyl-Brauer We study the case of (3.1.10), i.e., sacrificing order-3-ness. For every n, there exist operators $\sigma_1, \sigma_2, \ldots, \sigma_n$ such that $\sigma_i^* \sigma_i = 1$, $\sigma_i^3 = 1$, and $\sigma_i^* \sigma_j = -\sigma_j^* \sigma_i$ for all $i \neq j$. One needs to work a little to prove this existence. Here we are going to establish the existence only in high level terms. First consider the group with presentation

$$G_n = \langle \sigma_1, \ldots, \sigma_n, J : \sigma_i^3, J^2, [J, \sigma_i], J(\sigma_i^{-1} \sigma_j)^2 : \text{ for all } i \neq j \rangle$$

where we have $n+1$ generators, the special generator J commutes with every other generators and is of order 2, and we have this exotic relation $\sigma_i^{-1} \sigma_j = J \sigma_j^{-1} \sigma_i$. Generator J is clearly playing the role of -1. Now consider the subgroup P_n generated by $\sigma_i^{-1} \sigma_j$ for all i, j. With a little work one can show that P_n is indeed isomorphic to the Pauli group (the defining property of the Pauli group is that every pair of element either commutes or anticommutes and this is clearly the case with P_n by construction). Furthermore one immediately observes that conjugation by σ_i preserves P_n. Therefore σ_i belongs to the Clifford group (Clifford group is the group of automorphisms of the Pauli group and should not be confused with Clifford algebras that appeared earlier in this note). Now resorting to the simple representation theory of Pauli and Clifford groups, one can show that for every n, G_n has an irreducible that sends $J \mapsto -1$. This proves the existence of the operators with our desired exotic anticommutation.

A deterministic approximation algorithm for NC-Max-3-Cut

We now have everything to design an approximation algorithm for NC-Max-3-Cut. With the exotic anticommutation of type (3.1.10), it is a matter of simple calculations to observe that $A = \sum a_i \sigma_i$ for $a \in \mathbb{R}^n$ is a unitary if and only if $\|a\|_2 = 1$. How do we use this algebra to solve

NC-Max-3-Cut? Well just like before we have a basic SDP relaxation. The basic SDP is:

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} \frac{2 - X_{ij} - X_{ji}}{3} \\ \text{subject to:} \quad & X_{ii} = 1, \text{ for all } i, \\ & X \geq 0. \end{aligned} \tag{3.1.14}$$

We can always assume without loss of generality that the optimal solution X of this SDP is real, because $(X + X^*)/2$ is also a feasible solution with the same objective value as X. So we can rewrite the above SDP as

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} \frac{2 - X_{ij} - X_{ji}}{3} \\ \text{subject to:} \quad & X \in \mathbb{R}^{n \times n}, \\ & X_{ii} = 1, \text{ for all } i, \\ & X \geq 0. \end{aligned} \tag{3.1.15}$$

Furthermore, we can always assume that $X_{ij} \geq -1/2$. To prove this one needs to go to the second-level SDP relaxation of NC-Max-3-Cut. First observe that for any pair of order-3 unitary operators X_i and X_j, the 3-by-3 matrix

$$\begin{bmatrix} 1 & \langle X_i, X_j \rangle & \langle X_j, X_i \rangle \\ \langle X_j, X_i \rangle & 1 & \langle X_i, X_j \rangle \\ \langle X_i, X_j \rangle & \langle X_j, X_i \rangle & 1 \end{bmatrix}$$

must be positive semidefinite. This is because if we let $M = x_i, N = x_j, P = X_j^{-1} X_i^{-1}$, then

$$\begin{bmatrix} 1 & \langle X_i, X_j \rangle & \langle X_j, X_i \rangle \\ \langle X_j, X_i \rangle & 1 & \langle X_i, X_j \rangle \\ \langle X_i, X_j \rangle & \langle X_j, X_i \rangle & 1 \end{bmatrix} = \begin{bmatrix} 1 & \langle M, N \rangle & \langle M, P \rangle \\ \langle N, M \rangle & 1 & \langle N, P \rangle \\ \langle P, M \rangle & \langle P, N \rangle & 1 \end{bmatrix} \geq 0.$$

For this to be true it is not too difficult to show that it must hold that $\langle X_i, X_j\rangle + \langle X_j, X_i\rangle \geq 1$. Now since we can assume these inner products are real we conclude that $\langle X_i, X_j\rangle$ is at least $-1/2$. This is enough to show that the following SDP is a relaxation of the NC-Max-3-Cut

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} \frac{2 - X_{ij} - X_{ji}}{3} \qquad (3.1.16)\\ \text{subject to:} \quad & X \in \mathbb{R}^{n\times n} \\ & X_{ii} = 1, \\ & X_{ij} \geq -1/2, \\ & X \succeq 0. \end{aligned}$$

We call this the basic SDP for Max-3-Cut.

Now let X be a feasible solution in this SDP and let v_i be vectors such that $\langle v_i, v_j\rangle = X_{ij}$. If we now construct operators $X_i = \sum_j v_{ij}\sigma_j$ (where σ_j are the generalized Weyl-Brauer operators), we immediately get that X_i are unitary. Unfortunately however they are not a feasible solution to NC-Max-3-Cut because they are not order-3. However we are lucky in that X_i are not too far from being order-3. Let us make this precise. First note that just like before we have the inner product property that $\langle X_i, X_j\rangle = \langle v_i, v_j\rangle$. This follows from the representation theory of the Pauli group P_n that states that in the unique nontrivial irreducible of the Pauli group every representing matrix is traceless except for the identity operator. Finally since $\sigma_i^*\sigma_j \in P_n$ we have $\langle \sigma_i, \sigma_j\rangle = \text{tr}(\sigma_i^*\sigma_j) = 0$.

Now if X_i and X_j were order-3, then we would have had

$$\langle X_i^2, X_j^2\rangle = \langle X_i^*, X_j^*\rangle = \langle X_j, X_i\rangle = \langle v_j, v_i\rangle = \langle v_i, v_j\rangle = \langle X_i, X_j\rangle. \qquad (3.1.17)$$

Even though X_i and X_j are not generally order-3, something close to the identity (3.1.17) holds:

$$\langle X_i^2, X_j^2\rangle = \langle X_i, X_j\rangle^2. \qquad (3.1.18)$$

This equality, which states that the inner product of squares is the square of the inner product, follows again from the representation theory of G_n (in particular it relies on the Pauli subgroup P_n of G_n and the fact that the unique nontrivial irreducible of the Pauli group has the property that all the representing matrices are traceless).

The final step is a rounding scheme to produce order-3 unitaries $\widehat{X}_i$ from X_i. We use the following simple construction. We let

$$\widehat{X}_i = \begin{bmatrix} 0 & X_i & 0 \\ 0 & 0 & X_i \\ X_i^{-2} & 0 & 0 \end{bmatrix}.$$

These operators are now unitary and order-3. Furthermore using the square law (3.1.18), we can write

$$\langle \widehat{X}_i, \widehat{X}_j \rangle = \frac{2}{3}\langle X_i, X_j \rangle + \frac{1}{3}\langle X_i, X_j \rangle^2 = \frac{2}{3}X_{ij} + \frac{1}{3}X_{ij}^2,$$

and putting all these together

$$\frac{2 - \langle \widehat{X}_i, \widehat{X}_j \rangle - \langle \widehat{X}_j, \widehat{X}_i \rangle}{3} = (1 + \frac{1}{3}X_{ij})(\frac{2 - X_{ij} - X_{ji}}{3}) \geq \frac{5}{6}(\frac{2 - X_{ij} - X_{ji}}{3}),$$

in which we used the fact that $X_{ij} \geq -1/2$. So the objective value of the $\widehat{X}_i$ in NC-Max-3-Cut is at least $\frac{5}{6}$ times the SDP value. This gives a $\frac{5}{6}$-approximation algorithm for NC-Max-3-Cut.

This approach can be easily modified (by modifying the group G_n) to all NC-Max-k-Cuts. For example the approximation ratio of our deterministic rounding method for $k = 3, 4, 5$ is $0.83333, 0.85185, 0.86718$, respectively. The paper [95] achieves an approximation ratio (with respect to the same SDP but using randomized rounding method) for the original Max-k-Cut that is slightly better than our approximation ratios. However the analysis of this algorithm is much more complicated. In fact it took about seven years since the publication of [95] and the work of many authors culminating in [96], that achieved expected ratios that are larger than our simple deterministic algorithm. In the next section we suggest a randomized rounding algorithm that may achieve approximation ratios that are much larger than the work of [95], although at this point this is still conjectural. For example we think our randomized rounding algorithm achieves an expected approximation ratio of $13/15 = 0.86666$ for NC-Max-3-Cut problem.

Randomized rounding

In the previous sections, we analysed a deterministic approximation algorithm for NC-Max-k-Cut problems. Here we outline how we may improve the approximation ratios using randomized rounding. We again focus on the case of Max-3-Cut.

We saw earlier that operators that are constructed from linear combinations of generalized Weyl-Brauer σ_i, though not order 3, are close to being order 3. The closeness property we used was that $\langle A^2, B^2 \rangle$ is close to $\langle A, B \rangle$ whenever A, B are linear combinations of generalized Weyl-Brauer operators (indeed if A, B were order-3 then $\langle A^2, B^2 \rangle = \langle A, B \rangle$). We were able to then take advantage of this property and design a deterministic approximation algorithm that achieved a ratio of $5/6$. In this section we observe another metric under which these operators A, B are close to being order 3. We then use this metric to design a randomized approximation algorithm that does better than the algorithm in the previous section. So when designing and analysing approximation algorithms for NC-Max-k-Cut, together with the choice of algebra, one also has to make a decision on a proper metric. This metric dictates how closely the operators obtained from SDP are satisfying the sacrificed property, in this case order-3-ness.

For λ a complex number with modulus 1, we let $\widetilde{\lambda}$ denote the closest third root of unity to λ. Suppose $\lambda = e^{i\theta}\omega^k$ for some $|\theta| < \pi/3$ and $k \in \{0, 1, 2\}$. Then $\widetilde{\lambda} = \omega^k$ and thus $\lambda\widetilde{\lambda}^* = e^{i\theta}$. The closer λ is to a third root of unity, the larger the real part of $\lambda\widetilde{\lambda}^*$. So $\text{real}(\lambda\widetilde{\lambda}^*)$ is a sort of fidelity measure for how close λ is to a third root of unity. To get a sense for this quantity note that if we sample λ uniformly from the unit circle in the complex plane then the fidelity $\text{real}(\lambda\widetilde{\lambda}^*)$ is on average $\frac{\cos(\pi/6)}{\pi/3} = \frac{3\sqrt{3}}{2\pi} \approx 0.82699$.

Similarly given a unitary operator U we can always find the closest order-3 unitary $\widetilde{U}$. In fact if the spectral decomposition is $U = \sum \lambda_i \phi_i \phi_i^*$ with eigenvalues λ_i, then by Hoffman-Wielandt theorem [97], we have $\widetilde{U} = \sum \widetilde{\lambda}_i \phi_i \phi_i^*$. The closeness is in the sense that $\|U - \widetilde{U}\| \leq \|U - V\|$ for all order-3 unitary V and where $\| \cdot \|$ is the Frobenius norm. Now inspired by the scalar case we define the fidelity of U to be $\langle \widetilde{U}, U \rangle = \frac{1}{\dim(U)} \sum \lambda_i \widetilde{\lambda}_i^*$. If we sample U from the Haar measure, the marginal distribution of every eigenvalue λ_i is uniform over the unit circle. So on expectation the fidelity of a Haar random unitary is also $\frac{3\sqrt{3}}{2\pi}$.

What is the fidelity for our special operators $A = \sum a_i \sigma_i$? Well we have strong numerical evidence that when $a \in \mathbb{R}^n$ is sampled from the Haar measure on the unit sphere of the 2-norm, the fidelity $\langle \widetilde{A}, A \rangle$ on expectation is at least $0.84 > \frac{3\sqrt{3}}{2\pi}$. If one can prove this numerical observation, this then leads to a proof that the following randomized approximation algorithm has an approximation ratio of $\frac{13}{15} = 0.8\bar{6}$ on expectation:

1. Solve the SDP (3.1.16) to obtain optimal solution X
2. Obtain vectors $u_i \in \mathbb{R}^n$ such that $\langle u_i, u_j \rangle = X_{ij}$
3. Sample orthogonal matrix Q acting on $\mathbb{R}^n$ from the Haar measure and let $v_i = Q u_i$
4. Construct operators $X_i = \sum_j v_{ij} \sigma_j$
5. Output operators $\widetilde{X_i}$

This is much better than the approximation ratio of $5/6 = 0.8\bar{3}$ we gave in the previous section using a deterministic algorithm.

Earlier we mentioned two types of exotic anticommutations (3.1.10) and (3.1.11). We so far used the algebra generated by relation (3.1.10) to obtain the above approximation algorithms. One could similarly design approximation algorithms using the algebra generated by relation (3.1.11). Also, everything we said carries over to the case of noncommutative Max-k-cut for larger k. For any given noncommutative combinatorial optimization problem there could be many choices for a natural algebra that fit the problem best. Each of these algebras and their representations, following the basic recipe that we outlined here, give rise to approximation algorithms (although each one will achieve different ratios and require its own analysis).

Open problems

We close this section with a few open problems:

1. What is the integrality gap of the basic SDP for NC-Max-k-Cut problems?

2. Is basic SDP the best for designing approximation algorithms for noncommutative CSPs? For example could we hope to have a theory similar to Raghavendra's result [93], that shows that the best approximation ratio of any approximation algorithm for any NC-Max-2-Lin problem is the same as the integrality gap of the basic SDP for that NC-Max-2-Lin problem (assuming of course UGC)?

3. Does the approximation ratio for our randomized rounding algorithm for NC-Max-k-Cut achieve the integrality gap of the basic SDP?

   We know that assuming UGC, for classical Max-k-Cut the algorithm of [95] is asymptotically optimal (that is as $k \to \infty$) and achieves the integrality gap of the basic SDP. This is first proved in [98]. However for small values, for example when $k = 3, 4, 5$, the best hardness of approximation results are far from the guarantees of the algorithm in [95].

4. (Finite-dimensionality of optimal solutions) All the indications are that NC-Max-3-Cut are the simplest noncommutative CSPs that are still harder than the NC-Max-Cut. However for all we know there could exist instances of NC-Max-3-Cut such that the optimal solution could only be attained over infinite-dimensional Hilbert spaces. Could this be exhibited by an example or else refuted by showing that the optimal solution of all NC-Max-3-Cut instances are finite-dimensional? It is quite fascinating to us that we do not have tools that could prove finite-dimensionality for any class of non-local games aside from the case of NC-Max-Cut.

5. Crucial to the design of our approximation algorithm using the generalized Weyl-Brauer operators satisfying relations (3.1.12) was that the basic SDP for Max-k-Cut (for example (3.1.15) in the case of Max-3-Cut) could be assumed is real without loss of generality. This

was essential because $A = \sum_i a_i\sigma_i$ is a unitary whenever a is a real vector and $\|a\|_2 = 1$. The criterion for unitariness of A is more complicated when a is a complex vector.

However for Max-2-Lin problems with equations in the constraints (as opposed to inequations which was the case with Max-k-Cuts), we cannot assume that the basic SDP is real. For example consider ternary linear unique games. An instance of this problem is a set of variables $x_1, \ldots, x_n$ taking values in $\{1, \omega, \omega^2\}$ and constraints are equations $x_i x_j^* = \omega^{c_{ij}}$ for every $i > j$. Then we can immediately phrase this CSP as

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} \frac{1 + \omega^{c_{ij}} x_i^* x_j + \omega^{-c_{ij}} x_j^* x_i}{3} \\ \text{subject to:} \quad & x_i \in \{1, \omega, \omega^2\}. \end{aligned} \tag{3.1.19}$$

The noncommutative analogue is now the problem

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} \frac{1 + \omega^{c_{ij}} \langle X_i, X_j \rangle + \omega^{-c_{ij}} \langle X_j, X_i \rangle}{3} \\ \text{subject to:} \quad & X_i^3 = X_i^* X_i = 1. \end{aligned} \tag{3.1.20}$$

Finally the basic SDP is

$$\begin{aligned} \text{maximize:} \quad & \sum w_{ij} \frac{1 + \omega^{c_{ij}} X_{ij} + \omega^{-c_{ij}} X_{ji}}{3} \\ \text{subject to:} \quad & X \in \mathbb{C}^{n \times n}, \\ & X_{ii} = 1, \\ & X_{ij} + X_{ji} \geq -1, \\ & X \geq 0. \end{aligned} \tag{3.1.21}$$

What algebra is best suited for designing approximation algorithms for this problem?

3.2 Classical solutions from noncommutative ones

In the last section we saw how we may solve noncommutative CSPs. Of course the noncommutative problem could be considered a relaxation of the original classical problem. For example when the variables take values ± 1 in the orignal problem, the noncommutative problem allows the variables to be the higher dimensional generalization of ± 1: Unitaries with eigenvalues ± 1.

Is there a sense in which the noncommutative problem is more general than the classical problem? Could we for example always recover a good classical solution from any noncommutative solution? What is the best rounding scheme for that? We investigate these questions in this section.

The idea of relaxing a constraint satisfaction problem so that variables, rather than assuming values in a finite set, say ± 1, can now be higher dimensional analogues of $\{\pm 1\}$, say unit normed vectors, has a beautiful history that (at least when combined with semidefinite programming techniques) started with the celebrated Goemans-Williamson algorithm for Max-Cut [99]. In [99] and the revolution that ensued, the higher-dimensional analogues are always vectors. Even if in the original problem the finite set had the structure of a ring (for example integers mod m), in the higher dimensional analogues studied in the literature we would have always lost this structure (we cannot multiply the vectors). The noncommutative relaxation on the other hand preserves the ring structure. In the rest of this note we argue that the noncommutative route is superior: more information about the classical problem is preserved in the noncommutative solution.

In the previous section we saw the vector relaxation approach to Max-Cut, the Goemans-Williamson algorithm, and its analysis. How much of this story extends to Max-k-Cut? In Max-k-Cut even the random assignment to $x_i \in \{1, \omega, \ldots, \omega^{k-1}\}$ achieves a cut that is on expectation of size $\frac{k-1}{k}$ times the number of edges. The best approximation ratio for Max-3-Cut, to this day, is also given by Goemans-Williamson [100] and is 0.836008. This is obtained by an algorithm that is very similar to the one they gave for Max-Cut. The staring point is to solve the basic SDP relaxation (3.1.16) (remember this was also the starting point of our algorithm for noncommutative Max-3-Cut). After obtaining the optimal solution X they obtain vectors v_i such that $\langle v_i, v_j \rangle = X_{ij}$.

Finally the rounding procedure samples three vectors r_0, r_1, r_2 independently and uniformly at random. Now if $\langle r_k, v_i \rangle = \max(\langle r_0, v_i \rangle, \langle r_1, v_i \rangle, \langle r_2, v_i \rangle)$, let $x_i = \omega^k$. Unlike Max-Cut the analysis of this rounding procedure and proof of the approximation ratio of 0.836 is much more complicated. Also unlike Max-Cut where we know that the 0.878 approximation ratio of Goemans-Williamson is optimal up to the unique games conjecture, no such result is known for Max-3-Cut. We only know we cannot do better than 0.944 unless $\mathsf{P} = \mathsf{NP}$ [101].

We propose a rounding scheme to round noncommutative solutions to commutative ones.[4] Suppose X, Y are given order-m unitaries. We want to obtain scalars $x, y \in \{1, \omega, \ldots, \omega^{m-1}\}$ such that some objective polynomial $f(x, y)$ (or rather its expectation if the rounding procedure is randomized) is as close as possible to $\operatorname{tr}(f(X, Y))$. For example for Max-Cut the objective polynomial of interest is $f(x, y) = \frac{1-xy}{2}$. The effectiveness of the rounding procedure depends on the polynomial f. The rounding scheme we propose here seem to work well with Max-k-Cut problems at least when evaluated numerically. This will become clear shortly.

For the remainder of this section we further assume that operators X, Y are traceless. This is justified because for all Max-2-Lin instances if $X_1, \ldots, X_n$ is a noncommutative solution then so are the m-by-m block matrices

$$\widehat{X_i} = \begin{bmatrix} 0 & X_i & 0 & \cdots & 0 \\ 0 & 0 & X_i & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & X_i \\ X_i & 0 & 0 \cdots & 0 & \end{bmatrix}.$$

Furthermore the objective value of $\widehat{X_i}$ and X_i are the same and $\widehat{X_i}$ are traceless.

Now we explain the rounding scheme. Sample a traceless order-k unitary R from Haar measure.[5] Now consider the m-simplex on the complex plane inscribed in the unit circle with the

[4] At this moment we do not worry about the efficiency of this rounding scheme.

[5] To be precise the distribution is over all matrices UDU^* where the unitary U is sampled from Haar measure and the traceless diagonal matrix D with $\{1, \omega, \ldots, \omega^{m-1}\}$ on its diagonal entries is sampled uniformly at random.

m-roots of unity $\{1, \omega, \ldots, \omega^{m-1}\}$ as its vertices. It is straightforward to verify that the inner product $\langle R, X\rangle$ falls in this simplex. We let x (resp. y) be the closest root of unity (i.e., the closest vertex of the simplex) to $\langle R, X\rangle$ (resp. $\langle R, Y\rangle$).

Let us go back to Max-Cut and discuss the effectiveness of this rounding procedure. For this we need to calculate the largest ρ such that $\mathbb{E}(1-xy) \geq \rho(1-\langle X, Y\rangle)$. This quantity could depend on the dimension k of operators X, Y. So we want to know the largest nonnegative real number ρ_k for which $\mathbb{E}(1-xy) \geq \rho_k(1-\langle X, Y\rangle)$ for all traceless order-2 unitaries X, Y acting on a Hilbert space of dimension k.

If $k = 2$ then we can immediately show that ρ_k is exactly the Goemans-Williamson constant 0.878.[6] At dimension four this quantity provably drops to about 0.85. From there on as we increase the dimension this quantity rapidly increases back again to the Goemans-Williamson constant as we observed from extensive numerical analysis. In other words it seems that $\rho_k \to \rho_2 = 0.878$, from below, as $k \to \infty$. We state this as a conjecture in a moment. We then propose one way of proving this conjecture in the next section.

For every m and $k \geq m$ we can define a noncommutative Goemans-Williamson constant $\rho_{m,k}$: This is the largest nonnegative real number for which

$$\mathbb{E}\sum_{i=1}^{m-1} 1 - x^{-i}y^{i} \geq \rho_{m,k}\sum_{i=1}^{m-1} 1 - \langle X^{i}, Y^{i}\rangle$$

for all traceless order-m unitary X, Y acting on a k-dimensional Hilbert space and where x, y are random variables obtained from the randomized rounding scheme we proposed above.

Conjecture 3.1. *It holds that $\rho_{m,k} \to \rho_{m,m}$ as $k \to \infty$.*

Since every noncommutative solution can be trivially embedded into a larger dimensional solution, assuming this conjecture, we can always recover a classical solution to Max-Cut from a noncommutative solution in such a way that the objective value of the rounded classical solution is

[6] We can also show that if X, Y are linear combinations of the generators of the Weyl-Brauer operators of any dimension then $\mathbb{E}(1-xy) \geq 0.878(1-\langle X, Y\rangle)$.

at least 0.878 times the objective value of the noncommutative solution. So in the case of Max-Cut this operator rounding scheme cannot do better than the vector rounding of Goemans-Williamson.

However this story becomes much more interesting in the case of Max-k-Cut for $k \geq 3$. We mentioned that the approximation algorithm of Goemans-Williamson based on vector rounding achieved a ratio of 0.836 in Max-3-Cut. However assuming the above conjecture, the classical solution obtained from rounding a noncommutative solution achieves a value of $\rho_{3,3}$ times the value of the noncommutative solution. The constant $\rho_{3,3}$ is something we can estimate very well by estimating a simple integral. This value is at least 0.89 which is much larger that the ratio of 0.836 obtained from vector relaxation.

3.2.1 The geometric picture

In this section, we focus on the conjecture for when $m = 2$. We first need to study the quantity

$$\mathbb{E}\frac{1 - xy}{2} = \mathrm{PR}(\mathrm{sign}\langle R, X\rangle \neq \mathrm{sign}\langle R, Y\rangle)$$

a little more carefully. Recall that in the Goemans-Williamson algorithm for Max-Cut this quantity was exactly $\frac{\theta}{\pi}$ where the θ was the angle between the vector relaxations. It turns out that this geometric picture in the form of angles plays a significant role in the noncommutative story as well. Next, we present this geometric picture in the noncommutative case.

Suppose X, Y are traceless order-2 unitaries of dimension $2k$. Then $P = (1 + X)/2$ and $Q = (1 + Y)/2$ are projections onto two k-dimensional subspaces $\mathcal{X}, \mathcal{Y}$ respectively. From the work of Jordan [102] we can associate k canonical angles $0 \leq \theta_1 \leq \cdots \leq \theta_k \leq \pi/2$ between these two subspaces. These angles are exactly the arccos of the singular values of the operator PQ. This all means that there are orthonormal bases $x_1, \ldots, x_k$ and $y_1, \ldots, y_k$ for $\mathcal{X}, \mathcal{Y}$ such that θ_i is the angle between x_i and y_i and $PQ = \sum_i \cos(\theta_i) x_i y_i^*$.

Now by CS-decomposition [103] (also known as Jordan's lemma in quantum information community), we know there is a change of basis such that X, Y are block diagonal matrices with 2-by-2 block matrices

$$X_i = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, Y_i = \begin{bmatrix} \cos(2\theta_i) & \sin(2\theta_i) \\ \sin(2\theta_i) & -\cos(2\theta_i) \end{bmatrix}$$

on the diagonal. Read more on canonical angles and CS-decomposition in Chapter 7 of Matrix Analysis [104].

Since our rounding scheme is independent of change of basis we see that the quantity $\mathbb{E}\frac{1-xy}{2}$ is only a function of the canonical angles. We can prove that when canonical angles are all the same $\theta_1 = \cdots = \theta_k = \theta$, then

$$\mathbb{E}\frac{1-xy}{2} = \frac{2\theta}{\pi} = \frac{\arccos\langle X, Y\rangle}{\pi}.$$

This is exactly the same quantity as in the vector relaxation, so in this case the noncommutative setting recovers the vector setting.

In general this quantity $\mathbb{E}\frac{1-xy}{2}$ is rather tough to precisely calculate, but there is always a good approximation of this quantity by simple trigonometric functions. For example when $k = 2$, we get that $\mathbb{E}\frac{1-xy}{2} \approx \frac{1}{2}(1 - \cos(\theta_1) + \sin(\theta_2))$.

Finally numerical evidence strongly suggests the following conjecture

Conjecture 3.2. *The quantity* $\mathbb{E}\frac{1-xy}{2}$ *approaches*

$$\frac{2\theta_1 + \cdots + 2\theta_k}{k\pi}$$

from below as $k \to \infty$*.*

If one proves this conjecture, this immediately proves our previous conjecture that $\rho_{2,2k} \to \rho_{2,2} = 0.878$ as $k \to \infty$. This is because we already know from Goemans-Williamson that $\frac{2\theta}{\pi} \geq 0.878\frac{1-\cos(2\theta)}{2}$ for all $\theta \in [0, \pi/2]$, and thus

$$\frac{2\theta_1 + \cdots + 2\theta_k}{k\pi} \geq 0.878\frac{1 - \langle X, Y\rangle}{2}.$$

More work is needed to fully understand this quantity and the noncommutative Goemans-

Williamson constant.

3.2.2 Back to the algebraic picture

We saw that when the angles between subspaces are the same we recover the vector setting. So when is it that the canonical angles are all the same? To answer this first note the anticommutator of the blocks satisfy

$$X_iY_i + Y_iX_i = \begin{bmatrix} 2\cos(2\theta_i) & 0 \\ 0 & 2\cos(2\theta_i) \end{bmatrix} = 2\cos(2\theta_i)I.$$

So we get that the canonical angles are all the same $\theta_1 = \cdots = \theta_n = \theta$ if and only if $XY + YX$ is a scalar matrix.

This relation is something we know a lot about. We know that operators $X_1, \ldots, X_n$ for which pariwise anticommutators $X_iX_j + X_jX_i$ are scalars generate the Clifford algebra. As we saw earlier in this note, the noncommutative solution that Tsirelson's theorem gives us for the NC-Max-Cut are also elements of the Clifford algebra (Weyl-Brauer operators generate the Clifford algebra). Therefore together with the remarks we made in the previous section, our operator rounding scheme for noncommutative solutions recovers the Goemans-Williamson ratio of 0.878.

In fact in the case of Clifford solutions we can replace our rounding scheme by a scheme that is far more efficient. Suppose $X = a_1\sigma_1 + \ldots + a_n\sigma_n, Y = b_1\sigma_1 + \ldots + b_n\sigma_n$ are linear combinations of the Weyl-Brauer operators $\sigma_1, \ldots, \sigma_n$. Sample vector $r \in \mathbb{R}^n$ from the unit sphere of 2-norm and let $R = r_1\sigma_1 + \cdots + r_n\sigma_n$. Also let $x = \text{sign}\langle R, X\rangle = \text{sign}\langle r, a\rangle$ and $y = \text{sign}\langle R, Y\rangle = \text{sign}\langle r, b\rangle$. Then on expectation $1 - xy$ is at least $0.878(1 - \langle X, Y\rangle) = 0.878(1 - \langle a, b\rangle)$. This is exactly the hyperplane rounding algorithm of Goemans-Williamson restated in the language of operators.

It seems that this connection between angles and the Weyl-Brauer operators is preserved when we move to generalizations of Weyl-Brauer operators to order-k operators by means of the exotic anticommutation relations (3.1.10) and (3.1.11). More work is needed to understand this connection better.

References

[1] J. Canny, “Some algebraic and geometric computations in PSPACE,” ser. STOC ’88, Chicago, Illinois, USA: Association for Computing Machinery, 1988, 460–467, ISBN: 0897912640.

[2] J. W. Helton, “Positive noncommutative polynomials are sums of squares,” *Annals of Mathematics*, vol. 156, pp. 675–694, 2002.

[3] I. Klep, C. Scheiderer, and J. Volčič, “Globally trace-positive noncommutative polynomials and the unbounded tracial moment problem,” *Mathematische Annalen*, 2022.

[4] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, “$\mathsf{MIP}^* = \mathsf{RE}$,” *arXiv preprint arXiv:2001.04383*, 2020.

[5] W. Slofstra, “The set of quantum correlations is not closed,” in *Forum of Mathematics, Pi*, Cambridge University Press, vol. 7, 2019.

[6] R. Cleve, L. Liu, and W. Slofstra, “Perfect commuting-operator strategies for linear system games.,” *Journal of Mathematical Physics*, vol. 58, no. 012202, 2017, `https://doi.org/10.1063/1.4973422`.

[7] H. Mousavi, S. S. Nezhadi, and H. Yuen, “Nonlocal games, compression theorems, and the arithmetical hierarchy,” in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, ser. STOC 2022, Rome, Italy: Association for Computing Machinery, 2022, 1–11, ISBN: 9781450392648.

[8] W. Slofstra, “Tsirelson’s problem and an embedding theorem for groups arising from nonlocal games.,” *Journal of the American Mathematical Society*, 2019.

[9] A. Connes, “Classification of injective factors cases II_1, II_∞, III_λ, $\lambda \neq 1$,” *Annals of Mathematics*, pp. 73–115, 1976.

[10] N. Ozawa, “About the Connes embedding conjecture: Algebraic approaches.,” *Jpn. J. Math.*, vol. 8, 147–183, 1 2013.

[11] V. B. Scholz and R. F. Werner, “Tsirelson’s problem,” *arXiv preprint arXiv:0812.4305*, 2008.

[12] T. Fritz, “Tsirelson’s problem and Kirchberg’s conjecture,” *Reviews in Mathematical Physics*, vol. 24, no. 05, p. 1 250 012, 2012.

[13] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, and R. F. Werner, “Connes’ embedding problem and Tsirelson’s problem,” *Journal of Mathematical Physics*, vol. 52, no. 1, p. 012 102, 2011.

[14] M. Navascués, S. Pironio, and A. Acín, “A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations,” *New Journal of Physics*, vol. 10, no. 7, p. 073 013, 2008.

[15] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner, “The quantum moment problem and bounds on entangled multi-prover games,” in *2008 23rd Annual IEEE Conference on Computational Complexity*, IEEE, 2008, pp. 199–210.

[16] S. Pironio *et al.*, “Random numbers certified by Bell’s theorem,” *Nature*, vol. 464, no. 7291, pp. 1021–1024, 2010.

[17] T. Netzer and A. Thom, “Hyperbolic polynomials and generalized Clifford algebras,” *Discrete & Computational Geometry*, vol. 51, no. 4, pp. 802–814, 2014.

[18] J. Canny, “Some algebraic and geometric computations in PSPACE,” ser. STOC ’88, Chicago, Illinois, USA: Association for Computing Machinery, 1988, 460–467, ISBN: 0897912640.

[19] A. Natarajan and J. Wright, “$\mathsf{NEEXP} \subseteq \mathsf{MIP}^*$,” in *IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, 2019, pp. 510–518.

[20] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, “Device-independent parallel self-testing of two singlets,” *Physical Review A*, vol. 93, no. 6, p. 062 121, 2016.

[21] A. Natarajan and T. Vidick, “Low-degree testing for quantum states, and a quantum entangled games PCP for QMA,” in *IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE, 2018, pp. 731–742.

[22] T. Ito and T. Vidick, “A multi-prover interactive proof for nexp sound against entangled provers,” in *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, IEEE, 2012, pp. 243–252.

[23] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, “Quantum soundness of the classical low individual degree test,” *arXiv preprint arXiv:2009.12982*, 2020.

[24] M. Bavarian, T. Vidick, and H. Yuen, “Hardness amplification for entangled games via anchoring,” in *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, 2017, pp. 303–316.

[25] I. Goldbring and B. Hart, “A computability-theoretic reformulation of the Connes Embedding Problem,” *arXiv preprint arXiv:1308.2638*, 2013.

[26] H. Mousavi, S. S. Nezhadi, and H. Yuen, "On the Complexity of Zero Gap MIP*," in *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, A. Czumaj, A. Dawar, and E. Merelli, Eds., ser. Leibniz International Proceedings in Informatics (LIPIcs), vol. 168, Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2020, 87:1–87:12, ISBN: 978-3-95977-138-2.

[27] Z. Ji, "Compression of quantum multi-prover interactive proofs," in *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, ser. STOC 2017, Montreal, Canada: Association for Computing Machinery, 2017, 289–302, ISBN: 9781450345286.

[28] J. Fitzsimons, Z. Ji, T. Vidick, and H. Yuen, "Quantum proof systems for iterated exponential time, and beyond," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, ser. STOC 2019, Phoenix, AZ, USA: Association for Computing Machinery, 2019, 473–480, ISBN: 9781450367059.

[29] M. Coudron and A. Natarajan, "The parallel-repeated magic square game is rigid.," Sep. 2016.

[30] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, "Quantum soundness of testing tensor codes," *Forthcoming draft*, 2021.

[31] R. Jain, A. Pereszlényi, and P. Yao, "A parallel repetition theorem for entangled two-player one-round games under product distributions," in *2014 IEEE 29th Conference on Computational Complexity (CCC)*, 2014, pp. 209–216.

[32] I. Dinur, D. Steurer, and T. Vidick, "A parallel repetition theorem for entangled projection games," in *2014 IEEE 29th Conference on Computational Complexity (CCC)*, 2014, pp. 197–208.

[33] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay, "Perfect parallel repetition theorem for quantum xor proof systems," *Computational Complexity*, vol. 17, no. 2, pp. 282–299, 2008.

[34] V. I. Paulsen, S. Severini, D. Stahlke, I. G. Todorov, and A. Winter, "Estimating quantum chromatic numbers," *Journal of Functional Analysis*, vol. 270, no. 6, pp. 2188–2222, 2016.

[35] W. Helton, K. P. Meyer, V. I. Paulsen, and M. Satriano, "Algebras, synchronous games and chromatic numbers of graphs," *arXiv preprint arXiv:1703.00960*, 2017.

[36] S.-J. Kim, V. Paulsen, and C. Schafhauser, "A synchronous game for binary constraint systems," *Journal of Mathematical Physics*, vol. 59, no. 3, p. 032 201, 2018.

[37] B. Blackadar, *Operator algebras: theory of C^*-algebras and von Neumann algebras*. Springer Science & Business Media, 2006, vol. 122.

[38] J. Kempe and T. Vidick, “Parallel repetition of entangled games,” in *Proceedings of the forty-third annual ACM Symposium on Theory of Computing*, 2011, pp. 353–362.

[39] M. de la Salle, “Orthogonalization of positive operator valued measures,” *arXiv preprint arXiv:2103.14126*, 2021.

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

[41] I. Šupić and J. Bowles, “Self-testing of quantum systems: A review,” *Quantum*, vol. 4, p. 337, 2020.

[42] D. Mermin, “Simple unified form for the major no-hidden-variables theorems,” *Physical Review Letters*, vol. 65, no. 27, p. 3373, 1990.

[43] A. Peres, “Incompatible results of quantum measurements,” *Physics Letters A*, vol. 151, no. 3-4, pp. 107–108, 1990.

[44] P. Aravind, “A simple demonstration of Bell’s theorem involving two observers and no probabilities or inequalities,” *arXiv preprint quant-ph/0206070*, 2002.

[45] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, “Device-independent parallel self-testing of two singlets,” *Physical Review A*, vol. 93, no. 6, 2016.

[46] V. Jones, *von Neumann Algebras*, `https://math.berkeley.edu/~vfr/VonNeumann2009.pdf`, 2009.

[47] R. Chao, B. W. Reichardt, C. Sutherland, and T. Vidick, “Test for a large amount of entanglement, using few measurements,” *Quantum*, vol. 2, p. 92, 2018.

[48] C. H. Papadimitriou, *Computational Complexity*. Addison-Wesley, 1994.

[49] N. D. Jones, *Computability and complexity: from a programming perspective*. MIT press, 1997, vol. 21.

[50] G. Gutoski and J. Watrous, “Toward a general theory of quantum games,” in *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, ser. STOC ’07, San Diego, California, USA: Association for Computing Machinery, 2007, 565–574, ISBN: 9781595936318.

[51] S. Pironio, M. Navascués, and A. Acin, “Convergent relaxations of polynomial optimization problems with noncommuting variables,” *SIAM Journal on Optimization*, vol. 20, pp. 2157–2180, Jan. 2010.

[52] D. Cui, A. Mehta, H. Mousavi, and S. S. Nezhadi, "A generalization of CHSH and the algebraic structure of optimal strategies," *Quantum*, vol. 4, p. 346, Oct. 2020.

[53] J. S. Bell, "On the einstein-podolsky-rosen paradox.," *Physics*, vol. 1, p. 195, 1964.

[54] D. Mayers and A. Yao, "Self testing quantum apparatus.," *Quantum Info. Comput.*, vol. 4, no. 4, pp. 273–286, 2004, `https://doi.org/10.1007/11786986_8`.

[55] A. Natarajan and T. Vidick, "Low-degree testing for quantum states, and a quantum entangled games pcp for qma," *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 731–742, 2018, `https://doi.org/10.1109/focs.2018.00075`.

[56] J. Fitzsimons, Z. Ji, T. Vidick, and H. Yuen, "Quantum proof systems for iterated exponential time, and beyond," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, ser. STOC 2019, `https://doi.org/10.1145/3313276.3316343`, Phoenix, AZ, USA: ACM, 2019, pp. 473–480, ISBN: 978-1-4503-6705-9.

[57] A. Natarajan and J. Wright, "Neexp in mip," *ArXiv*, vol. abs/1904.05870, 2019, `https://doi.org/10.1109/focs.2019.00039`.

[58] U. Vazirani and T. Vidick, "Certifiable quantum dice: Or, true random number generation secure against quantum adversaries," in *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, ser. STOC '12, `http://doi.acm.org/10.1145/2213977.2213984`, New York, New York, USA: ACM, 2012, pp. 61–76, ISBN: 978-1-4503-1245-5.

[59] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks.," *Phys. Rev. Lett.*, vol. 98:230501, 2007, `https://doi.org/10.1103/physrevlett.98.230501`.

[60] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 113, p. 140 501, 14 2014, `https://doi.org/10.1145/3310974`.

[61] A. Coladangelo, A. B. Grilo, S. Jeffery, and T. Vidick, "Verifier-on-a-leash: New schemes for verifiable delegated quantum computation, with quasilinear resources," in *Advances in Cryptology – EUROCRYPT 2019*, Y. Ishai and V. Rijmen, Eds., `https://doi.org/10.1007/978-3-030-17659-4_9`, Cham: Springer International Publishing, 2019, pp. 247–277, ISBN: 978-3-030-17659-4.

[62] I. Supić and J. Bowles, "Self-testing of quantum systems: A review.," `https://doi.org/10.22331/q-2020-09-30-337`, 2019.

[63] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories.," *Phys. Rev. Lett.*, vol. 23, p. 880, 1969.

[64] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, "Consequences and limits of nonlocal strategies," in *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, ser. CCC '04, https://doi.org/10.1109/CCC.2004.9, Washington, DC, USA: IEEE Computer Society, 2004, pp. 236–249, ISBN: 0-7695-2120-7.

[65] S. J. Summers and R. Werner, "Maximal violation of bell's inequalities is generic in quantum field theory," *Comm. Math. Phys.*, vol. 110, no. 2, pp. 247–259, 1987, https://doi.org/10.1007/BF01207366.

[66] B. Tsirelson, "Some results and problems on quantum bell-type inequalities.," *Hadronis Journal Supplement*, vol. 8, pp. 320–331, 1993.

[67] R. Cleve and R. Mittal, "Characterization of binary constraint system games.," in *International Colloquium on Automata, Languages, and Programming (ICALP) 2012*, https://doi.org/10.1007/978-3-662-43948-7_27, 2012, 320–331.

[68] N. D. Mermin, "Simple unified form for the major no-hidden-variables theorems.," *Phys. Rev. Lett.*, vol. 65, no. 27, p. 3373, 1990, https://doi.org/10.1103/PhysRevLett.65.3373.

[69] M. Coudron and A. Natarajan, "The parallel-repeated magic square game is rigid," arXiv:1609.06306 [quant-ph], 2016.

[70] C. Bamps and S. Pironio, "Sum-of-squares decompositions for a family of clauser-horne-shimony-holt-like inequalities and their application to self-testing.," *Phys. Rev. A*, vol. 91, no. 052111, 2015, https://doi.org/10.1103/PhysRevA.91.052111.

[71] A. Coladangelo, K. T. Goh, and V. Scarani, "All pure bipartite entangled states can be self-tested.," *Nature Communications*, vol. 8, no. 15485, 2017, https://doi.org/10.1038/ncomms15485.

[72] M. McKague, T. H. Yang, and V. Scarani, "Robust self-testing of the singlet.," *Journal of Mathematical Physics*, vol. 45, p. 455 304, 45 2012, http://doi.org/10.1088/1751-8113/45/45/455304.

[73] A. Natarajan and T. Vidick, "Robust self-testing of many-qubit states.," in *STOC*, https://doi.org/10.1038/s41534-018-0120-0, 2017.

[74] A. Coladangelo, "Parallel self-testing of (tilted) epr pairs via copies of (tilted) chsh," *Quantum Information and Computation*, vol. 17, p. 35, 2016.

[75] M. Mckague, "Self-testing in parallel with chsh," *Quantum*, vol. 1, 2016, https://doi.org/10.22331/q-2017-04-25-1.

[76] B. W. Reichardt, F. Unger, and U. Vazirani, “A classical leash for a quantum system: Command of quantum systems via rigidity of chsh games,” in *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, ser. ITCS ’13, Berkeley, California, USA: ACM, 2013, pp. 321–322, ISBN: 978-1-4503-1859-4.

[77] A. Coladangelo and J. Stark, “Robust self-testing for linear constraint system games.,” in *QIP 2018*, 2018.

[78] W. T. Gowers and O. Hatami, “Inverse and stability theorems for approximate representations of finite groups.,” *Sbornik: Mathematics*, vol. 208, no. 12, p. 1784, 2017, `https://doi.org/10.1070/SM8872`.

[79] T. Vidick, “A simplified analysis on robust self-testing of *n* epr pairs.,” Available at `http://users.cms.caltech.edu/~vidick/`, 2018.

[80] W. Slofstra, “The set of quantum correlations is not closed,” *Forum of Mathematics, Pi*, vol. 7, e1, 2019, `https://doi.org/10.1017/fmp.2018.3`.

[81] M. Navascués, S. Pironio, and A. Acín, “A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations.,” *New Journal of Physics*, vol. 10, no. 7, p. 073 013, 2008, `https://doi.org/10.1088/1367-2630/10/7/073013`.

[82] H. Buhrman and S. Massar, “Causality and Tsirelson’s bounds,”, vol. 72, no. 5, 052103, p. 052 103, Nov. 2005. arXiv: `quant-ph/0409066 [quant-ph]`.

[83] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[84] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, “Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems.,” Available at `https://arxiv.org/pdf/1807.03332.pdf`, 2018.

[85] W. Slofstra, “Lower bounds on the entanglement needed to play xor non-local games,” *Journal of Mathematical Physics*, vol. 52, no. 10, p. 102 202, 2011.

[86] J. Kaniewski, “Weak form of self-testing,” *Physical Review Research*, vol. 2, no. 3, 2020.

[87] L. Mančinska, T. G. Nielsen, and J. Prakash, *Glued magic games self-test maximally entangled states*, 2021. arXiv: `2105.10658 [quant-ph]`.

[88] J. Watrous, *The Theory of Quantum Information.* Cambridge University Press, 2018, `https://doi.org/10.1017/9781316848142`.

[89] I. Chuang and M. Nielsen, *Quantum Computation and Quantum Information.* Cambridge University Press, 2010, https://doi.org/10.1017/CBO9780511976667.

[90] S. J. Harris, S. K. Pandey, and V. Paulsen, "Entanglement and non-locality.," Available at https://www.math.uwaterloo.ca/~vpaulsen/EntanglementAndNonlocality_LectureNotes_7.pdf, 2016.

[91] X. Wu, J.-D. Bancal, M. Mckague, and V. Scarani, "Device-independent parallel self-testing of two singlets," *Physical Review A*, vol. 93, 2015, https://doi.org/10.1103/PhysRevA.93.062121.

[92] J. Kempe, O. Regev, and B. Toner, "Unique games with entangled provers are easy," *SIAM Journal on Computing*, vol. 39, no. 7, pp. 3207–3229, 2010. eprint: https://doi.org/10.1137/090772885.

[93] P. Raghavendra, "Optimal algorithms and inapproximability results for every csp?" In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, ser. STOC '08, Victoria, British Columbia, Canada: Association for Computing Machinery, 2008, 245–254, ISBN: 9781605580470.

[94] B. Tsirelson, "Some results and problems on quantum bell-type inequalities.," *Hadronis Journal Supplement*, vol. 8, pp. 320–331, 1993.

[95] A. M. Frieze and M. Jerrum, "Improved approximation algorithms for max k-cut and max bisection," in *Conference on Integer Programming and Combinatorial Optimization*, 1995.

[96] E. de Klerk, D. V. Pasechnik, and J. P. Warners, "On approximate graph colouring and max-k-cut algorithms based on the θ-function," *Journal of Combinatorial Optimization*, vol. 8, pp. 267–294, 2004.

[97] A. J. Hoffman and H. W. Wielandt, "The variation of the spectrum of a normal matrix," *Duke Mathematical Journal*, vol. 20, no. 1, pp. 37 –39, 1953.

[98] S. Khot, G. Kindler, E. Mossel, and R. O'Donnell, "Optimal inapproximability results for max-cut and other 2-variable csps?" *SIAM Journal on Computing*, vol. 37, no. 1, pp. 319–357, 2007. eprint: https://doi.org/10.1137/S0097539705447372.

[99] M. X. Goemans and D. P. Williamson, "Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming," *J. ACM*, vol. 42, no. 6, 1115–1145, 1995.

[100] M. X. Goemans and D. P. Williamson, "Approximation algorithms for max-3-cut and other problems via complex semidefinite programming," *Journal of Computer and System Sciences*, vol. 68, no. 2, pp. 442–470, 2004, Special Issue on STOC 2001.

[101] G. Andersson, L. Engebretsen, and J. Håstad, “A new way of using semidefinite programming with applications to linear equations mod p,” *Journal of Algorithms*, vol. 39, no. 2, pp. 162–204, 2001.

[102] C. Jordan, “Essai sur la géométrie à *n* dimensions,” *Bulletin de la Société Mathématique de France*, vol. 3, pp. 103–174, 1875.

[103] G. W. Stewart, “On the perturbation of pseudo-inverses, projections and linear least squares problems,” *SIAM Review*, vol. 19, no. 4, pp. 634–662, 1977.

[104] R. Bhatia, *Matrix Analysis*. Springer, 1997, vol. 169, ISBN: 0387948465.