QUANTUM GAMES, GRAPHS, AND GÖDEL

by

Seyed Sajjad Nezhadi

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2025

Advisory Committee:
Professor Andrew Childs, Chair
Professor Matthew Coudron, Advisor
Professor Carl Miller
Professor Runzhou Tao
Professor Alexander Barg

Dedication

To my parents Sayyed Hossein Nezhadi and Fereshteh Keshavarz.

Acknowledgments

First and foremost I am very grateful to my advisor Matthew Coudron whose support and scientific curiosity were crucial in allowing me to explore many different interests including those present in this dissertation aswell as other works in the areas of quantum hamiltonian complexity and machine learning. He always made sure I was able to focus on doing good science and exploring my interests and shielded me from other concerns.

I would equally like to thank my undergraduate advisor, mentor and friend Henry Yuen. It was during his quantum computing course in the fall of 2018 that I fell in love with the field in which I ended up completing a PhD. I am immensely thankful to him for taking me on as a research assistant during my year long gap before grad school, during which I was able to jump start my research career. His energy and kindness always brings me joy. That same energy attracted many amazing students that ended up being some of my most frequent collaborators and friends.

I would like to thank my other collaborators, who made research exciting and fulfilling, Hamoon Mousavi, David Cui, Jon Nelson, Nolan Coble, Arthur Mehta, Lev Stambler, Laura Mančinska, Vern Paulsen, Bill Helton, David Roberson, Travis Russel, Andrew Marks.

I would like to thank Bill Gasarch for involving me in his student mentorship programs. Getting to advise students was one of the most fulfilling experiences of my PhD. I would like to thank the great students I got to advise: Kevin Yao (Summer 2022 High School REU), Jakin Ng (Summer 2024 REU-CAAR), and Bea Fatima (Summer 2024 REU-CAAR).

Finally, I would like to thank my family who without their support this thesis would be impossible. Especially my parents, Sayyed Hossein Nezhadi and Fereshteh Keshavarz, my brother Sadiq Nezhadi, and my beloved wife Fatemeh Khorasani.

Table of Contents

List of Tables

List of Figures

Introduction

A recurring theme in theoretical computer science has been the interplay between graph theory, computational complexity theory and property testing via nonlocal games, otherwise known as multiprover interactive proof systems. Nonlocal games consist of two separated (entangled in the quantum setting) yet cooperating players, usually dubbed Alice and Bob, who receive questions from a verifier according to a known distribution and respond with answers via a previously agreed upon strategy to try and win the verifiers game. These games can decide global decision problems via local checks, which allows them to be used for highly efficient property testing. For instance, graph properties like k-colorability or CSP satisfiability can be expressed through local constraints over a graph. When the constraint graph has good expansion properties, the verifier can test satisfiability with strong soundness bounds.

Graph theory plays a central role in the theory of NP-completeness. Many canonical NP-complete problems such as 3-Colorability, Hamiltonian Cycle, Vertex Cover, Independent Set are graph-theoretic. Graph based problems are particularly nice to use for hardness reductions due to their flexibility, making them usefull for hardness-of-approximation reductions [1]. The PCP theorem [2, 3] shows that every NP language has a proof verifiable by a constant number of query bits. The PCP theorem came on the footsteps of the MIP = NEXP [4] result. Historically, the first proofs of the PCP theorem used nonlocal games and techniques such as gap-amplification using parallel repetition [5]. MIPs where originally invented to provide zero-knowledge proofs for NP in the information-theoretic setting [6]. A standard example is the zero-knowledge proof for graph 3-coloring, where provers respond to local queries with a hidden coloring under random permutations. The verifier checks for consistent and correct colorings without learning the coloring itself.

In this thesis, we explore the quantum variant of this connection that has been developing recently in the literature. That is the interplay between newly defined so called quantum graph properties, computability theory and entangled nonlocal games, known also as entangled multiprover interactive proof systems.

Quantum variants of graph properties such as quantum chromatic number, quantum independence number, quantum clique number, quantum graph homomorphism, and quantum isomorphism [7, 8, 9, 10, 11] are defined using nonlocal games. These are developed by first looking at nonlocal games that function as property tests for these classical graph properties. These games are used as local test of graph properties, where Alice and Bob usually receive either some random vertex or edge of the graph and must respond in such a way to prove that the graph has the requisite property, the game is a test of a property if it has a classical strategy that wins with probability one if and only if the underlying graph has that property. Since each round of the game only consists of sampling a couple of vertices/edges the tests are highly efficient. Then the nonlocal games are relaxed to allow for quantum entangled strategies. The graph is then said to hold the quantum variant of the graph property if the test is perfectly winnable with an entangled strategy. In many interesting cases this develops a distinct well-motivated relaxation of the classical graph property. A particularly elegant example of this phenomenon is quantum isomorphism. Two non-isomorphic graphs may be quantum isomorphic, there is a striking combinatorial characterization of quantum isomorphism that naturally emerges as a relaxation of the classical test for graph isomorphism. In [9], the authors demonstrate that two graphs G and H are quantum isomorphic if and only if the homomorphism counts from any planar graph into them are identical, i.e., $\forall$ planar $K, |\mathrm{Hom}(K, G)| = |\mathrm{Hom}(K, H)|$. This contrasts with the classical result, where two graphs G and H are isomorphic if and only if the homomorphism counts from any graph (not necessarily planar) into them are the same, i.e., $\forall K, |\mathrm{Hom}(K, G)| = |\mathrm{Hom}(K, H)|$.

A well studied example of such a nonlocal graph property test is the graph homomorphism game [7]. This game tests for the existence of a graph homomorphism from some graph G into another graph H. Almost all other quantum graph properties in the literature, quantum chromatic, independence, clique numbers, are defined using this game. In the game Alice and Bob each recieve a random vertex g_a, g_b from G and respond with verticies h_a, h_b in H, ideally according to a previously agreed upon homomorphism. The players then win the game if the following conditions are satisified: if $g_a = g_b$ then $h_a = h_b$, if g_a and g_b are edge connected then so are h_a and h_b, finally if g_a and g_b are neither identical or edge connected then similarly h_a and h_b should also be neither.

In chapter 1 of this thesis we define a family of new quantum graph properties. We define nonlocal games that test for perfect matching in graphs and hypergraphs, L-perfect matching for bipartite graphs and finally fractional perfect matching. These are a set of novel games that dont arise from the graph homomorphism game. We show that by looking at entangled strategies we get the distinct quantum perfect matching property for graphs and hypergraphs. We then characterize these quantum properties by quantizing a classical relationship in graph theory. A graph (or hypergraph) G classically has a perfect matching if and only if its line graph $L(G)$ has a maximal independence number. We show that a graph (hypergraph) has a quantum perfect matching if and only if its line graph has maximal quantum independence number. In the case of the bipartite and fractional perfect matching games we show that a new quantum property is not developed, the games have perfect entangled strategies if and only if they have perfect classical startegies. But we show that there can be interesting examples of quantum advantage for these games. If we look at the further relaxation to nonsignaling strategies then all the games define distinct properties from the classical and quantum ones. Nonsignaling strategies are a generalization of quantum strategies where the only requirement is that Alice's local marginal distribution is independent of Bob's questions, and vice-versa. We show that a graph has a nonsignaling perfect matching if and only if the graph has a classical fractional perfect matching that avoids triangles. We also show that a bipartite graph has a nonsiganling L-perfect matching if and only if the bipartite graph can be decomposed into a classically matchable subgraph and a left-degree 2 subgraph.

Deciding if a nonlocal game is perfectly classically winnable is a problem that is complete for the class $NEXP$ of nondeterministic exponential time. Surprisingly, when looking at entangled nonlocal games this same problem becomes undecidable[12, 13]. Furthermore, in a groundbreaking result it was shown that even approximately deciding the entangled value of a nonlocal game, when promised it is either 1 or at most $\frac{1}{2}$ is RE-complete [14]. In chapter 2 of this thesis we look at completely characterizing the hardness of deciding if an entangled nonlocal game is perfectly winnable. We show that it is not only undecidable but is doubly undecidable. In particular, the problem is complete for the computability class Π_2 which lives in the second level of the arithmetical hierarchy. This is the class of all problems for which no-instances are recognizable if a

Turing machine is equipped with an oracle for the halting problem. Equivalently, we show that the problem of deciding the value of a noncommutative polynomial optimization is Π_2-complete. This is in stark contrast to commutative polynomial optimization which belongs to the class $PSPACE$ [15].

Deciding the entangled value of nonlocal games is generally undecidable, but so is deciding many of the quantum graph properties such as quantum isomorphism and calculating the quantum chromatic, independence and clique numbers [16]. In Chapter 1 we also show that deciding quantum perfect matching for hypergraphs is undecidable. Whether it is also undecidable for graphs remains an interesting open problem.

To prove the Π_2-completeness result, in chapter 2, we further develop a technique known as iterated compression which was originally developed by Ji [17] and further used to prove undecidability results for MIP^* [12, 14]. A compression procedure takes the description of a family of nonlocal games and returns another family where the values of the games are related, that is the nth game in the new family is perfectly quantum winnable if and only if the nth game in the original was. Furthermore, the games in the new family are exponentially more efficient for the verifier to play than the games in the original family, to sample questions and to decide if the players won. Then compression can be used in an iterated way to produce reductions that take instances of undecidable problems about Turing machines to games.

Compression is done in two steps. First the size of the questions involved in a game are exponentially reduced and then later the size of the answers. To perform answer reduction the idea is to delegate the verifiers decision, whether the players answers win the nonlocal game, to the players themselves. This is done via a quantum sound variant of essentially a cook-levin reduction. To perform question reduction the idea is to delegate the task of sampling questions to the players themselves. This requires some unique properties of entangled strategies for nonlocal games known as rigidity or self-testing. Many entangled nonlocal games, such as the magic square game [18, 19], have essentially unique optimal quantum strategies. That is any strategy that wins perfectly or close to perfect must be using a quantum state and measurements that are close to one that is locally unitarily equivalent to a particular canonical strategy. These type of rigidity properties allow the verifier to put a leash on the players behavior and guarantee that the players perform particular measurements when playing optimally. In particular, for question reduction we use rigidity to guarantee that the players are sampling questions according to the appropriate distribution.

In chapter 3, we study rigidity and self-testing for a family of new linear constarint system games that generalize the classical CHSH game [20]. These games involve two inconsistent two-variable linear equations over 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. Alice receives a random equation and Bob a random variable. Alice must provide an assignment that satisfies her equation and Bob must provide an assignment that is consistent with Alice. For $n = 2$ this game is exactly the classical CHSH game. We show that these games all exhibit quantum advantage and that the, conjectured optimal, strategy for these games has quantum value which approaches $\frac{1}{2} + \frac{1}{\pi}$ as $n \longrightarrow \infty$ and all the games have classical value $\frac{3}{4}$. We then go on to prove self-testing results for $n = 3$ by developing a noncommutative sum-of-squares framework for proving self-testing in cases where the optimal quantum value is bounded below 1 but there is a sum-of-squares proof of optimality. By deriving algebraic constraints on optimal strategies from the sum-of-squares we identify algebraic groups for which we prove that all optimal strategies must be state-dependent representations of said group. And then by studying the irreducible representations of that group we can derive self-testing results for the canonical strategies entangled state and measurements.

Throughout this thesis, in particular chapters 1 and 2, we have been looking at synchronous games and synchronous strategies. Synchronous games are games where Alice and Bob must respond with identical answers to win if they receive the same question. Synchronous strategies are those strategies in which Alice and Bob respond identically on the same question. Synchronous strategies can be modeled much easier than general strategies. In the classical case a synchronous strategy consists of a single deterministic strategy used by both Alice and Bob. Synchronous entangled strategies all use maximally entangled states and Alice and Bob share identical projective measurements. These make synchronous strategies very convenient to work with and study. It turns out that synchronous games have a perfect strategy if and only if they have prefect synchronous strategies. Therefore when studying perfectly winnable synchronous games, such as the games studied in chapters 1 and 2 and much of the nonlocal game and quantum graph theory literature, it is enough to study synchronous strategies.

In chapter 4 of this thesis we study synchronous strategies of games in scenarios where they are not well understood. In particular, synchronous strategies for non-synchronous games and synchronous games that are not perfectly winnable. We study the synchronous strategies for the c-coloring game of the k-clique, where $c < k$, and 2-coloring odd cycles. We provide an alternative SDP from [21] to compute the synchronous values for XOR games. And also look at the synchronous value of the parallel repetition of games, with a stark example of a non-synchronous game for which the synchronous value of its parallel repetition increases.

Chapter 1: Games and Graphs

This chapter is taken verbatim from our paper "Quantum Perfect Matchings" [22]. All authors of this work contributed equally.

1.1 Introduction

In this work, we investigate "quantum" notions of classical graph properties. To do this, we take the perspective of two-prover property testing, also known as nonlocal games. In this setup, there is a single verifier who wants to determine whether a particular object has a particular property. The verifier is allowed to quiz two spatially separated provers, often dubbed Alice and Bob, and cross-check their answers to verify whether the property holds. We say that a property test captures a particular property if the classical provers can convince the verifier with certainty if and only if the property holds. There is a vast literature on property testing [23]. In these tests, we can also allow for the provers to use quantum entangled strategies [24, 25, 26, 27]. We can then say that the object has a quantum analog of the property if and only if the verifier can be perfectly convinced by the provers using a quantum entangled strategy. Previous works have established quantum analogs for several graph properties, such as quantum chromatic numbers, quantum independence numbers, and quantum graph homomorphisms and isomorphisms [7, 8, 9, 10, 11].

In some cases, such as 2-colorability of graphs, the quantum and classical properties coincide. We refer to such tests as quantum sound, since quantum strategies cannot "fool" the classical test.

However, in many interesting cases, the quantum property diverges from its classical counterpart, leading to new and well-motivated definitions of quantum properties. A particularly elegant example of this phenomenon is quantum isomorphism. While two non-isomorphic graphs may be quantum isomorphic, there is a striking combinatorial characterization of quantum isomorphism that naturally emerges as a relaxation of the classical test for graph isomorphism. In [9], the authors demonstrate that two graphs G and H are quantum isomorphic if and only if the homomorphism counts from any planar graph into them are identical, i.e., $\forall$ planar $K, |\mathrm{Hom}(K, G)| = |\mathrm{Hom}(K, H)|$. This contrasts with the classical result, where two graphs G and H are isomorphic if and only if the homomorphism counts from any graph (not necessarily planar) into them are the same, i.e., $\forall K, |\mathrm{Hom}(K, G)| = |\mathrm{Hom}(K, H)|$. This combinatorial characterization is remarkable as the definition of a quantum isomorphism prima facie is not combinatorial in nature: the existence of a perfect quantum strategy is a highly continuous property in that it is defined through arbitrary high dimensional Hilbert spaces with arbitrary operators.

In this paper, we continue down this line of work and introduce natural nonlocal games to test for perfect matchings in graphs and hypergraphs, L-perfect matchings in bipartite graphs, and fractional perfect matchings. We then examine both quantum entangled strategies and nonsignaling strategies for these games. nonsignaling strategies generalize quantum strategies by imposing only one condition: Alice's local marginal distributions must remain independent of Bob's question, and vice-versa. Through these games, we define quantum and nonsignaling versions of perfect matchings, L-perfect matchings, and fractional perfect matchings. Additionally, we provide combinatorial characterizations for when a graph satisfies the nonsignaling properties, and we connect the quantum properties to other quantum graph properties, such as the quantum independence number.

1.1.1 Our results

In section 1.3, we define four separate synchronous nonlocal games that test for L-perfect matching for bipartite graphs, perfect matching for general graphs, fractional perfect matching and finally perfect matching for hypergraphs. We prove that these games characterize the classical graph properties. Namely, they have a perfect classical winning probability if and only if the underlying graphs have the requisite perfect matching property. Almost all other quantum graph properties in the literature are defined using the graph homomorphism game. Our tests represent a novel class of games that don't map onto the homomorphism games.

In section 1.4, we explore quantum and nonsignaling strategies for the L-perfect matching game. We prove that the game is quantum sound, by using Hall's theorem in graph theory and a result about the quantum chromatic number of clique graphs. As a consequence we also get that the fractional perfect matching test is quantum sound. We then go on to show that there are many bipartite graphs that only have perfect nonsignaling strategies for the game. We provide a full characterization for when a bipartite graph has this nonsignaling L-perfect matching property. In particular we prove the following theorem

Theorem 1.1.1. *Let $G = (L \sqcup R, E)$ be a bipartite graph. Then the following are equivalent:*

1. $\omega^{ns}(BPM_G) = 1$,

2. *$G^{\#}$ contains no lone vertices in $L^{\#}$,*

3. *there exists a perfect matching subgraph $P \subset G$ and left-degree 2 subgraph S such that $P \sqcup S \subset G$ covering all of L.*

Where $G^{\#} = (L^{\#} \sqcup R^{\#}, E^{\#})$ is the graph where the degree 1 vertices in L and their neighbour in R are iteratively removed until none remain.

Given that the L-perfect matching test is quantum sound a natural question, is whether there is any quantum advantage for these games at all. In section 1.5, we explore the quantum values of the game for the bipartite complete graphs $K_{n,2}$. We fully characterize the quantum values by providing sum-of-square proofs of optimallity. We show that only $K_{3,2}$ has quantum advantage and that the optimal value is achieved via a synchronous strategy. In particular any synchronous strategy where the players three observables sum to 0 are optimal for this game and those are the only ones. Interestingly for all $n \geq 4$ the optimally quantum and classical strategies for the games are non-synchronous.

Finally, in section 1.6 we turn to the perfect matching of general graphs. We show that, unlike fractional perfect matching and L-perfect matching, quantum strategies for the perfect matching game define a distinct property. In particular, K_n for odd $n \geq 7$ have the quantum perfect matching property. We then provide a full characterization for the quantum perfect matching property. In particular we prove the following theorem

Theorem 1.1.2. *Let G be a graph. Then the following are equivalent:*

1. *G has a quantum perfect matching.*
2. *$L(G)$ has a projective packing of value $|V(G)|/2$.*
3. *$\alpha_q(2L(G)) = |V(G)|$.*

This result mirrors the classical characterization of perfect matching. Where a graph G has a perfect matching if and only if $\alpha(L(G)) = |V|/2$.

We then explore the nonsignaling perfect matching property. This further develops a distinct property from the quantum one. In particular, the cycle graphs C_n for odd $n \geq 5$ have a nonsignaling perfect matching but not quantum or classical ones. We then provide a full characterization for the nonsignaling perfect matching property. In particular we prove the following theorem

Theorem 1.1.3. *For a graph G, $\omega^{ns}(PM_G) = 1$ if and only if G has a fractional perfect matching avoiding triangles.*

Finally, we show in the last part of the section that the quantum perfect matching property for hypergraphs is undecidable and in fact equivalent to that of deciding the quantum independence number of graphs.

1.1.2 Further directions

There are several further directions related to this work.

Decidability of quantum perfect matching games and line graph problems Deciding whether a nonlocal game can be perfectly won with quantum strategies is generally undecidable [13, 14, 28]. Additionally, it has been established that determining the quantum chromatic number, independence number, and quantum isomorphism are also undecidable [29, 9, 16]. In section 1.6.3, we demonstrate that quantum perfect matching for hypergraphs is undecidable. A natural open question is whether quantum perfect matching itself is undecidable. This turns out to be equivalent to whether the quantum independence number remain undecidable when restricted to only line graphs.

One could more broadly ask: what about other graph properties restricted to line graphs, such as the chromatic number of line graphs? One natural approach is to use the classical reduction of Holyer which reduces 3SAT to edge coloring [30]. Here, one 3SAT clause is mapped to a gadget graph where the edge coloring of the entire graph encodes the 3SAT clause assignment. Unfortunately, due to this type of gadget construction, the reduction does not “quantize” easily. To ensure that the reduction is quantum sound, i.e., if the 3SAT instance is not quantum satisfiable, then the reduced edge coloring instance is not quantum satisfiable, one would need to be able to simultaneously measure the entire gadget graph to recover an assignment to the 3SAT clauses. This requires commutativity. [29] gets around this issue by introducing a commutativity gadget which does not affect quantum satisfying solutions while enforcing that certain variables must commute. However, the approach of [29] was very specific to graph (vertex) coloring and such a commutativity gadget does not translate easily to edge problems. Hence, we ask whether one can construct such commutativity gadgets for the edge coloring problem. Furthermore, more generally, what kinds of constraint satisfaction problems admit commutativity gadgets?

Characterization of the existence of quantum strategies for the perfect matching game Mančinska and Roberson show that two graphs are quantum isomorphic exactly when their homomorphism counts from any planar graphs are equal [9]. This is a completely combinatorial characterization of the existence of a perfect quantum strategy for the graph isomorphism game. In our work, we give a combinatorial characterization for the existence of a nonsignaling perfect strategy. Does there exist such a characterization for the perfect matching games?

Additional characterization for nonsignaling perfect matching In Theorem 1.6.10, we show that the nonsignaling value of the perfect matching game on graph G is 1 if and only if G has a fractional perfect matching avoiding triangles. A fractional perfect matching of G is just a function $f : E(G) \to [0, 1]$ such that around any vertex, the sum of f is 1. There is a classic theorem from graph theory that says that in fact we can restrict the codomain to just $\{0, 1/2, 1\}$ which is equivalent to the fact that the graph can be decomposed into odd cycles and single matchings [31]. The proof of this theorem follows by choosing a fractional perfect matching with the smallest support and showing that this is the candidate fractional perfect matching with weights in $\{0, 1/2, 1\}$. To accomplish this, certain subgraphs in the support are barred by showing that if they existed, then there is a transformation of the edge weights which would reduce the support even further. Unfortunately, not all of these transformations preserve the sum of edge weights on triangles and hence some adaptation is required for the case of fractional perfect matchings avoiding triangles. Nonetheless, we believe a statement like this should be true. In particular,

Conjecture 1.1.4. G has a fractional perfect matching avoiding triangles if and only if G has a fractional perfect matching avoiding triangles taking values in $\{0, 1/2, 1\}$.

Note that this would imply that the graph G also have a decomposition into odd cycles with size ≥ 5 and single matchings.

1.2 Preliminaries

1.2.1 Nonlocal games

Definition 1.2.1. A *nonlocal game* $\mathcal{G}$ is a tuple $(\mathcal{X}, \mathcal{A}, V)$ consisting of a finite set $\mathcal{X}$ of inputs for Alice and Bob, and a finite set $\mathcal{A}$ of outputs as well as a verification function $V : \mathcal{X} \times \mathcal{X} \times \mathcal{A} \times \mathcal{A} \to \{0, 1\}$.

A nonlocal game is played by a verifier and two provers, Alice and Bob. In the game, the verifier samples a pair (x, y) uniformly at random and sends x to Alice and y to Bob. Alice and

Bob respond with a and b, respectively. They win if $V(x, y, a, b) = 1$. The players are not allowed to communicate during the game, but they can agree on a strategy beforehand. Their goal is to maximize their winning probability.

Definition 1.2.2. A nonlocal game is called *synchronous* if on simultaneously receiving the same questions Alice and Bob must respond identically to win, i.e. $V(x, x, a, b) = 0$ if $a \neq b$. Furthermore, we call a nonlocal game *bisynchronous* if it is synchronous and additionally on receiving differing questions they may not respond with the same answer to win, i.e. $V(x, y, a, a) = 0$ if $x \neq y$.

Definition 1.2.3. A *classical strategy* S for a nonlocal game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, V)$ is a tuple $S = (f_A, f_B)$, consisting of maps $f_A : \mathcal{X} \to \mathcal{A}$ for Alice and $f_B : \mathcal{X} \to \mathcal{A}$ for Bob.

Definition 1.2.4. A *quantum (tensor) strategy* S for a nonlocal game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, V)$ is a tuple $S = (\mathcal{H}_A, \mathcal{H}_B, |\psi\rangle, \{A_{xa}\}, \{B_{yb}\})$, consisting of finite dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, a bipartite state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, PVMs $\{A_{xa}\}_{a \in \mathcal{A}}$ acting on $\mathcal{H}_A$ for each $x \in \mathcal{X}$ for Alice and PVMs $\{B_{yb}\}_{b \in \mathcal{A}}$ acting on $\mathcal{H}_B$ for each $y \in \mathcal{X}$ for Bob. Often we will drop the Hilbert spaces, and just write $S = (|\psi\rangle, \{A_{xa}\}, \{B_{yb}\})$.

Here we restrict without loss of generality to pure states and projective measurements (PVMs). For a strategy $S = (|\psi\rangle, \{A_{xa}\}, \{B_{yb}\})$, the probability of Alice and Bob answering a, b when obtaining x, y is given by $p(a, b|x, y) = \langle\psi|A_{xa} \otimes B_{yb}|\psi\rangle$. Therefore, the *winning probability* of a quantum strategy S for the nonlocal game $\mathcal{G}$ is given by

$$\omega^*(S, \mathcal{G}) = \sum_{x,y} \frac{1}{|\mathcal{X}^2|} \sum_{a,b} V(x, y, a, b) p(a, b|x, y) = \sum_{x,y} \frac{1}{|\mathcal{X}^2|} \sum_{a,b} V(x, y, a, b) \langle\psi|A_{xa} \otimes B_{yb}|\psi\rangle.$$

For a nonlocal game $\mathcal{G}$, we define the *quantum value* $\omega^*(\mathcal{G}) = \sup_S \omega^*(S, \mathcal{G})$ to be the supremum over all quantum tensor strategies compatible with $\mathcal{G}$. A game is said to exhibit pseudotelepathy if it has a quantum perfect strategy but no classical perfect strategy.

The tensor-product structure is a way of mathematically representing the locality of the players employing a quantum strategy in a nonlocal game. However, there is a more general way to model this nonlocality mathematically.

Definition 1.2.5. A *commuting operator strategy* $\mathcal{S}$ for a nonlocal game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, V)$ is a tuple $\mathcal{S} = (\mathcal{H}, |\psi\rangle, \{A_{xa}\}, \{B_{yb}\})$, consisting of a Hilbert space $\mathcal{H}$, a state $|\psi\rangle \in \mathcal{H}$, and two collections of mutually commuting PVMs $\{A_{xa}\}_{a\in\mathcal{A}}$ acting on $\mathcal{H}$ for each $x \in \mathcal{X}$ for Alice and PVMs $\{B_{yb}\}_{b\in\mathcal{A}}$ acting on $\mathcal{H}$ for each $y \in \mathcal{X}$ for Bob, i.e. $[A_{xa}, B_{yb}] = 0$ for all $a, b, x, y \in \mathcal{A} \times \mathcal{A} \times \mathcal{X} \times \mathcal{X}$. Like for quantum strategies, we will often omit the Hilbert space and write $\mathcal{S} = (|\psi\rangle, \{A_{xa}\}, \{B_{yb}\})$ for a commuting operator strategy.

We can also define the commuting operator (also known as the quantum commuting) value of a nonlocal game $\omega^{qc}(\mathcal{G}) = \sup_S \omega^{qc}(\mathcal{S}, \mathcal{G})$ to be the supremum over all commuting operator strategies S compatible with $\mathcal{G}$. It is not hard to see that every quantum (tensor) strategy is a commuting operator strategy. The converse holds if we restrict our commuting operator strategies to be finite dimensional (i.e. $\mathcal{H}$ is finite dimensional). However, there are examples of nonlocal games $\mathcal{G}$ for which there is a perfect (wins with probability 1) commuting operators strategy but no perfect tensor-product strategy, see for example [13].

Definition 1.2.6. A *nonsignaling strategy* for a nonlocal game is any strategy where

$$\sum_a p(a, b, x, y) = \sum_a p(a, b, x', y) \text{ for every } b, y, x, x'$$

and similarly,

$$\sum_b p(a,b,x,y) = \sum_b p(a,b,x,y') \text{ for every } a,x,y,y'.$$

The nonsignaling value of a nonlocal game $\omega^{ns}(\mathcal{G}) = \sup_S \omega^{ns}(\mathcal{S},\mathcal{G})$ to be the supremum over all nonsignaling strategies S compatible with $\mathcal{G}$. There are many games for which there is an optimal nonsignaling strategy but no quantum one. An example is the CHSH game for which any optimal quantum strategy wins with at most $\sim .85$ probability.

Definition 1.2.7. We say that a strategy is *synchronous* if $p(a,b,x,y) = 0$ whenever $x = y$ and $a \neq b$. Classical synchronous strategies are those for which Alice and Bob use the same map $f_A = f_B : \mathcal{X} \to \mathcal{A}$. Quantum synchronous strategies involve Alice and Bob using an identical set of measurements and a tracial state.

We define the synchronous values of a nonlocal game $\omega^{t,s}(\mathcal{G}) = \sup_S \omega^t(\mathcal{S},\mathcal{G})$ to be the supremum over all t-type synchronous strategies S compatible with $\mathcal{G}$, t here being any of classical, quantum, commuting operator or nonsignaling. There are many games for which the synchronous and non-synchronous values differ [32]. But for synchronous games we have the following result

Theorem 1.2.8 ([32])**.** *If a synchronous game has a perfect strategy, then it also has a perfect synchronous strategy. This is true in all of the classical, quantum, commuting operator and nonsignaling settings.*

1.2.2 Graph games

Definition 1.2.9. Given graphs $G = (V_G, E_G)$ and $H = (V_H, E_H)$, the homomorphism game $Hom(G,H)$ is the synchronous game with question set V_G and answer set V_H. The players win if when they receive vertices in G they respond with vertices in H that preserve the adjacency relations between the players. I.e. on questions g_A, g_B they respond with h_A, h_B such that $g_A \sim g_B$ if and only if $h_A \sim h_B$.

Definition 1.2.10. The quantum chromatic number $\chi_q(G)$ of a graph G is the smallest c such that $Hom(G, K_c)$ has a perfect quantum strategy.

The quantum chromatic number is sandwiched between the classical clique and chromatic numbers $\omega(G) \leq \chi_q(G) \leq \chi(G)$. [10]

Definition 1.2.11. The quantum independence number $\alpha_q(G)$ of a graph G is the largest c such that $Hom(K_c, \bar{G})$ has a perfect quantum strategy, where $\bar{G}$ is the graph complement of G.

Definition 1.2.12. The quantum clique number $\omega_q(G)$ of a graph G is the largest c such that $Hom(K_c, G)$ has a perfect quantum strategy.

Definition 1.2.13. Given graphs $G = (V_G, E_G)$ and $H = (V_H, E_H)$, the isomorphism game $Iso(G, H)$ is the synchronous game with question set $V_G \cup V_H$ and answer set $V_G \cup V_H$. The players must respond with a vertex in the opposite graph from that which they received a vertex. After which they will have $g_A, g_B \in G$ and $h_A, h_B \in H$. The players win if vertices in G (which may have been question or answer vertices for either) have the same adjacency relationship to those in H.

1.2.3 Graph theory

Definition 1.2.14. Given a (hyper)graph $G = (V, E)$, a *matching* $M \subset E$ is a set of pairwise non-adjacent edges. A *perfect matching* is a matching which covers all vertices in G.

Definition 1.2.15. Given a bipartite graph $G = (L \sqcup R, E)$, an *L-perfect matching* $M \subset E$ is a matching which covers all vertices in L.

The following definition is a linear relaxation of the definition of a perfect matching.

Definition 1.2.16. A graph $G = (V, E)$ has a *fractional perfect matching* if there exists a function $f : E \to [0, 1]$ such that for each vertex $v \in V$, $\sum_{(u,v)\in E} f\big((u, v)\big) = 1$.

Theorem 1.2.17 ([31])**.** *Given a graph with a fractional perfect matching, there is one where* $f : E \to \{0, \frac{1}{2}, 1\}$.

Given a graph $G = (V, E)$, denote $N_G(S) \subset V$ the set of vertices adjacent to the subset $S \subset V$.

Theorem 1.2.18 (Hall's marriage theorem)**.** *Let $G = (L \sqcup R, E)$ be a bipartite graph. G has a L-perfect matching if and only if every subset $S \subset L$ satisfies*

$$|S| \leq |N_G(S)|.$$

Theorem 1.2.19 ([33])**.** *A graph $G = (V, E)$ has a perfect matching if and only if for every subset $S \subset V$, the subgraph $G[V \setminus S]$ has at most $|U|$ odd connected components.*

Theorem 1.2.20 ([33])**.** *A graph $G = (V, E)$ has a fractional perfect matching if and only if there is a collection of edges that form a disjoint covering of the vertices made up of matchings and odd cycles.*

Lastly, we define the notion of a line graph of a graph.

Definition 1.2.21. Given a graph $G = (V, E)$, the *line graph of G* denoted by $L(G)$ is the graph with vertices E and edges $(e, f) \in E \times E$ such that $e \cap f \neq \emptyset$.

Proposition 1.2.22. *A graph $G = (V, E)$ has a perfect matching if and only if the independence number of its line graph is $\alpha(L(G)) = |V|/2$.*

1.3 Nonlocal games from perfect matchings

In this section, we give nonlocal games corresponding to graph matching properties. These games are the main objects of study in this paper.

1.3.1 The bipartite perfect matching game

Definition 1.3.1. Given a bipartite graph $G = (L \sqcup R, E)$, the *bipartite L-perfect matching game BPM_G* is a synchronous game with question set L and answer set E. The players win if and only if the question-answer pairs $(v_1, v_2) \in L \times L$ and $e_1, e_2 \in E \times E$ satisfy

1. (adjacency) $v_1 \in e_1$ and $v_2 \in e_2$; and
2. (consistency and edge disjointedness) either $e_1 = e_2$ or $e_1 \cap e_2 = \emptyset$.

The second condition says that if both players are given the same vertex then they have to give the same matching; and if they are given different vertices then they need to give different matchings. We can more eloquently write this condition as

$$e_1 \cap e_2 \neq \emptyset \implies e_1 = e_2.$$

We now show that these are indeed the natural games to define for the bipartite perfect matching property.

Theorem 1.3.2. *Given a bipartite graph $G = (L \sqcup R, E)$, the game BPM_G has a perfect classical strategy if and only if G has an L-perfect matching.*

Proof. Let G be a bipartite graph with an L-perfect matching M. On questions (v_1, v_2), Alice and

Bob will respond with $e_1 \ni v_1$ and $e_2 \ni v_2$, according to the matching M. Clearly, if $v_1 = v_2$ then $e_1 = e_2$. Now, since M is a perfect matching if $v_1 \neq v_2$ then $e_1 \cap e_2 = \emptyset$.

Now suppose the game BPM_G has a perfect classical strategy. Since BPM_G is a synchronous game, by Theorem 1.2.8 it must also have a perfect synchronous strategy where Alice and Bob both respond according to the same function $f : L \to E$. Since f is a perfect strategy and the defining conditions of BPM_G are exactly those which define an L-perfect matching, $M = f(V)$ is an L-perfect matching. □

1.3.2 The perfect matching game

We now give the natural extension of the bipartite perfect matching game to perfect matchings on an entire graph.

Definition 1.3.3. Given a graph $G = (V, E)$, the *perfect matching game* PM_G is a synchronous game with question set V and answer set E. The players win if and only if the question-answer pairs $(v_1, v_2) \in V \times V$ and $e_1, e_2 \in E \times E$ satisfy

1. (adjacency) $v_1 \in e_1$ and $v_2 \in e_2$; and
2. (consistency and edge disjointedness) $e_1 \cap e_2 \neq \emptyset \implies e_1 = e_2$.

Theorem 1.3.4. *Given a graph* $G = (V, E)$ *the game* PM_G *has a perfect classical strategy if and only if* G *has a perfect matching.*

Proof. The proof is identical to that of Theorem 1.3.2 except where M is a perfect matching not an L-perfect matching. □

1.3.3 The fractional perfect matching game

In the graph theory literature, there is a notion of having a *fractional perfect matching*. This is a relaxation of the usual notion of perfect matching where now the selected edges have a weight and the condition is that for all vertices, the weights of the edges incident to the vertex sum to 1. We shall also define a nonlocal game which represents this property.

Given $G = (V, E)$, the *bipartite double cover of* G is $G \times K_2$. We shall give a subset of the bipartite perfect matching games a different name. The motivation for this will be justified in the following theorems.

Definition 1.3.5. Given a graph $G = (V, E)$, the *fractional perfect matching game* FPM_G is the synchronous game $BPM_{G \times K_2}$.

This definition is natural as we have the following lemma from graph theory.

Lemma 1.3.6. *G has a fractional perfect matching if and only if $G \times K_2$ has a L-perfect matching.*

Proof. Suppose G has a fractional perfect matching. In particular then the graph has a covering made of disjoint odd cycles and matchings. To recover a L-perfect matching lift this cover onto the $G \times K_2$. Where the cycles are given some orientation and in the bipartite graph a vertex on the left is matched with a vertex on the right only if there was an outgoing edge in the original graph. Then this gives a matching since every left vertex is covered and its clearly disjoint.

Now suppose $G \times K_2$ has a L-perfect matching. Then we can recover a a collection of disjoint odd cycles and matching on the original graph by mapping the edges in the L-perfect matching back onto G. Therefore, since there is a covering of G by disjoint odd cycles and matching, G has a perfect fractional matching. □

Corollary 1.3.7. *FPM_G has a perfect classical strategy if and only if G has a fractional perfect matching.*

Proof. By definition, FPM_G has a perfect classical strategy if and only if $BPM_{G\times K_2}$ has a perfect classical strategy. Then by Theorem 1.3.2 and Lemma 1.3.6, $BPM_{G\times K_2}$ has a perfect classical strategy if and only if $G \times K_2$ has a perfect matching if and only if G has a fractional perfect matching. □

We give another perspective on the fractional perfect matching games as a relaxation of PM_G. The consistency condition for the perfect matching game from before can be equivalently given by the following set of conditions: If $e_1 = (v_1, w_1)$ and $e_2 = (v_2, w_2)$, then

1. if $v_1 = v_2$ then $w_1 = w_2$,
2. if $v_1 \neq v_2$ then $w_1 \neq w_2$, and
3. $v_1 = w_2$ if and only if $v_2 = w_1$.

Without the final "symmetry" condition this alternatively defines the fractional perfect matching game.

1.3.4 The hypergraph perfect matching game

Continuing down this line of definitions, we can define the analogous perfect matching game for hypergraphs.

Definition 1.3.8. Given a hypergraph $G = (V, E)$, the *perfect matching game PM_G* is a synchronous game with question set V and answer set E. Here E represents a set of hyperedges. The players win if and only if the question-answer pairs $(v_1, v_2) \in V \times V$ and $e_1, e_2 \in E \times E$ satisfy

1. (adjacency) $v_1 \in e_1$ and $v_2 \in e_2$; and

2. (consistency and edge disjointedness) $e_1 \cap e_2 \neq \emptyset \implies e_1 = e_2$.

Again, we can show that classical perfect strategies for this game exactly correspond to hypergraph perfect matchings.

Theorem 1.3.9. *Given a hypergraph $G = (V, E)$ the game PM_G has a perfect classical strategy if and only if G has a perfect matching.*

Proof. The proof is identical to that of Theorem 1.3.4. □

1.4 Quantum and nonsignaling bipartite perfect matching

1.4.1 Quantum bipartite perfect matchings

Let $K_{n,k}$ be the complete bipartite graph. Then $BM_{K_{n,k}}$ is the same as the k-coloring game for the complete graph on n vertices K_n. Therefore, for $k < n$ we have $\omega^*(BM_{K_{n,k}}) < 1$ since the quantum chromatic number of K_n is $\chi_q(K_n) = n$ [10]. It turns out that no bipartite graph has quantum pseudo-telepathy for the bipartite perfect matching game precisely because of this fact.

Theorem 1.4.1. *For any bipartite graph $G = (L \sqcup R, E)$, we have $\omega^*(BPM_G) = 1$ if and only if $\omega(BPM_G) = 1$.*

Proof. It suffices to prove that if $\omega^*[BPM_G] = 1$ then $\omega[BPM_G] = 1$. We do this by proving the converse. Suppose $\omega(BPM_G) < 1$ then from Theorem 1.3.2 G has no L-perfect matching. Hence, by **??** 1.2.18, there is some set $S \subset L$ such that $|N_G(S)| < |S|$. Let $n = |S|$ and $k = |N_G(S)|$.

Considering the subgraph $G[S]$ induced by the subset S, we immediately see that

$$\omega^*(BPM_{G[S]}) \leq \omega^*(BPM_{K_{n,k}}) < 1$$

where the last inequality follows from the fact that $BPM_{K_{n,k}}$ is equal to the k-coloring game for K_n. Finally, since $\omega^*(BPM_{G[S]}) < 1$ then $\omega^*(BPM_G) < 1$ since any perfect strategy for BPM_G could just be restricted to $BPM_{G[S]}$. □

Since the fractional perfect matching game is just a subset of the bipartite perfect matching games, there is no pseudo-telepathy for all fractional perfect matching games as well.

Corollary 1.4.2. *For any graph G, we have $\omega^*(FPM_G) = 1$ if and only if $\omega(FPM_G) = 1$.*

Even though quantum fractional and bipartite perfect matchings do not define new properties, we will see in section 1.5 these games can have quantum advantage.

1.4.2 Nonsignaling bipartite perfect matchings

Let $G = (L \sqcup R, E)$ be a bipartite graph. Then let $G^\# = (L^\# \sqcup R^\#, E^\#)$ be the graph where we iteratively removed the degree 1 vertices in L and their neighbours in R until none remain. This process is well defined up to isomorphism. In this section we show that a bipartite graph G has nonsignaling L-perfect matching if and only if $G^\#$ contains no lone vertices in $L^\#$.

In particular, the complete bipartite graphs $K_{n,k}$ with $k \geq 2$ satisfy the above property. Therefore, letting $n > k$, we get an infinite family of graphs with nonsignaling L-perfect matching but no classical L-perfect matching.

Intuitively, this process just pairs off "forced matchings" and removes them from the graph.

Once all of the "forced matchings" are removed, if there are any vertices in $G^{\#}$ which cannot be paired (i.e., they are isolated) then there can be no possible strategy.

Theorem 1.4.3. *Let $G = (L \sqcup R, E)$ be a bipartite graph. Then the following are equivalent:*

1. *$\omega^{ns}(BPM_G) = 1$,*
2. *$G^{\#}$ contains no lone vertices in $L^{\#}$,*
3. *there exists a perfect matching subgraph $P \subset G$ and left-degree 2 subgraph S such that $P \sqcup S \subset G$ covering all of L.*

Proof. We shall first show that a left-degree 2 graph G always has a nonsignaling perfect strategy. We shall explicitly define the nonsignaling correlation p. Take the correlation to be supported on $e_1 \in E(v_1)$ and $e_2 \in E(v_2)$, and set

$$p(e_1, e_2 | v_1, v_2) = \begin{cases} \frac{1}{2}, & \text{if } v_1 = v_2 \text{ and } e_1 = e_2 \\ \frac{1}{2}, & \text{if } v_1 \neq v_2, N(v_1) \cap N(v_2) \neq \emptyset, \text{and } e_1 \cap e_2 = \emptyset, N(v_1) \cap N(v_2) \subset e_1 \cup e_2 \\ \frac{1}{4}, & \text{if } v_1 \neq v_2 \text{ and } N(v_1) \cap N(v_2) = \emptyset \\ 0, & \text{otherwise.} \end{cases}$$

We see that this defines a probability distribution. For $v_1 = v_2$,

$$\sum_{e_1, e_2 \in E} p(e_1, e_2 | v_1, v_1) = \sum_{e \in E(v_1)} \frac{1}{2} = \frac{1}{2} |E(v_1)| = 1.$$

For $v_1 \neq v_2$, let $N(v_1) = \{w_1, w_2\}$ and $N(v_2) = \{u_1, u_2\}$. If, without loss of generality, $w_1 = u_1$

and $w_2 \neq u_2$ then

$$\sum_{e_1,e_2 \in E} p(e_1, e_2|v_1, v_2) = p((v_1, w_1), (v_2, u_2)|v_1, v_2) + p((v_1, w_2), (v_2, u_1)|v_1, v_2) = 1.$$

If $N(v_1) = N(v_2)$, then

$$\sum_{e_1,e_2 \in E} p(e_1, e_2|v_1, v_2) = p((v_1, w_1), (v_2, w_2)|v_1, v_2) + p((v_1, w_2), (v_2, w_1)|v_1, v_2) = 1.$$

Finally, if $v_1 \neq v_2$ and $N(v_1 \cap N(v_2) = \emptyset$, then

$$\sum_{e_1,e_2 \in E} p(e_1, e_2|v_1, v_2) = \sum_{e_1 \in E(v_1), e_2 \in E(v_2)} p(e_1, e_2|v_1, v_2) = \frac{1}{4}|E(v_1)||E(v_2)| = 1.$$

It is easy to see that this probability distribution satisfies perfectly all of the rules of the bipartite perfect matching game. Hence, we just need to check that it satisfies the nonsignaling condition. Indeed, for any $v_1, v_2 \in L$ and $e_2 \in E(v_2)$ (or else p is just 0 and the nonsignaling condition trivially holds), we have

$$\sum_{e_1} p(e_1, e_2|v_1, v_2) = \frac{1}{2}$$

in all cases. This shows that if one can find a perfect matching subgraph P and left-degree 2 subgraph S such that P and S partition L, then we have a nonsignaling perfect strategy for G and establishes (3) implies (1).

Now, suppose that $G^\#$ contains a lone vertex in $L^\#$. A degree 1 vertex can only pick its unique edge in a perfect strategy, which also removes its neighboring right vertex from any other left vertices strategy. Therefore, the graph with the degree 1 left vertex and its neighbor removed has a perfect nonsignaling matching if and only if the original graph did. Then, it is clear that there is no nonsignaling strategy for G since the lone vertex can not be matched in $G^{\#}$ and G has a perfect nonsignaling matching if and only if G does. This establishes (1) implies (2).

Finally, we show that (2) implies (3). However, if $L^{\#}$ contains no lone vertices and the process has terminated then it must mean that $G^{\#}$ has left-degree ≥ 2. Let P be the removed degree 1 edges and $S = G^{\#}$ and we obtain the desired condition for (3). □

From the above we also get that a graph $G = (V, E)$ has nonsignaling perfect fractional matching if $(G \times K_2)^{\#}$ has no lone vertices on the left.

1.5 Quantum bipartite matching $K_{n,2}$

In section 1.4, we showed that the bipartite matching game does not produce a separate quantum bipartite perfect matching property, this is fundamentally because $\omega^*(BPM_{K_{n,k}}) < 1$ for $k < n$.

However, this does not imply that quantum strategies do not exhibit advantage for the bipartite matching game. To study this we will look at the $K_{n,2}$ graphs and completely characterize their quantum and classical values. This is, in some sense, the most simple class of bipartite graphs one could consider which could have quantum advantage.

We first begin with deriving an expression for the winning probability in terms of quantum operators. We know that for a general strategy p,

$$
\begin{aligned}
\omega(BPM_{K_{n,2}}, p) &= \frac{1}{n^2} \sum_{v_1, v_2 \in [n]} \sum_{e_1 \in E(v_1), e_2 \in E(v_2)} p(e_1, e_2 | v_1, v_2) V_{BPM_{K_{n,2}}}(e_1, e_2, v_1, v_2) \\
&= \frac{1}{n^2} \sum_{v \in [n]} \sum_{e \in E(v)} p(e, e, | v, v) + \frac{1}{n^2} \sum_{v_1 \neq v_2 \in [n]} \sum_{\substack{e_1 \in E(v_1), e_2 \in E(v_2): \\ e_1 \cap e_2 = \emptyset}} p(e_1, e_2 | v_1, v_2) \\
&= \frac{1}{n^2} \sum_{v \in [v]} \sum_{a \in [2]} p((v, a), (v, a) | v, v) + \frac{1}{n^2} \sum_{v_1 \neq v_2 \in [n]} \sum_{a_1 \neq a_2 \in [2]} p((v_1, a_1), (v_2, a_2) | v_1, v_2).
\end{aligned}
$$

Note that once the question, which is a left vertex, is fixed, a right vertex completely determines the edge. Hence, for a quantum strategy, we have operators $\{A_{va}\}$ and $\{B_{ub}\}$ with state ρ such that

$$
\omega(BPM_{K_{n,2}}, p) = \frac{1}{n^2} \mathrm{TR}[\sum_{v \in [v]} \sum_{a \in [2]} A_{va} B_{va} + \sum_{v_1 \neq v_2 \in [n]} \sum_{a_1 \neq a_2 \in [2]} A_{v_1 a_1} B_{v_2 a_2}] \rho.
$$

Noting that

$$
\begin{aligned}
2\omega(BPM_{K_{n,2}}, p) - 1 =& \frac{1}{n^2} \mathrm{Tr} \Bigg(\Bigg(\sum_{v \in [v]} [\sum_{a \in [2]} A_{va} B_{va} - \sum_{a_1 \neq a_2 \in [2]} A_{va_1} B_{va_2}] \\
& + \sum_{v_1 \neq v_2 \in [n]} [\sum_{a_1 \neq a_2 \in [2]} A_{v_1 a_1} B_{v_2 a_2} - \sum_{a \in [2]} A_{v_1 a} B_{v_2 a}] \Bigg) \rho \Bigg).
\end{aligned}
$$

Defining $A_v := A_{v1} - A_{v2}$ and $B_v := B_{v1} - B_{v2}$, we see that

$$
\begin{aligned}
\omega(BPM_{K_{n,2}}, p) &= \frac{1}{2n^2} \mathrm{TR}[\sum_{v \in [n]} A_v B_v - \sum_{v_1 \neq v_2 \in [n]} A_{v_1} B_{v_2}] \rho + \frac{1}{2} \\
&= \frac{1}{2n^2} \mathrm{TR}[n^2 I - \sum_{v_1 \in [n]} A_{v_1} [\sum_{v_2 \in [n]} (-1)^{\delta_{v_1 = v_2}} B_{v_2}]] \rho
\end{aligned}
$$

Lets start by looking at quantum synchronous strategies, we have that the winning probability is described by a single set of observables $\{A_v\}$. Thus,

$$\begin{aligned}\omega(BPM_{K_{n,2}}, p) &= \frac{1}{2n^2}\mathrm{TR}\sum_{v\in[n]} A_v^2 - \sum_{v_1\neq v_2\in[n]} A_{v_1}A_{v_2} + \frac{1}{2}\\ &= \frac{1}{2n^2}\mathrm{TR}nI - \sum_{v_1\neq v_2\in[n]} A_{v_1}A_{v_2} + \frac{1}{2}\\ &= \frac{1}{2n^2}\mathrm{TR}2nI - \sum_{v_1, v_2\in[n]} A_{v_1}A_{v_2} + \frac{1}{2}\\ &= \frac{1}{2} + \frac{1}{n} - \frac{1}{2n^2}\mathrm{TR}[\sum_{v} A_v]^2.\end{aligned}$$

This shows that whenever we have observables such that $\sum_v A_v = 0$, then we have a quantum synchronous strategy achieving value $\frac{1}{2} + \frac{1}{n}$. Hence we've shown the following lowerbound.

Lemma 1.5.1. *$\omega^*(BPM_{K_{n,2}}) \geq \frac{1}{2} + \frac{1}{n}$ for all $n \geq 2$.*

Additionally, we have that

$$\frac{1}{2} + \frac{1}{n} - [\frac{1}{2n^2}\sum_{v\in[n]} A_v^2 - \sum_{v_1\neq v_2\in[n]} A_{v_1}A_{v_2} + \frac{1}{2}] = \frac{1}{2n^2}[\sum_{v} A_v]^2$$

at the algebra level. This sum-of-squares decomposition proves $\frac{1}{2} + \frac{1}{n}$ is optimal for quantum synchronous strategies and therefore $\omega^{*,s}(BPM_{K_{n,2}}) = \frac{1}{2} + \frac{1}{n}$.

Now we will upperbound the general quantum value of the $K_{n,2}$ games.

Lemma 1.5.2. *We have the following upperbounds*

1. *$\omega^*(BPM_{K_{3,2}}) \leq \frac{5}{6}$.*

2. *$\omega^*(BPM_{K_{n,2}}) \leq 1 - \frac{1}{n}$ for $n \geq 4$.*

Proof. Consider the Frobenius norm with respect to some state ρ. We have that

$$\begin{aligned}
\frac{1}{2n^2}\left\|n^2 - \sum_{v_1} A_{v_1}\left(\sum_{v_2}(-1)^{\delta_{v_1=v_2}}B_{v_2}\right)\right\|_\rho &\le \frac{1}{2} + \frac{1}{2n^2}\left\|\sum_{v_1} A_{v_1}\left(\sum_{v_2}(-1)^{\delta_{v_1=v_2}}B_{v_2}\right)\right\|_\rho \\
&\le \frac{1}{2} + \frac{1}{2n^2}\sum_{v_1}\|A_{v_1}\|_\rho \left\|\left(\sum_{v_2}(-1)^{\delta_{v_1=v_2}}B_{v_2}\right)\right\|_\rho \\
&\le \frac{1}{2} + \frac{1}{2n^2}\sum_{v_1}\left\|\left(\sum_{v_2}(-1)^{\delta_{v_1=v_2}}B_{v_2}\right)\right\|_\rho \\
&= \frac{1}{2} + \frac{1}{2n^2}\sqrt{n}\sqrt{\sum_{v_1}\left\|\left(\sum_{v_2}(-1)^{\delta_{v_1=v_2}}B_{v_2}\right)\right\|_\rho^2}.
\end{aligned}$$

Focusing on the last factor in the last term,

$$\begin{aligned}
\sum_{v_1}\|[\sum_{v_2}(-1)^{\delta_{v_1=v_2}}B_{v_2}]\|_\rho^2 &= \sum_{v_1}\sum_{v_2,v_2'}(-1)^{\delta_{v_1=v_2}+\delta_{v_1=v_2'}}\mathrm{TR}B_{v_2}, B_{v_2'}\rho \\
&= n^2 + \sum_{v_1}\sum_{v_2\neq v_2'}(-1)^{\delta_{v_1=v_2}+\delta_{v_1=v_2'}}\mathrm{TR}B_{v_2}, B_{v_2'}\rho \\
&= n^2 + \sum_{v_2\neq v_2'}\left(\sum_{v_1}(-1)^{\delta_{v_1=v_2}+\delta_{v_1=v_2'}}\right)\mathrm{TR}B_{v_2}, B_{v_2'}\rho \\
&= n^2 + \sum_{v_2\neq v_2'}(n-4)\mathrm{TR}B_{v_2}, B_{v_2'}\rho \\
&= n^2 - (n-4)n + (n-4)\left\|\sum_{v_2}B_{v_2}\right\|_\rho^2 .
\end{aligned}$$

Then, the above becomes

$$\begin{aligned}\frac{1}{2n^2}\left\|n^2-\sum_{v_1}A_{v_1}\left(\sum_{v_2}(-1)^{\delta_{v_1=v_2}}B_{v_2}\right)\right\|_\rho &= \frac{1}{2}+\frac{1}{2n^2}\sqrt{n}\sqrt{n^2-(n-4)n+(n-4)\left\|\sum_{v_2}B_{v_2}\right\|^2}\\ &= \frac{1}{2}+\frac{1}{2n^2}\sqrt{n}\sqrt{4n+(n-4)\left\|\sum_{v_2}B_{v_2}\right\|^2}\end{aligned}$$

For $n=3$, $(n-4)=-1$, the above quantity is upperbounded by

$$\frac{1}{2}+\frac{1}{2n^2}\sqrt{n}\sqrt{4n}=\frac{5}{6}.$$

For $n \geq 4$, we need to upperbound $\left\|\sum_{v2}B_{v_2}\right\|^2$ by n^2. This gives us

$$\frac{1}{2}+\frac{\sqrt{n^2-4n+4}}{2n}=\frac{1}{2}+\frac{|n-2|}{2n}$$

which is $1-\frac{1}{n}$ for $n \geq 4$. □

The synchronous quantum strategy saturates the $\frac{5}{6}$ bound for $K_{3,2}$.

For $BPM_{K_{n,2}}$ for $n \geq 4$ we show that we have classical strategies which saturate the quantum upperbound.

Lemma 1.5.3. *$\omega(BPM_{K_{n,2}}) \geq 1-\frac{1}{n}$ for all $n \geq 4$.*

Proof. Consider the “trivial” classical strategy where Alice always outputs the first right vertex and Bob always outputs the second right vertex. We note that this strategy only fails when Alice and Bob receive the same vertex. This constitutes n of the n^2 vertex pairs that the players could be asked which establishes the result. □

We now finally give a classical upperbound for $BPM(K_{3,2})$ which completes the study of the quantum and classical values for $K_{n,2}$ bipartite perfect matching games.

Lemma 1.5.4. $\omega(BPM_{K_{3,2}}) = \frac{7}{9}$.

Proof. The optimal classical value can be achieved via a deterministic strategy. Let $a_i, b_j \in \{\pm 1\}$ be the expected value for the deterministic strategy with $+1$ be the weighting for the first right vertex and -1 be the weighting for the second right vertex.

Without loss of generality, $a_1 = a_2$. Then,

$$\begin{aligned} \frac{1}{18}[9 - a_1[-b_1 + b_2 + b_3] - a_2[b_1 - b_2 + b_3] - a_3[b_1 + b_2 - b_3]] &= \frac{1}{18}[9 - 2a_1 b_3 - a_3[b_1 + b_2 - b_3]] \\ &\leq \frac{14}{18} = \frac{7}{9}. \end{aligned}$$

We see that this is optimal as setting $a_1 = a_2 = -1$, $a_3 = 1$, $b_1 = b_2 = -1$, and $b_3 = 1$ yields the value $\frac{7}{9}$. □

This shows that we only have quantum advantage for $n = 3$ for the graph $K_{3,2}$, which is also the only case where the optimal quantum value is achieved by playing synchronously. We summarize all the bounds in the theorem below.

Theorem 1.5.5. *For the $BPM_{K_{n,2}}$ games, we have the following:*

1. $\omega(BPM_{K_{3,2}}) = \frac{7}{9} < \frac{5}{6} = \omega^*(BPM_{K_{3,2}})$,
2. $\omega(BPM_{K_{n,2}}) = \omega^*(BPM_{K_{n,2}}) = 1 - \frac{1}{n}$ *for all* $n \geq 4$,
3. $\omega^{*,s}(BPM_{K_{n,2}}) = \frac{1}{2} + \frac{1}{n}$ *for all* $n \geq 2$.

Additionally, we have a sum-of-squares decomposition for $BPM_{K_{3,2}}$ which gives an alternative proof of $\omega^*(BPM_{K_{3,2}}) = \frac{5}{6}$.

$$
\begin{aligned}
6I - &(A_1(B_1 - B_2 - B_3) + A_2(-B_1 + B_2 - B_3) + A_3(-B_1 - B_2 + B_3)) \\
&= \frac{1}{2}[A_1 - A_3 - B_1 + B_3]^2 + \frac{1}{2}[A_1 - A_2 - B_1 + B_2]^2 \\
&\quad + \frac{1}{4}[A_1 + A_2 + A_3 + B_1 + B_2 + B_3]^2 + \frac{1}{12}[A_1 + A_2 + A_3 - B_1 - B_2 - B_3]^2
\end{aligned}
$$

Furthermore, any optimal strategy for this game must satisfy the identities $\sum_i A_i = \sum_i B_i = 0$. This can be derived from the sum-of-square proof of optimality by adding the last two terms to get

$$(A_1 + A_2 + A_3 + B_1 + B_2 + B_3) + (A_1 + A_2 + A_3 - B_1 - B_2 - B_3) = 2\sum_i A_i = 0$$

and similarly,

$$(A_1 + A_2 + A_3 + B_1 + B_2 + B_3) - (A_1 + A_2 + A_3 - B_1 - B_2 - B_3) = 2\sum_i B_i = 0.$$

1.6 Perfect matching

In this section, we take the same approach to define the notions of quantum and nonsignaling perfect matching for general graphs.

1.6.1 Quantum perfect matching

Unlike the bipartite and fractional games, the perfect matching game exhibits quantum pseudo-telepathy for many graphs. Therefore quantum perfect matching defines a distinct property to perfect matching.

First we give a simple characterization of quantum strategies for the perfect matching game.

Lemma 1.6.1. *Given a graph $G = (V, E)$ any perfect synchronous quantum strategy for PM_G given by projectors Π_x^y for $x, y \in V$ will have the following properties:*

1. $\Pi_{(x,y)} := \Pi_x^y = \Pi_y^x$ *for every* $x, y \in V$.

2. $\Pi_e = 0$ *if* $e \notin E$.

3. $\sum_{e \in E(x)} \Pi_e = I$ *for every* $x \in V$.

4. $\Pi_e \Pi_h = \delta_{e=h} \Pi_e$ *for every* $e, h \in E$ *where* $e \cap h \neq \emptyset$.

Proof. Rule games imply (1,2,4), (3) because its a strategy. □

We will see that a graph G having a quantum perfect matching is equivalent to its line graph $L(G)$ having a projective packing of value $|V(G)|/2$, which is equivalent to $2L(G)$ (the disjoint union of two copies of $L(G)$) having quantum independence number $|V(G)|$. First we must define projective packing number and quantum independence number.

Definition 1.6.2 ([34, 35])**.** A *d-dimensional projective packing* of a graph G is an assignment $x \longrightarrow \Pi_x \in \mathbb{C}^{d \times d}$ of projections to the vertices of $V(G)$ such that $x \sim y$ implies that $\Pi_x \Pi_y = 0$. The *value* of such a projective packing is

$$\frac{1}{d} \sum_{x \in V(G)} \mathrm{rk}(\Pi_x) = \frac{1}{d} \sum_{x \in V(G)} \mathrm{Tr}(\Pi_x) = \frac{1}{d} \mathrm{Tr}\left(\sum_{x \in V(G)} \Pi_x \right).$$

Additionally, the *projective packing number* of a graph G, denoted $\alpha_p(G)$ is the supremum of the values of projective packings of G.

The quantum independence number of a graph G is defined as the maximum k such that there is a perfect quantum strategy for the k-independent set game on G. However, this is equivalent to the following definition which will be of more direct use for us.

Definition 1.6.3 ([7, 35])**.** Let G be a graph. The *quantum independence number* of G, denoted $\alpha_q(G)$, is the maximum $k \in \mathbb{N}$ such that there exists finite dimensional projections $\Pi_{i,x}$ for all $i \in [k]$ and $x \in V(G)$ satisfying the following:

1. $\sum_{x \in V(G)} \Pi_{i,x} = I$ for all $i \in [k]$.

2. $\Pi_{i,x}\Pi_{j,y} = 0$ if $i \neq j$ and $x = y$ or $x \sim y$.

Note that the first condition implies that $\Pi_{i,x}\Pi_{i,y} = 0$ if $x \neq y$.

It is known that if projections $\Pi_{i,x}$ for $i \in [k]$ and $x \in V(G)$ give a quantum k-independent set of G, then the projections $\Pi_x := \sum_{i \in [k]} \Pi_{i,x}$ are a projective packing of G of value k and thus G always has a projective packing of value equal to its quantum independence number and thus $\alpha_q(G) \leq \alpha_p(G)$.

We now show that a quantum perfect matching of G is equivalent to a projective packing of $L(G)$ of value $|V(G)|/2$. We remark that this is the maximum possible value of a projective packing of $L(G)$.

Theorem 1.6.4. *Let G be a graph. Then the following are equivalent:*

1. *G has a quantum perfect matching.*

2. *$L(G)$ has a projective packing of value $|V(G)|/2$.*

3. *$\alpha_q(2L(G)) = |V(G)|$.*

Proof. We will show that (1) $\Leftrightarrow$ (2) ((2) $\Leftrightarrow$ (3) follows from the above discussion). We first prove that if G has a quantum perfect matching, then $L(G)$ has a projective packing of value $|V(G)|/2$. Since G has a quantum perfect matching, by Lemma 1.6.1 there is an assignment $e \to \Pi_e \in \mathbb{C}^{d\times d}$ (for some d) of projections to the edges of G such that $\Pi_e\Pi_f = 0$ if e and f are incident and $\sum_{e\in E(X)} \Pi_e = I$ for all $x \in V(G)$. Since incidence of edges is adjacency in the line graph, we have that this is in fact a projective packing of $L(G)$. To compute its value, note that

$$2\frac{1}{d}\mathrm{Tr}\left(\sum_{e\in E(G)} \Pi_e\right) = \frac{1}{d}\mathrm{Tr}\left(\sum_{x\in V(G)}\sum_{e\in E(x)} \Pi_e\right) = \frac{1}{d}\mathrm{Tr}(|V(G)|I) = |V(G)|.$$

Therefore the projective packing of $L(G)$ has value $|V(G)|/2$.

Now suppose that $L(G)$ has a projective packing $e \to \Pi_e \in \mathbb{C}^{d\times d}$ of value $|V(G)|/2$. Note that these projections satisfy the orthogonality requirements of Lemma 1.6.1 and thus to prove that G has a quantum perfect matching it is only left to show that $\sum_{e\in E(x)} \Pi_e = I$ for all $x \in V(G)$. For any $x \in V(G)$, we have that $\Pi_e\Pi_f = 0$ for any two distinct $e, f \in E(x)$. Therefore, $\sum_{e\in E(x)}$ is a projection and thus

$$\mathrm{Tr}\left(\sum_{e\in E(x)}\right) \le \mathrm{Tr}(I) = d,$$

with equality if and only if the sum is equal to the identity. Therefore,

$$\frac{1}{d}\mathrm{Tr}\left(\sum_{e\in V(L(G))} \Pi_e\right) = \frac{1}{2d}\mathrm{Tr}\left(\sum_{x\in V(G)}\sum_{e\in E(x)} \Pi_e\right) \le |V(G)|/2,$$

with equality if and only if $\sum_{e\in E(x)} \Pi_e = I$ for all $x \in V(G)$. But we do have equality by assumption, and therefore we have proven that G has a quantum perfect matching. We remark that the above also shows that $|V(G)|/2$ is always an upper bound on the value of a projective packing of

$L(G)$, and so G has a quantum perfect matching precisely when this maximum possible value is attainable. □

Lemma 1.6.5. *K_5 has no quantum pseudotelepathy.*

Proof. We shall show that there cannot be projectors satisfying the above properties for K_5. We begin by showing that if all the above properties are satisfied then all of the projectors must be orthogonal. Indeed, consider edges (x, y) and (z, w) which do not share a vertex. Then, there is a unique vertex $a \neq x, y, z, w$ and so

$$\Pi_{(x,y)} = \Pi_{(x,y)}[\sum_{i\neq a} \Pi_{(i,a)}] = \Pi_{(x,y)}[\Pi_{(z,a)} + \Pi_{(w,a)}].$$

Therefore,

$$\Pi_{(x,y)}\Pi_{(z,w)} = \Pi_{(x,y)}[\Pi_{(z,a)} + \Pi_{(w,a)}]\Pi_{(z,w)} = 0.$$

Now, for any edge (x, y),

$$I = [\sum_{a\neq y} \Pi_{(a,y)}][\sum_{b\neq x} \Pi_{(x,b)}] = \Pi^2_{(x,y)} = \Pi_{(x,y)}$$

which is impossible. □

Lemma 1.6.6. $\omega^*(PM_{K_7}) = 1$.

Proof. A projective packing of $L(K_7)$ is provided by the 7-context Kochen-Specker sets in Section 2 of [36]. □

Theorem 1.6.7. $\omega^*(PM_{K_n}) = 1$ *if and only if* $n \neq 1, 3, 5$.

Proof. Since K_5 does not have a quantum perfect matching, neither does K_3. K_n has a quantum perfect matching for odd $n \geq 7$ as it can be broken into K_7 and an even number of additional verticies that can be classically matched. □

1.6.2 Nonsignaling perfect matching

The cycle graphs C_n for odd $n \geq 5$ are an infinite family of graphs with nonsignaling perfect matching and no quantum or classical perfect matching.

Theorem 1.6.8. *For odd $n \geq 5$, $\omega^{ns}(PM_{C_n}) = 1$.*

Proof. The following defines a simple perfect nonsignaling strategy p. Here → and ← represent the two edges at any vertex of the cycle graph where some orientation of the edges is fixed.

1. $p(\rightarrow, \rightarrow, x, x) = p(\leftarrow, \leftarrow, x, x) = \frac{1}{2}$ for every vertex x.

2. $p(\rightarrow, \leftarrow, x, y) = p(\leftarrow, \rightarrow, x, y) = \frac{1}{2}$ for any two adjacent vertices $x \sim y$.

3. $p(\rightarrow, \rightarrow, x, y) = p(\leftarrow, \leftarrow, x, y) = p(\rightarrow, \leftarrow, x, y) = p(\leftarrow, \rightarrow, x, y) = \frac{1}{4}$ for any two disconnected vertices $x \nsim y$.

□

Definition 1.6.9. Given graph G, we say that a fractional perfect matching $f : E(G) \rightarrow \mathbb{R}$ *avoids triangles* if $\sum_{e \in t} f(e) \leq 1$ for all triangles t in G.

Theorem 1.6.10. *For a graph G, $\omega^{ns}(PM_G) = 1$ if and only if G has a fractional perfect matching avoiding triangles.*

Proof. In this proof, it will be convenient to consider vertices instead of edges for the answers where responding to the question x with vertex a specifies the edge (a, x).

Suppose $\omega^{ns}(PM_G) = 1$ and let p be a bisynchronous nonsignaling correlation witnessing this. We will show that $f(a, x) := p(a|x)$, the marginal of p defines a fractional perfect matching avoiding triangles. Firstly, since p is nonsignaling, for any $a, x \in V(G)$ and any $y \in V(G)$,

$$p(a|x) = \sum_{b \in N(y)} p(a, b|x, y).$$

Substituting $y = x$, we have

$$p(a|x) = \sum_{b \in N(x)} p(a, b|x, x) = p(a, a|x, x)$$

and substituting $y = a$, we have

$$p(a|x) = \sum_{b \in N(a)} p(a, b|x, a) = p(a, x|x, a).$$

This shows that

$$p(a|x) = p(a, a|x, x) = p(a, x|x, a) = p(x, x|a, a) = p(x|a).$$

Now, fix $x \in V(G)$, then

$$\sum_{(a,x) \in E(x)} f(a, x) = \sum_{(a,x) \in E(x)} p(a|x) = \sum_{(a,x) \in E(x)} p(a, a|x, x) = 1.$$

Hence, f is a fractional perfect matching. Now, fix a triangle $\{v, u, w\} \subset V(G)$. Then,

$$\begin{aligned}
1 &= \sum_{a \in N(v), b \in N(u)} p(a, b|v, u) \\
&\geq p(u, v|v, u) + \sum_{a \in N(v)} p(a, w|v, u) + \sum_{b \in N(u)} p(w, b|v, u) \\
&= p(u|v) + p(w|u) + p(w|v) \\
&= f(u, v) + f(w, u) + f(w, v),
\end{aligned}$$

where we used the fact that marginals are well-defined from the nonsignaling condition from line 2 to 3. Hence, f is bounded by 1 on triangles. This completes the forward direction.

Now, for the backwards direction note that the existence of a fractional perfect matching can be formulated as feasibility of a linear program with only integer coefficients. Moreover, the triangle-avoiding condition can also be encoded as linear constraints with integer coefficients. Therefore, if G has a fractional perfect matching that avoids triangles, then it has one that is rational-valued. Let $f : E(G) \to \mathbb{Q}$ be a rational-valued fractional perfect matching of G. It follows that there is some value $r \in \mathbb{N}$ such that $h(e) := rf(e) \in \mathbb{Z}^{\geq 0}$ for all $e \in E(G)$. Note that this means that $\sum_{y \in N(x)} h(xy) = r$ for all $x \in V(G)$, and that $\sum_{e \in t} h(e) \leq r$ for all triangles t in G. We will show how to use f to construct a perfect nonsignaling correlation p for the perfect matching game for G whose marginals $p(y|x)$ are equal to $f(xy)$ for all $xy \in E(G)$.

First, define

$$p(y, y'|x, x) = \begin{cases} f(xy) & \text{if } y = y' \text{ and } xy \in E(G) \\ 0 & \text{otherwise} \end{cases}$$

Now let $x, x' \in V(G)$ with $x \neq x'$. If $xx' \in E(G)$, let $k = h(xx')$, and otherwise set $k = 0$.

Note that for any $y \in N(x) \cap N(x')$, we have that $h(xy) + h(x'y) \leq r - k$. Define a bipartite graph H with parts $A = \{(y, i, 0) : y \in N(x) \setminus \{x'\},\ i = 1, \ldots, h(xy)\}$ and $B = \{(y, i, 1) : y \in N(x') \setminus \{x\},\ i = 1, \ldots, h(x'y)\}$, where $(y, i, 0) \sim (y', j, 1)$ if $y \neq y'$. Note that $|A| = |B| = r-k$. We will show that H has a perfect matching via Hall's theorem. Consider a subset $S \subseteq A$, and define $T = \{y \in N(x) \setminus \{x'\} : \exists\, i \in [h(xy)] \text{ s.t. } (y, i, 0) \in S\}$. Note that if $|T| > 1$, then $N(S) = B$ and thus Hall's condition holds for S. Of course $|T| = 0$ if and only if $S = \varnothing$, so we may assume that $|T| = 1$ and thus there is some $\widehat{y} \in N(x) \setminus \{x'\}$ such that $S \subseteq \{(\widehat{y}, i, 0) : i \in [h(x\widehat{y})]\}$. Thus $|S| \leq h(x\widehat{y})$. Moreover, every vertex of S has the same neighborhood, which is $B \setminus \{(\widehat{y}, j, 1) : j \in [h(x'\widehat{y}]\}$. Therefore,

$$|N(S)| = |B| - h(x'\widehat{y}) = r - k - h(x'\widehat{y}).$$

Recalling that $h(x\widehat{y}) + h(x'\widehat{y}) \leq r - k$, we see that

$$|S| \leq h(x\widehat{y}) \leq r - k - h(x'\widehat{y}) = |N(S)|.$$

Thus Hall's condition holds for arbitrary $S \subseteq A$ and therefore H has a perfect matching.

Now let M be a perfect matching of H. For each $y \in N(x) \setminus \{x'\}$ and $y' \in N(x') \setminus \{x\}$, define $g(y, y')$ to be the number of edges in M of the form $(y, i, 0)(y', j, 1)$ for $i \in [h(xy)]$ and $j \in [h(x'y')]$. Then define

$$p(y, y'|x, x') = \begin{cases} f(xx') & \text{if } y = x',\ y' = x,\ \&\ xx' \in E(G) \\ g(y, y')/r & \text{if } y \in N(x) \setminus \{x'\} \ \&\ y' \in N(x') \setminus \{x\} \\ 0 & \text{otherwise.} \end{cases}$$

It is now straightforward to check that p is a valid correlation that wins the perfect matching game for G with probability 1, and that the marginals $p(y|x)$ are well-defined and equal to $f(xy)$ if $xy \in E(G)$ and equal to 0 otherwise. □

1.6.3 Undecidability of quantum perfect matching for hypergraphs

As we saw in section 1.3.4, the perfect matching game can be also played on hypergraphs. Unlike with graphs for which it remains open whether quantum perfect matching is decidable, for hypergraphs we get undecidability.

Theorem 1.6.11. *It is undecidable to decide if a hypergraph has a quantum perfect matching.*

Proof. From Theorem 1.6.4, we get that deciding quantum perfect matching for a hypergraph H is equivalent to deciding $\alpha_q(2L(H))$. A classical result in graph theory tell us that the set of line graphs of hypergraphs is equivalent to that of general graphs [37]. That is given a graph G there exists a hypergraph H such that $L(H) = G$. Therefore, deciding quantum perfect matching for hypergraphs is equivalent to deciding if a graph has a quantum independence number of $|V|$ which is undecidable [16]. □

Chapter 2: Games and Undecidability

This chapter is taken verbatim from our paper “Nonlocal Games, Compression Theorems, and the Arithmetical Hierarchy” [28]. All authors of this work contributed equally.

2.1 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 [13, 38]. As another example, the complexity-theoretic result $\mathsf{MIP}^* = \mathsf{RE}$ [14] (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 [39, 40].

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 $\mathscr{S} = (|\psi\rangle, A, B)$ in a game G is given by

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

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

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

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 $\{\widetilde{A}^x_a\}$ on $\mathcal{H}_A$ and $\{\widetilde{B}^y_b\}$ on $\mathcal{H}_B$ such that

$$\langle\psi|A^x_a\, B^y_b|\psi\rangle = \langle\widetilde{\psi}|\widetilde{A}^x_a \otimes \widetilde{B}^y_b|\widetilde{\psi}\rangle \ .$$

For a proof, see [41, 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

[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.

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 [41, 42].

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 [41]? 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 [39, 43, 42, 40]. 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.

Computability of nonlocal games. We now define computational problems associated with computing the value of nonlocal games. Fix $0 \leq \varepsilon < 1$ 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 [13], 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 [44, 45]. Thus the exact co-value problem is complete for coRE.

2. In [38], 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 [14], 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:

Theorem 2.1. *The problem of deciding whether $\omega_q(G) = 1$ for nonlocal games G is complete for Π_2.*

[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.

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 2.1, 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 [14]
$\omega_{co}(G) \pm \varepsilon$	Π_1 [13]	Π_1 (conjectured)

Figure 2.1: 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 2.1, 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 [44, 45, 46, 47]. 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:

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

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 2.1 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 2.8.

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 [15].

The main conceptual result of our paper is that all of the complexity statements about nonlocal games expressed in Figure 2.1 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 [13], 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) [38].

We then combine our gapless compression theorem with the gap-preserving one of [14] to obtain the Π_2-hardness of the exact q-value problem, establishing Theorem 2.1. 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 [48, 14], (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 [48, 14] are quite involved and rely on sophisticated results ranging from self-testing [49, 50] to the quantum soundness of the low-degree test [51, 26] to gap amplification methods [52]. 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 2.1.1 we give an overview of how compression of nonlocal games yields the complexity characterization shown in Figure 2.1. In Section 2.1.2 we give an overview of how our gapless compression theorem is proved. In Section 2.1.3 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.

2.1.1 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 $\texttt{Compress}$ 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 $\texttt{Compress}$ is a map from Turing machines to Turing machines. Importantly, the map $\texttt{Compress}$ 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 2.1.

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

Gapped compression for q-type strategies. The $\mathsf{MIP}^* = \mathsf{RE}$ result of [14] relies on the following *gap-preserving* (or *gapped* for short) compression procedure for q-type strategies (i.e. finite-dimensional strategies).

Theorem 2.2 (Gap-preserving compression, informally stated [14]). *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 2.2: 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 2.2 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 $\mathscr{G}$.

Where does the poly(n)-complexity assumption on $\mathscr{G}$ and the $O(\log n)$-complexity of $\mathscr{G}'$ con-

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

sequence of Theorem 2.2 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 $O(n^2) + O(1) + O(\log n) = \mathrm{poly}(n)$. 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 $\mathrm{poly}(n)$, 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 2.3 (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* $\mathrm{poly}(n)$*, 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 2.2, 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 2.3 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 [13, 38]. 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 2.6.3.

Combining gapped and gapless compression. The main application of our gapless compression theorem is to combine it with the gapped compression theorem of [14] to prove Theorem 2.1, 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 [14], 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 [14], 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 [14] 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 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 $\omega_q(G_{n+1})$:

$$\begin{aligned}
\omega_q(G_n) &= \frac{1}{2}\omega_q(G'_{n+1}) + \frac{1}{2}\omega_q(H_n) && \text{(Definition of the game } G_n\text{)} \\
&= \frac{1}{2}\omega_q(G'_{n+1}) + \frac{1}{2} && (S \text{ true} \Rightarrow \omega_q(H_n) = 1 \text{ for all } n) \\
&\geq \frac{1}{2}\Big(1 - \alpha\,(1 - \omega_q(G_{n+1}))\Big) + \frac{1}{2} && \text{(Theorem 2.3)} \\
&= 1 - \frac{\alpha}{2}\Big(1 - \omega_q(G_{n+1})\Big)
\end{aligned}$$

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 $1-\omega_q(G_n) \leq \Big(\frac{\alpha}{2}\Big)^k\Big(1 - \omega_q(G_{n+k})\Big)$ 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 2.3) 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 2.4 (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 [44, 45], or the procedure described by [53], can be used to implement M.

```
The verifier checks whether $\phi(x)$ is false for some $x \leq n$. If it is, then reject.
Compute the description of the nonlocal game $G_1$, the first game of the sequence $\mathscr{G}$.
Run $M$ on input $G_1$ for $n$ steps. If it halts, then accept.
Otherwise, compute $\mathscr{G}'$ by running $\texttt{GaplessCompress}_{co}$ on the description of $\mathscr{G}$.
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 2.4 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 2.4). 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 2.4 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 2.4, 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 2.4 in Section 2.1.2.

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 2.3?

In [54], 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 2.2). 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

[6] This trick of inserting the Turing machine M into the description of the game is also used by [14] to construct an explicit game whose commuting operator value differs from its quantum value.

quantum strategies.

We prove these equivalences in Section 2.6.5.

Relation to previous work The idea of using compression in order to obtain complexity lower bounds for nonlocal games was first due to Ji [17]. 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 [12], 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 [12] still only apply to games with three or more players, however. This is a fundamental limitation of the compression approach of [17, 12] 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 [48] and then further developed by [14] 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 simpli-

[7] View Section 2 of [48] for a more in-depth overview of the differences.

fied version of these techniques, which allows us to obtain our Π_2-hardness result for two-player games.

In [54], 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 [12] with the gapped compressed theorem of [14]. However as mentioned the requirement to have games with at least three players is intrinsic to the work of [17, 12]. Furthermore, all previous works only study the setting of finite-dimensional (i.e. q-type) strategies; ours is the first to study compression of games in the commuting operator setting.

2.1.2 Overview of the gapless compression theorem

We now provide an overview of the proof of Theorem 2.3, 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 [48] and developed further by [14]. 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* $G^{\text{intro}} = (\mathcal{X}^{\text{intro}}, \mathcal{A}^{\text{intro}}, D^{\text{intro}})$ where

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

$$\log |\mathcal{A}^{\text{intro}}| = \text{poly}(\log |\mathcal{A}|)$$

$$\text{Complexity of } D^{\text{intro}} = \text{poly}(\text{Complexity of } D) \ .$$

The Introspection game G^{intro} is equivalent to G in the sense that the value of $\omega_t(G^{\text{intro}}) = 1$ 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 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* [55]. What makes the search for a family of games QS_n more challenging is the additional requirement imposed by the property

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

To satisfy this requirement the Question Sampling can have at most $\mathrm{poly}(n)$ questions. So overall

[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.

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 2.3.2 we introduce a family of games called 2-out-of-n Magic Square and prove it is efficiently rigid.

Introspection first appeared in [48] 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 $\omega_q(G^{\text{intro}}) < 1/2$. 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* [50]. 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 [14].

- 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 [14] is based on the soundness of something called the *classical low-degree test* against entangled provers [26], 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 [50]. 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 [14] to the infinite dimensional setting, allowing us to get a gapless compression theorem for commuting operator strategies. As discussed earlier proving Theorem 2.4 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 [25]. 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 [56, 57, 52] but nothing is known yet in the context of commuting operator strategies (aside from the parallel repetition result of [21], 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 2.1.1.

2.1.3 The synchronous strategies framework

As mentioned, another goal of this paper is to present the proof of the gapless compression theorem (Theorem 2.3) 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 [14]. To that end, we express and prove all our results in the framework of *synchronous strategies*, a class of strategies first studied by [58]. 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

[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 $A, B \in \mathscr{A}$.

$\{M^x_a\}_{a \in \mathcal{A}}$ 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

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

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").

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 [58, 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 2.5 (Adapted from Theorem 3.2 of [59] and Theorem 3.6 of [60])**.** *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 2.5 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 $\omega_t^s(G) = 1$ and $\omega_t^s(G) < 1$ (resp. deciding between $\omega_t^s(G) = 1$ and $\omega_t^s(G) \leq 1/2$).

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.

2.2 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).

2.2.1 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 [61].

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* $\frac{1}{d}\operatorname{tr}(A)$. Thus in this case the τ-norm is the normalized Frobenius norm.

Proposition 2.6. *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 2.7. *Let $A, B \in \mathscr{A}$. Then $\|AB\|_\tau \leq \|A\| \cdot \|B\|_\tau$.*

Proof.

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

□

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

Proof. By Proposition 2.7

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

We also have

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

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

In applications of Proposition 2.8 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 2.9. *Let U be any unitary. If $|\tau(1 - U)| \leq \varepsilon$, then $\|1 - U\|_\tau \leq \sqrt{2\varepsilon}$*

Proof.

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

□

2.2.2 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 2.10. *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 $\mathcal{A}$.

2.2.3 Utility lemmas about measurements

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

Lemma 2.11 (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*

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

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

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

□

Lemma 2.12 (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.

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

□

Lemma 2.13 (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 2.14 (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 2.15 (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 2.16. *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 $R_b M_a \approx_\delta R_b N_a$:

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

where in the first inequality we used the assumption that $\sum_b R_b^* R_b \leq 1$. 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 [62], improved quantitatively in [26], and recently extended to the setting of von Neumann algebras by de la Salle [63].

Lemma 2.17 (Projectivization of POVMs [63])**.** *Let $\{M_a\} \subset \mathscr{A}$ be a POVM with outcomes indexed by a finite set $\mathcal{A}$. Suppose that the following holds:*

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

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 2.18 (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 2.18 in Section 2.7.

2.2.4 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 $\{M^x_a\}_{x,a}$. The *value* of a tracial strategy $\mathscr{S}$ in G is defined as

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

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., $M^x_a M^y_b = M^y_b M^x_a$ for all $a, b \in \mathcal{A}$.

The *synchronous commuting operator value* of a synchronous game G, denoted by $\omega^s_{co}(G)$, 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 $\omega^s_q(G)$, 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 2.5) requires games to have oracularizable strategies. "Oracularizability" is an invariant maintained by our compression procedure (as well as the compression procedures of [48, 14]).

Definition 2.19 (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 2.20 (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 [14], 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.

2.2.5 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 2.21 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 2.13 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 2.8, we get

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

With another application of Theorem 2.8, 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 2.8 and the triangle inequality, we get the desired result

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

2.3 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 [64], 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 $|\mathrm{EPR}\rangle = (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)/\sqrt{2}$, 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 $\mathcal{H}_A, \mathcal{H}_B$ 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 [65] for a survey of self-testing and its applications.

[10] A standard result in the theory of nonlocal games is that any finite-dimensional strategy can be expressed as a tensor-product strategy [41, Theorem 1].

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 $\{A_a^x\}$ and $\{B_b^y\}$ respectively that achieves value $\omega_{co}(CHSH)$ in the CHSH game must generate *anti-commuting observables*: defining the self-adjoint unitary operators $U^0 = A_0^0 - A_1^0$ and $U^1 = A_0^1 - A_1^1$, 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.

2.3.1 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) [18, 19, 66]. Rigidity of Magic Square is first proved in [67]. 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

$$\mathcal{X}_{\text{eqs}} = \{r_1, r_2, r_3, c_1, c_2, c_3\},$$

$$\mathcal{X}_{\text{vars}} = \{s_{11}, s_{12}, s_{13}, s_{21}, s_{22}, s_{23}, s_{31}, s_{32}, s_{33}\}.$$

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 2.1: 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 2.2 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 2.2: 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

$$\begin{aligned}(O^{11}\ O^{22})^2 &= (O^{12}\ O^{13})(O^{23}\ O^{21})(O^{21}\ O^{31})(O^{32}\ O^{12}) \\ &= O^{12}(O^{13}\ O^{23})(O^{21}\ O^{21})(O^{31}\ O^{32})O^{12} \\ &= -O^{12}\ O^{33}\ O^{33}\ O^{12} = -1. \end{aligned} \tag{2.3.1}$$

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 $\mathcal{O} = \{O^{ij}\}$ of observables satisfying relations **R1**, **R2**, and **R3**, we can define the synchronous strategy $\mathscr{S} = (\tau, \{M^x\})$ 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 $M^{s_{ij}}_b$ to be the projection onto the eigenspace of O^{ij} with eigenvalue $(-1)^b$. To aid notation we abbreviate $M^{s_{ij}}_b$ as M^{ij}_b. The operator M^e_a corresponding to a constraint question $e \in \mathcal{X}_{\text{eqs}}$ is the product

$$\prod_{s_{ij}\in e} M^{ij}_{a(s_{ij})} \tag{2.3.2}$$

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

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

for every $b_1, b_2 \in \{0, 1\}$. So the order of the product in Equation (2.3.2) doesn't matter, and thus M^e_a 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 $\mathscr{S}$ is a projective strategy. Indeed conditioned on receiving question pair (s_{ij}, s_{ij}), the probability of winning is

$$\tau(M^{ij}_0\ M^{ij}_0) + \tau(M^{ij}_1\ M^{ij}_1) = \tau(M^{ij}_0 + M^{ij}_1) = \tau(1) = 1.$$

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

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

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

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

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 $\omega(\text{MS}, \mathcal{S}) = 1$. 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 2.2, 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 $\mathcal{S} = (\tau, \{M^x\})$ denote a synchronous strategy for the Magic Square game. Each $\{M^{ij}_b\}_{b\in\mathcal{A}_{\text{MS}}}$ is a projective measurement with outcomes $b \in \mathcal{A}_{\text{MS}}$. 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.,

$$M_0^{ij} + M_1^{ij} = 1 \ . \tag{2.3.3}$$

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. (2.3.3)) 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 2.21 (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 (2.3.1), 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 2.1, 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

$$\sum_{a \in \mathcal{A}_{r_i}} \mathrm{TR}\left(R^i_a \, M^{ij}_{a(s_{ij})}\right) \geq 1 - |\mathcal{X}_{\mathrm{MS}}|^2 \varepsilon \; . \tag{2.3.4}$$

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 $\{R^{ij}_b\}_{b \in \{0,1\}}$ forms a projective measurement. We can similarly define, for all columns j and variables s_{ij}, projective measurement $\{C^{ji}_b\}$ consisting of operators

$$C^{ji}_b = \sum_{a \in \mathcal{A}_{c_j} : \; a(s_{ij}) = b} C^j_a .$$

We can rewrite (2.3.4) in terms of projective measurements $\{R^{ij}_b\}_{b\in\{0,1\}}$ as follows

$$1 - |\mathcal{X}_{\mathrm{MS}}|^2\varepsilon \leq \sum_{a\in\mathcal{A}_{r_i}} \mathrm{TR}\left(R^i_a\, M^{ij}_{a(s_{ij})}\right) = \sum_{b\in\mathcal{A}_{\mathrm{vars}}} \sum_{\substack{a\in\mathcal{A}_{r_i}:\\ a(s_{ij})=b}} \mathrm{TR}\left(R^i_a\, M^{ij}_b\right) = \sum_{b\in\mathcal{A}_{\mathrm{vars}}} \mathrm{TR}\left(R^{ij}_b\, M^{ij}_b\right).$$

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

$$R^{ij}_b \simeq_{|\mathcal{X}_{\mathrm{MS}}|^2\varepsilon} M^{ij}_b \ ,$$

where the answer set is $\mathcal{A}_{\mathrm{vars}} = \{0, 1\}$. By Theorem 2.13, we convert consistency to closeness to obtain

$$R^{ij}_b \approx_{|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} M^{ij}_b \ ,$$

and with a similar argument for columns we get that

$$C^{ji}_b \approx_{|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} M^{ij}_b \ .$$

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

$$R^{ij} = R^{ij}_0 - R^{ij}_1 \qquad \text{and} \qquad C^{ji} = C^{ji}_0 - C^{ji}_1 \ .$$

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

$$O^{ij} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} R^{ij}\ , \tag{2.3.5}$$

$$O^{ij} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} C^{ji}. \tag{2.3.6}$$

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

$$\begin{aligned} \|O^{ij}\,O^{ik} - O^{ik}\,O^{ij}\|_\tau^2 &\leq 2\|O^{ij}\,O^{ik} - R^{ij}\,R^{ik}\|_\tau^2 + 2\|R^{ij}\,R^{ik} - R^{ik}\,R^{ij}\|_\tau^2 + 2\|R^{ik}\,R^{ij} - O^{ik}\,O^{ij}\|_\tau^2 \\ &= 2\|O^{ij}\,O^{ik} - R^{ij}\,R^{ik}\|_\tau^2 + 2\|R^{ik}\,R^{ij} - O^{ik}\,O^{ij}\|_\tau^2\ . \end{aligned} \tag{2.3.7}$$

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 2.8, from (2.3.5), we get that $O^{ij}O^{ik} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} R^{ij}O^{ik}$. Again by Theorem 2.8, from (2.3.5), 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 (2.3.7) 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

$$O^{ij}\, O^{ik} \approx_{4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} O^{ik}\, O^{ij}\ , \tag{2.3.8}$$

$$O^{ji}\, O^{ki} \approx_{4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} O^{ki}\, O^{ji}\ , \tag{2.3.9}$$

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

As mentioned in Section 2.2.5, 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 2.8, 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 $1 - |\mathcal{X}_{\text{MS}}|^2\varepsilon$. By winning conditions in Table 2.1, 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

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

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

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

and in terms of observables this can be equivalently written as

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

By Theorem 2.9, we get that

$$R^{i1}\,R^{i2}\,R^{i3} \approx_{2|\mathcal{X}_{\mathrm{MS}}|\sqrt{\varepsilon}} 1 \quad \text{for } i = 1, 2, 3\ . \tag{2.3.10}$$

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 (2.3.5) and (2.3.10), and repeated applications of Theorem 2.8 and the triangle inequality, for every $i \in [3]$, we obtain

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

Therefore we have

$$O^{i1}\,O^{i2}\,O^{i3} \approx_{4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} 1 \quad \text{for } i = 1, 2, 3, \tag{2.3.11}$$

and following the same argument for columns

$$O^{1j}\,O^{2j}\,O^{3j} \approx_{4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} 1 \quad \text{for } j = 1, 2, \tag{2.3.12}$$

$$O^{13}\,O^{23}\,O^{33} \approx_{4|\mathcal{X}_{\mathrm{MS}}|\sqrt{2\varepsilon}} -1\ . \tag{2.3.13}$$

Finally to prove the approximate anticommutation $O^{11}\ O^{22} \approx -O^{22}O^{11}$, we follow the idea in the derivation 2.3.1: We start with $(O^{11}\ O^{22})^2$ and step by step, using relations (2.3.11)-(2.3.13), substitute O^{11} and O^{22} by unitaries that are nearby. By repeated applications of triangle inequality and Theorem 2.8 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

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

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

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

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 2.22. *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 [68], 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

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

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 2.8, we get that

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

By Theorem 2.8 again, we obtain that $\tau(M_s - M_s^2) \leq \delta(\varepsilon)$ for every s. So by Theorem 2.17, 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

$$B^{(i)}\, \Pi_0^{(i)}\, B^{(i)} \approx_{\delta(\varepsilon)} \Pi_1^{(i)}. \tag{2.3.14}$$

Now if we define unitary operators $U_{s,t} \coloneqq \prod_{i=1}^{n} (B^{(i)})^{s_i+t_i}$, 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 (2.3.14) 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 [69] and Natarajan and Vidick [50] showed that there exist families of games $\{G_n\}$ where the n-th game G_n certifies a 2^n-dimensional space using poly(n) question/answer pairs. The rigidity result of [50] 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 [14].[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 [69], which we call 2-out-of-n CHSH. We describe the 2-out-of-n Magic Square games next.

2.3.2 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 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 2.2: The nontrivial question pairs and winning conditions for the 2-OF-n-MS.

[11] In fact, the result of [14] 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!

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 $\mathscr{S}_{\text{MS}} = (\tau, \{M^x\})$, 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 $\mathscr{S}_{2\text{-OF-}n\text{-MS}} = (\tau^{\otimes n}, \{M^{i,j,x,y}\})$, where $M^{i,j,x,y} = \{M^{i,j,x,y}_{a,b}\}_{a,b \in \mathcal{A}_{\text{MS}}}$ is the projective measurement defined such that

$$M^{i,j,x,y}_{a,b} := 1 \otimes \cdots \otimes 1 \otimes M^x_a \otimes 1 \otimes \cdots \otimes 1 \otimes M^y_b \otimes 1 \otimes \cdots \otimes 1 \in \mathscr{A}^{\otimes n}$$

in which M^x_a and M^y_b 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 $\{M^{i,j,x,y}_{a,b}\}_{a,b \in \mathcal{A}_{\text{MS}}}$ 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 2.23 (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 $1 - |\mathcal{X}_{2\text{-OF-}n\text{-MS}}|^2\varepsilon$, thus

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

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

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

Therefore by Theorem 2.21, 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

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

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

Using Theorem 2.13 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 2.8, 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 2.22 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 $(1-\mathrm{poly}(n)\mathrm{poly}(\delta))2^{2n}$, which is nontrivial for $\delta < 1/\mathrm{poly}(n)$. Furthermore, this game is highly efficient because the number of questions and answers grows only *polynomially* with n. Observe that

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

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.

2.3.3 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 2.2, the observables $A^{(1)}, \ldots, A^{(2n)}, B^{(1)}, \ldots, B^{(2n)}$, defined in Theorem 2.23, 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 2.4, 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 2.23) 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 $A^{(1)}, \ldots, A^{(n)}$ (resp. $A^{(n+1)}, \ldots, A^{(2n)}$) to produce an n-bit string answer.

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

Here, "approximate consistency" is used in the sense defined in Section 2.2.2. 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 2.24.

We now formally define the game $\mathrm{QS}_n = (\mathcal{Q}_n, \mathcal{X}_n, D_{\mathrm{QS}_n})$. Its question set is defined to be $\mathcal{Q}_n = \mathcal{X}_{2\text{-OF-}n\text{-MS}} \cup \{S_A, S_B, E_A, E_B\}$, and thus $|\mathcal{Q}_n| = \mathrm{poly}(n)$. 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 $\mathcal{Q}$ (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-$\textsc{of}$-n-MS	$D_{\text{2-}\textsc{of}\text{-}n\text{-MS}}(q, r, x, y) = 1$
$q = (i, j, s_{11}, .) \in \mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}$ where $i \leq \frac{n}{2}, j > \frac{n}{2}$, and $r = S_A$	$x = (a_i, a_j) \in \mathcal{A}^2_{\mathrm{MS}}, y \in \{0,1\}^n$, and $y_{2i-1} = a_i$
$q = (i, j, s_{12}, .) \in \mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}$ where $i \leq \frac{n}{2}, j > \frac{n}{2}$, and $r = S_A$	$x = (a_i, a_j) \in \mathcal{A}^2_{\mathrm{MS}}, y \in \{0,1\}^n$, and $y_{2i} = a_i$
$q = (i, j, s_{11}, .) \in \mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}$ where $i > \frac{n}{2}, j \leq \frac{n}{2}$, and $r = S_B$	$x = (a_i, a_j) \in \mathcal{A}^2_{\mathrm{MS}}, y \in \{0,1\}^n$, and $y_{2(i-\frac{n}{2})-1} = a_i$
$q = (i, j, s_{12}, .) \in \mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}$ where $i > \frac{n}{2}, j \leq \frac{n}{2}$, and $r = S_B$	$x = (a_i, a_j) \in \mathcal{A}^2_{\mathrm{MS}}, y \in \{0,1\}^n$, and $y_{2(i-\frac{n}{2})} = a_i$
$q = (i, j, s_{22}, .) \in \mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}$ where $i \leq \frac{n}{2}, j > \frac{n}{2}$, and $r = E_A$	$x = (a_i, a_j) \in \mathcal{A}^2_{\mathrm{MS}}, y \in \{0,1\}^n$, and $y_{2i-1} = a_i$
$q = (i, j, s_{21}, .) \in \mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}$ where $i \leq \frac{n}{2}, j > \frac{n}{2}$, and $r = E_A$	$x = (a_i, a_j) \in \mathcal{A}^2_{\mathrm{MS}}, y \in \{0,1\}^n$, and $y_{2i} = a_i$
$q = (i, j, s_{22}, .) \in \mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}$ where $i > \frac{n}{2}, j \leq \frac{n}{2}$, and $r = E_B$	$x = (a_i, a_j) \in \mathcal{A}^2_{\mathrm{MS}}, y \in \{0,1\}^n$, and $y_{2(i-\frac{n}{2})-1} = a_i$
$q = (i, j, s_{21}, .) \in \mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}$ where $i > \frac{n}{2}, j \leq \frac{n}{2}$, and $r = E_B$	$x = (a_i, a_j) \in \mathcal{A}^2_{\mathrm{MS}}, y \in \{0,1\}^n$, and $y_{2(i-\frac{n}{2})} = a_i$

Table 2.3: The nontrivial question pairs and winning conditions for the n-th Question Sampling game. We used dot for example in $(i, j, s_{11}, .) \in \mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}$ to indicate that the fourth coordinate does not matter as long as the quadruple is a valid question in $\mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}$.

We now to describe an oracularizable synchronous strategy for QS_n with value 1. Let $\mathcal{S}_{\mathrm{MS}} = (\tau, \{M^q\}_{q \in \mathcal{X}_{\mathrm{MS}}})$ be the honest strategy for the Magic Square game on the Hilbert space $\mathcal{H}_{\mathrm{MS}} = \mathbb{C}^4$ and let $\mathcal{S}_{\text{2-}\textsc{of}\text{-}n\text{-MS}} = (\tau^{\otimes n}, \{M^q\}_{q \in \mathcal{X}_{\text{2-}\textsc{of}\text{-}n\text{-MS}}})$ be its extension to a perfect oracularizable synchronous strategy for the 2-$\textsc{of}$-n-MS as defined in Section 2.3.2. We extend this to a perfect finite-dimensional oracularizable synchronous strategy $\mathcal{S}_{\mathrm{QS}_n}$ for QS_n.

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

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

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 $\{M_y^{S_A}\}, \{M_y^{S_B}\}, \{M_y^{E_A}\}, \{M_y^{E_B}\}$ 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 2.3, the probability of winning is

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

[12] If we take the Magic Square strategy from Figure 2.2, these formulas simplify to

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

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

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 convenience we use the notational shorthand

$$S^A_x = M^{S_A}_x \qquad \text{and} \qquad S^B_x = M^{S_B}_x$$

$$E^A_x = M^{E_A}_x \qquad \text{and} \qquad E^B_x = M^{E_B}_x$$

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

$$O_u^{S_A} = \sum_{x \in \{0,1\}^n} (-1)^{u \cdot x} S_x^A \qquad \text{and} \qquad O_u^{S_B} = \sum_{x \in \{0,1\}^n} (-1)^{u \cdot x} S_x^B$$

$$O_u^{E_A} = \sum_{x \in \{0,1\}^n} (-1)^{u \cdot x} E_x^A \qquad \text{and} \qquad O_u^{E_B} = \sum_{x \in \{0,1\}^n} (-1)^{u \cdot x} E_x^B \; .$$

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 2.24 (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 2.2.5. For a detailed example see the proof of Theorem 2.21.

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

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

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

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

Using Theorem 2.13 we can write this as closeness relation

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

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 2.8, 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

$$\begin{aligned} S^B_x &\approx \prod_{i=1}^{n/2} M^{i+n/2,s_{11}}_{x_{2i-1}} M^{i+n/2,s_{12}}_{x_{2i}} \ , \\ E^A_x &\approx \prod_{i=1}^{n/2} M^{i,s_{22}}_{x_{2i-1}} M^{i,s_{21}}_{x_{2i}} \ , \\ E^B_x &\approx \prod_{i=1}^{n/2} M^{i+n/2,s_{22}}_{x_{2i-1}} M^{i+n/2,s_{21}}_{x_{2i}} \ . \end{aligned}$$

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

$$
\begin{aligned}
O_u^{S_A} &\approx (A^{(1)})^{u_1}(A^{(2)})^{u_2}\cdots(A^{(n)})^{u_n}\ ,\\
O_u^{S_A} &\approx (A^{(n/2+1)})^{u_1}(A^{(n/2+2)})^{u_2}\cdots(A^{(n)})^{u_n}\ ,\\
O_u^{E_A} &\approx (B^{(1)})^{u_1}(B^{(2)})^{u_2}\cdots(B^{(n)})^{u_n}\ ,\\
O_u^{E_A} &\approx (B^{(n/2+1)})^{u_1}(B^{(n/2+2)})^{u_2}\cdots(B^{(n)})^{u_n}\ ,
\end{aligned}
$$

where $A^{(i)}$ and $B^{(j)}$ are as defined in Theorem 2.23. Properties 1-3 now follow easily from the rigidity of 2-OF-n-MS in Theorem 2.23.

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 2.8, 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 2.8 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 2.25 (Entanglement bound for Question Sampling)**.** *Let $\mathscr{S} = (\tau, \{M^q\}_{q \in Q_n})$ be a synchronous strategy for* QS_n *over a von Neumann algebra $\mathscr{A} \subset B(\mathcal{H})$. If $\omega(\mathrm{QS}_n, \mathscr{S}) \geq 1 - \varepsilon$ 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 2.23 and Theorem 2.22. 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 $0 \preceq S_{0^n}^A (1 - S_{0^n}^B) S_{0^n}^A \preceq 1 - M$ 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 2.17 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 2.8 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 2.26. *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 [68]. 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 $\widehat{\mathscr{A}} \subset \mathscr{A}$. □

2.4 Question Reduction

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

Theorem 2.27 (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 $\beta = \mathrm{poly}(\alpha) \in \mathbb{N}$ and $n_0^{\text{intro}} = \mathrm{poly}(\beta, n_0) \in \mathbb{N}$ 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 [48, 14]. 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 2.4.5 we prove Theorem 2.27.

2.4.1 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 2.3.3, 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 2.24.

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.

2.4.2 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

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

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 2.4. 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	$D_{\mathrm{QS}_\ell}(q, r, \widehat{a}, \widehat{b}) = 1$
$q = I$	$\Big((x_A, x_B)$ is trivial for $G\Big)$ or $\Big(z = x_W \wedge c = a_W \wedge D(x_A, x_B, a_A, a_B) = 1\Big)$
$r = I_W$	where $\widehat{a} = (x_A, a_A, x_B, a_B) \in (\mathcal{X} \times \mathcal{A})^2$ and $\widehat{b} = (z, c) \in \mathcal{X} \times \mathcal{A}$
$q = I_W$	$z = x_W \wedge c = a_W$
$r = I_W S_{\overline{W}}$	where $\widehat{a} = (x_W, a_W) \in \mathcal{X} \times \mathcal{A}$ and $\widehat{b} = (z, c, x_{\overline{W}}) \in \mathcal{X} \times \mathcal{A} \times \mathcal{X}$
$q = I_W$	$z = x_W$
$r = S_W$	where $\widehat{a} = (x_W, a_W) \in \mathcal{X} \times \mathcal{A}$ and $\widehat{b} = z \in \mathcal{X}$
$q = I_W$	$z = x_W \wedge c = a_W$
$r = I_W E_{\overline{W}}$	where $\widehat{a} = (x_W, a_W) \in \mathcal{X} \times \mathcal{A}$ and $\widehat{b} = (z, c, x_{\overline{W}}) \in \mathcal{X} \times \mathcal{A} \times \mathcal{X}$
$q = I_W E_{\overline{W}}$	$z = x_{\overline{W}}$
$r = E_{\overline{W}}$	where $\widehat{a} = (x_W, a_W, x_{\overline{W}}) \in \mathcal{X} \times \mathcal{A} \times \mathcal{X}$ and $\widehat{b} = z \in \mathcal{X}$
$q = I_W S_{\overline{W}}$	$z = x_{\overline{W}}$
$r = S_{\overline{W}}$	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 2.4: 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 2.3. 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

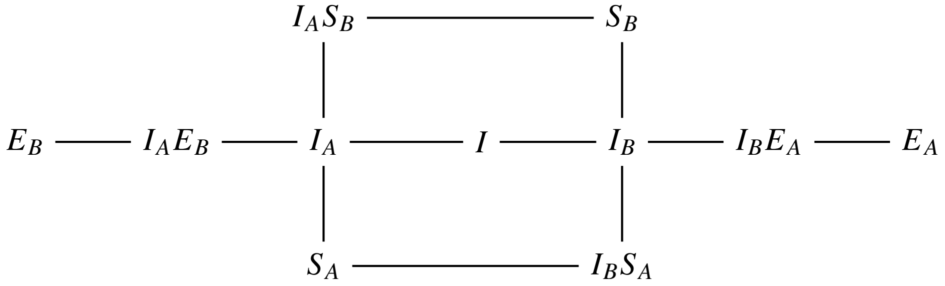

Figure 2.3: A node indicates a special question in G^{intro}. A pair of questions are connected with an edge if the pair is a nontrivial question pair as defined in Section 2.2.4. There should also be loops on every node (which we omitted here for clarity).

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

2.4.3 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 2.28 (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 2.19).

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 2.3.3. 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 2.24), 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

$$P^{I_W S_{\overline{W}}}_{x,a,y} = P^{I_W}_{x,a} \; S^{\overline{W}}_y = S^{\overline{W}}_y \; P^{I_W}_{x,a} \qquad \text{and} \qquad P^{I_W E_{\overline{W}}}_{x,a,y} = P^{I_W}_{x,a} \; E^{\overline{W}}_y = E^{\overline{W}}_y \; P^{I_W}_{x,a} \, . \tag{2.4.1}$$

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

$$P^I_{x,a,y,b} \coloneqq S^A_x \; S^B_y \otimes N^x_a \; N^y_b.$$

Since N^x_a and N^y_b 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

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

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 $\mathscr{S}^{\text{intro}}$ is finite-dimensional when $\mathscr{S}$ is finite-dimensional. Next we show that $\mathscr{S}^{\text{intro}}$ 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 $(q, r) \in \mathcal{Q}_{\mathrm{QS}_\ell}$. Since $\mathscr{S}_{\mathrm{QS}_\ell}$ 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 $\mathscr{S}_{\mathrm{QS}_\ell}$ succeeds with probability 1 in the game QS_ℓ and thus succeeds with probability 1 in G^{intro} conditioned on questions from $\mathcal{Q}_{\mathrm{QS}_\ell}$.

It remains to check the commutativity property and success probability for all question pairs that are connected via an edge in Figure 2.3. 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

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

where in the first equality we used (2.4.1).

$\underline{(I_W, I_W E_{\overline{W}})}$: 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 (2.4.1), 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 (2.4.1) 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 $\mathcal{S}^{\text{intro}}$ conditioned on players receiving question pair (I, I_A) is

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

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 $\mathcal{S}^{\text{intro}}$, except when they receive question pair (I, I_A) or (I, I_B) in which case they win with probability $\omega(G, \mathcal{S})$. From this we conclude that $\omega(G^{\text{intro}}, \mathcal{S}^{\text{intro}}) \geq \omega(G, \mathcal{S})$. □

2.4.4 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 2.29 (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 2.29 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 2.2.5 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

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

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

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 $\mathscr{S}^{\text{intro}} = (\rho, \{P^q\}_{q \in Q^{\text{intro}}})$ be a fixed synchronous strategy for G^{intro} with value $1 - \varepsilon$.

Lemma 2.30. *The following approximate relations hold*

$$\begin{aligned}
I^W_x &\approx S^W_x \\
I^W_{x,a} S^W_y &\approx S^W_y I^W_{x,a} \\
I^W_{x,a} S^{\overline{W}}_y &\approx S^{\overline{W}}_y I^W_{x,a} \\
I^W_{x,a} E^{\overline{W}}_y &\approx E^{\overline{W}}_y I^W_{x,a} \\
I^W_{x,a} O^{\overline{W}}_u &\approx O^{\overline{W}}_u I^W_{x,a}.
\end{aligned}$$

Proof. As mentioned in Section 2.2.5, when we write $I^W_x \approx S^W_x$ we mean $I^W_x \approx_{\delta(\varepsilon)} S^W_x$ 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 2.13, we get that $I^W_x \approx S^W_x$. By Proposition 2.8, 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 2.31. *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 2.13. 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 2.24 and Theorem 2.8, 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

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

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 2.30, we obtain

$$\sum_a \rho(I_{x,a,y,\cdot}(S^B_y\ I^A_{x,a}\ S^B_y)) \approx \sum_a \rho(I_{x,a,y,\cdot}(I_y\ I^A_{x,a}\ I_y)) = \sum_a \rho(I_{x,a,y,\cdot}\ I^A_{x,a}) \approx 2^{-2\ell}. \tag{2.4.2}$$

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

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

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 (2.4.2) 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 2.29. 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 2.30, 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 2.31 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 2.30 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 2.29. 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 2.26.

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

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

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

$$\widetilde{W}^x_\perp \coloneqq 1 - \sum_{a \in \mathcal{A}} \widetilde{W}^x_a \; .$$

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

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

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

These are clearly positive semidefinite operators and

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

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

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

$$\rho(\widehat{A}_a^x \ \widehat{B}_b^y) \approx \rho(I_{x,a}^A \ I_{y,b}^B). \tag{2.4.3}$$

We achieve this by repeatedly applying Theorem 2.8. First recall from Theorem 2.25 that $\Pi \approx S_0^A S_0^B$. Here we use 0 as a shorthand notation for 0^ℓ. So we have

$$\begin{aligned}\rho(\widehat{A}_a^x \ \widehat{B}_b^y) &= \rho(\Pi \ \widetilde{A}_a^x \ \Pi \ \widetilde{B}_b^y \ \Pi) \\ &\approx \rho(S_0^A \ \widetilde{A}_a^x \ S_0^A \ S_0^B \ \widetilde{B}_b^y \ S_0^B),\end{aligned}$$

where we used Theorem 2.24 which states that S_0^A and S_0^B 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 2.24 which states that $S_0^W \ O_x^W \approx O_x^W \ S_x^W$. By Theorem 2.30

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 2.30 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 (2.4.3).

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 $a, b \in \mathcal{A}$

$$\widehat{W}_a^x \widehat{W}_b^x \approx \widehat{W}_a^x \mathbf{1}_{a=b} \tag{2.4.4}$$

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

$$\widehat{W}_a^x \widehat{W}_b^x = \Pi \; O_x^W \; I_{x,a}^W \; O_x^W \; \Pi \; O_x^W \; I_{x,b}^W \; O_x^W \; \Pi$$

$$\approx \Pi \; O_x^W \; I_{x,a}^W \; O_x^W (S_0^{\overline{W}} \; S_0^W \; S_0^{\overline{W}}) O_x^W \; I_{x,b}^W \; O_x^W \; \Pi$$

where in the last line we used the fact that $\Pi \approx S_0^{\overline{W}} \; S_0^W \; S_0^{\overline{W}}$ by Theorem 2.25. Now sampling projections $S^{\overline{W}}$ commute with erasure observables O^W and Introspection projections I^W so

$$\Pi \; O_x^W \; I_{x,a}^W \; O_x^W (S_0^{\overline{W}} \; S_0^W \; S_0^{\overline{W}}) O_x^W \; I_{x,b}^W \; O_x^W \; \Pi \approx \Pi \; S_0^{\overline{W}} \; O_x^W \; I_{x,a}^W \; O_x^W \; S_0^W \; O_x^W \; I_{x,b}^W \; O_x^W \; S_0^{\overline{W}} \; \Pi$$

$$\approx \Pi \; O_x^W \; I_{x,a}^W \; O_x^W \; S_0^W \; O_x^W \; I_{x,b}^W \; O_x^W \; \Pi$$

where in the last line we use the fact that $\Pi \approx S_0^{\overline{W}} \; S_0^W \; S_0^{\overline{W}}$, and hence $\Pi \; S_0^{\overline{W}} \approx \Pi \approx S_0^{\overline{W}} \; \Pi$. Now moving S_0^W passed O_x^W using the relation $O_x^W \; S_0^W \approx S_x^W \; O_x^W$, and then using the fact that $(O_x^W)^2 = I$ (as O_x^W is an observable), we get

$$\Pi \; O_x^W \; I_{x,a}^W \; O_x^W \; S_0^W \; O_x^W \; I_{x,b}^W \; O_x^W \; \Pi \approx \Pi \; O_x^W \; I_{x,a}^W \; S_x^W \; (O_x^W)^2 \; I_{x,b}^W \; O_x^W \; \Pi$$

$$= \Pi \; O_x^W \; I_{x,a}^W \; S_x^W \; I_{x,b}^W \; O_x^W \; \Pi$$

Now substituting I_x^W in place of S_x^W we get

$$\Pi \; O_x^W \; I_{x,a}^W \; S_x^W \; I_{x,b}^W \; O_x^W \; \Pi \approx \Pi \; O_x^W \; I_{x,a}^W \; I_x^W \; I_{x,b}^W \; O_x^W \; \Pi$$

$$\approx \; \Pi \; O_x^W \; I_{x,a}^W \; I_{x,b}^W \; O_x^W \; \Pi$$

$$= \widehat{W}_a^x \; \delta_{a,b},$$

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 (2.4.4). 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 2.8, this in turn implies that

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

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

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

So far we established that $\widehat{W}^x_a$, as operators in $\widehat{\mathscr{A}}$ acting on $\widehat{\mathcal{H}}$, are close to projections. So applying Theorem 2.17, for every $W \in \{A, B\}$ and $x \in \mathcal{X}$, there exists a projective measurement $\{W^x_a\}_a \subset \widehat{\mathscr{A}}$ that is close to $\{\widehat{W}^x_a\}_a$.

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 $\{A^x_a\}_a$ and $\{B^y_b\}_b$ to the original measurements $I^A_{x,a}$ and $I^B_{y,b}$. For every $x, y \in \mathcal{X}, a, b \in \mathcal{A}$, we can write

$$\sigma(A^x_a B^y_b) \approx \sigma(\widehat{A}^x_a \widehat{B}^y_b) = \frac{\rho(\widehat{A}^x_a \widehat{B}^y_b)}{\rho(\Pi)} \approx \frac{\rho(\widehat{A}^x_a \widehat{B}^y_b)}{2^{-2\ell}} \approx \frac{\rho(I^A_{x,a} I^B_{y,b})}{2^{-2\ell}}.$$

From this and Theorem 2.31, 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 2.31, 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

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

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

$$\sum_{x,y} \frac{1}{2^{2\ell}} \sum_{a,b\in\mathcal{A}} D(x,y,a,b)\sigma(A^x_a\ B^y_b) = 1 - \delta(\varepsilon). \tag{2.4.5}$$

To summarize, at a high level, we constructed a set of operators A^x_a and B^y_b 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 (2.4.5), 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 2.13, 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 (2.4.5) we conclude that

$$\sum_{x,y\in\mathcal{X}} \frac{1}{2^{2\ell}} \sum_{a,b\in\mathcal{A}} D(x,y,a,b)\sigma(A_a^x\ A_b^y) = 1 - \delta(\varepsilon). \tag{2.4.6}$$

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 (2.4.6), 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 2.25, 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 2.26 which is a subspace of $\mathcal{H}$.

□

2.4.5 Proof of Theorem 2.27

From Theorem 2.20, 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 2.20, 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 2.4.2. 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

$$S_A, E_A, I_A, I_A S_B, I_A E_B, S_B, E_B, I_B, I_B S_A, I_B E_A,$$

then the pair is nontrivial if they are connected by an edge or a self-loop in Figure 2.3. 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 $\text{poly}(\alpha, \log n)$ (see Table 2.3).

Next we bound the complexity of $D^{\text{intro}}(n)$. The bit length of questions in the Introspection game G_n^{intro} is $\text{poly}(\alpha, \log n)$. 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 $\text{poly}(n^\alpha)$ whether the answer format of G_n^{intro} is respected. The decider, by simulating $D(n)$ and $C(n)$, can compute in time $\text{poly}(|D|, |C|, \alpha, n^\alpha)$ whether a give quadruple $(q, r, \widehat{a}, \widehat{b})$ is an accepting quadruple in G_n^{intro} according to Table 2.4.

The completeness, soundness, and the dimension bound follow immediately from Propositions 2.28 and 2.29.

2.5 Answer Reduction

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

Theorem 2.32 (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 $n \geq n_0$,*

$$\textit{The questions of } G_n \textit{ have length at most } \log^\beta(n),$$
$$\mathsf{TIME}_C(n) = \log^\beta n\ , \textit{ and}$$
$$\mathsf{TIME}_D(n) \leq n^\beta$$

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. $Q(n) \leq \text{poly}(\log T(n))$), 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 $\text{poly}(\log T(n))$ and in particular both the question and answer lengths of G_n^{ans} are at most $\text{poly}(\log T(n))$.

We describe and analyze the answer reduction transformation $G \mapsto G^{\text{ans}}$ for a single game (rather than a sequence), and then prove Theorem 2.32 in Section 2.5.5.

2.5.1 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 $G^{\mathrm{ans}} = (\mathcal{X}^{\mathrm{ans}}, \mathcal{A}^{\mathrm{ans}}, D^{\mathrm{ans}})$. 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 [70, 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 2.33 (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 $L = \text{poly}(|D_{x,y}|, T) = \text{poly}(|D|, Q, T)$. Here we used that the description length $|D_{x,y}| = O(|D| + |x| + |y|) = \text{poly}(|D|, Q)$.

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

$$\mathcal{X}^{\text{ans}} = \mathcal{X}^{\text{orac}} \times ([L] \cup [L]^2 \cup [L]^3) \qquad\qquad \mathcal{A}^{\text{ans}} = \{0, 1\} \cup \{0, 1\}^2 \cup \{0, 1\}^3$$

where $\mathcal{X}^{\text{orac}} = \mathcal{X} \cup \mathcal{X}^2$ 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.

2.5.2 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 2.5. 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 2.5: The nontrivial question pairs and winning conditions for the game G^{ans}.

Table 2.5 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.

2.5.3 Completeness of answer reduction

We now prove the completeness property of the answer reduction transformation. Similarly to Section 2.4, the completeness property implies that the value of G^{ans} is lower bounded by the value of G.

Proposition 2.34. *For all oracularizable synchronous strategies $\mathscr{S}$ for G, there exists an oracularizable synchronous strategy $\mathscr{S}^{\mathrm{ans}}$ for G^{ans} such that*

$$\omega(G_n^{\mathrm{ans}}, \mathscr{S}^{\mathrm{ans}}) \geq \frac{1}{2} + \frac{1}{2}\omega(G_n, \mathscr{S}) \ .$$

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

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 $\mathscr{S}^{\mathrm{ans}} = (\tau, \{N^x\})$ for G^{ans}. Before doing so, we define some intermediate measurements. Let $\mathcal{X}$ and $\mathscr{A}$ denote the question and answer sets of G, respectively. For all $x, y \in \mathcal{X}, a, b \in \mathscr{A}$:

- $N^{x,y}_{a,b} = \begin{cases} M^x_a \ M^y_b & \text{if } (x,y) \text{ is a nontrivial question for } G \\ 1 & \text{if } (x,y) \text{ is a trivial question for } G \text{ and } a = b = 0 \\ 0 & \text{otherwise} \end{cases}$
- $N^x_a = M^x_a$.

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. □

2.5.4 Soundness of answer reduction

Proposition 2.35. *For all $t \in \{q, co\}$, $\omega_t^s(G) < 1 \implies \omega_t^s(G^{\mathrm{ans}}) < 1$.*

Proof. Let $\mathscr{S}^{\mathrm{ans}} = (\tau, \{N^{\hat{x}}\})$ 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 $\mathscr{S}^{\mathrm{ans}}$.

From the condition that the strategy $\mathscr{S}^{\mathrm{ans}}$ 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 2.2.5 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 2.36. *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 2.13 we get that for all $i \in [t]$,

$$A_{[r \mapsto r_i | c]} \approx_{\sqrt{2\delta}} B^i_r . \tag{2.5.1}$$

Using Theorem 2.16 we can right-multiply Equation (2.5.1) for $i = 1$ by the measurement $A_{[r \mapsto r_{2:d}]}$ to deduce

$$A_{[r \mapsto r_1]} \cdot A_{[r \mapsto r_2]} \approx_{\sqrt{2\delta}} B^1_{r_1} \cdot A_{[r \mapsto r_2]} \tag{2.5.2}$$

Using using Theorem 2.16 again we get that the right hand side of Equation (2.5.2) 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 2.16, 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 2.36 with $A = N^{x,i,j}$, $B^1 = N^{x,y,\eta(i)}$ and $B^2 = N^{x,y,\eta(j)}$, we get

$$N^{x,y,\eta(j)}_s \cdot N^{x,y,\eta(i)}_r \approx N^{x,y,\eta(i)}_r \cdot N^{x,y,\eta(j)}_s . \tag{2.5.3}$$

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 2.16

twice we get

$$N_s^{x,y,\eta(j)} \cdot N_r^{x,y,\eta(i)} \approx N_s^{x,y,\eta(j)} \cdot N^{x,i,k}_{[(a_i,a_k)\mapsto a_i|r]} \approx N^{x,j,k}_{[(a_j,a_k)\mapsto a_j|s]} \cdot N^{x,i,k}_{[(a_i,a_k)\mapsto a_i|r]}$$

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 (2.5.3), 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 2.18) on the set of measurements $\{N^{x,i}\}_{i\in[T]}$, and obtain a projective measurement $M^x = \{M^x_a\}$ 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

$$M^x_{[a\mapsto a_i|r]} \approx N_r^{x,y,\eta(i)} \ . \tag{2.5.4}$$

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 2.36 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 2.16 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 2.36. Since $M_\pi^{x,y}$ is projective, we have that

$$M^{x,y}_{[\pi\mapsto(\pi_i,\pi_j,\pi_k)|(r,s,t)]} \approx N^{x,y,i,j,k}_{r,s,t} \ . \tag{2.5.5}$$

We now relate the $M^{x,y}$ measurements to the M^x measurements constructed previously. Using the triangle inequality with Equation (2.5.4) we get for all $x, y \in \mathcal{X}$ and $j \in [T]$,

$$M^{x,y}_{[\pi\mapsto\pi_{\eta(j)}|r]} \approx M^{x}_{[a\mapsto a_j|r]} \tag{2.5.6}$$

and similarly

$$M^{x,y}_{[\pi\mapsto\pi_{\lambda(j)}|r]} \approx M^{y}_{[a\mapsto a_j|r]} \ . \tag{2.5.7}$$

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 2.37. *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 2.16 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 2.37 to Equations (2.5.6) and (2.5.7) 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

$$M^{x,y}_{[(a,b,w)\mapsto a]} \approx M^x_a \tag{2.5.8}$$

$$M^{x,y}_{[(a,b,w)\mapsto b]} \approx M^y_b \ . \tag{2.5.9}$$

Using Theorem 2.16 several times with Equations (2.5.8) and (2.5.9) 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

$$M^{x,y}_{[(a,b,w)\mapsto (a,b)]} \approx M^x_a \cdot M^y_b \cdot M^x_a \ . \tag{2.5.10}$$

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 2.13 applied to Equation (2.5.10) 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 2.15 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 2.33 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 2.5.2), 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 2.13 with Equation (2.5.5), 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 2.15 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

$$\begin{aligned}
&\mathop{\mathbf{E}}_{x,y} \sum_{i,j,k} \sum_{\pi} \mathbf{1}[(\pi_i, \pi_j, \pi_k) \text{ unsat. } \varphi_{x,y}] \cdot \tau\left(M_\pi^{x,y}\right) \\
&\leq \mathop{\mathbf{E}}_{x,y} \sum_{i,j,k} \sum_{\pi_i, \pi_j, \pi_k} \mathbf{1}[(\pi_i, \pi_j, \pi_k) \text{ unsat. } \varphi_{x,y}] \cdot \tau(N_{\pi_i,\pi_j,\pi_k}^{x,y,i,j,k}) + 2\nu \\
&\leq L^3 \left(\frac{\varepsilon}{\theta} + 2\nu\right) .
\end{aligned}$$

Let $\zeta = L^3\left(\frac{\varepsilon}{\theta} + 2\nu\right) + 2\delta$. Then we deduce that

$$\omega(G, \mathcal{S}) \geq 1 - \zeta.$$

Since δ, ν are proper error functions of ε, so is ζ. Thus $\zeta \to 0$ as $\varepsilon \to 0$. Furthermore, the strategy $\mathcal{S}$ is finite-dimensional if and only if $\mathcal{S}^{\text{ans}}$ is finite-dimensional. Thus, suppose that $\omega_t^s(G^{\text{ans}}) = 1$ for $t = q$ (resp. for $t = co$). This implies that there is a sequence of finite-dimensional (resp. commuting operator) strategies $\mathcal{S}^{\text{ans}}$ such that $\omega(G^{\text{ans}}, \mathcal{S}^{\text{ans}})$ approaches 1. This in turn implies the existence of a sequence of finite-dimensional (resp. commuting operator) strategies $\mathcal{S}$ such that $\omega(G, \mathcal{S})$ approaches 1, and thus $\omega_t^s(G) = 1$. Taking the contrapositive, we conclude that

$$\omega_t^s(G) < 1 \Longrightarrow \omega_t^s(G^{\text{ans}}) < 1 .$$

This finishes the proof of the Proposition. □

2.5.5 Proof of Theorem 2.32

We now prove the main result of this section, Theorem 2.32. 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 2.5, 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 2.5, 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 2.5 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 2.5. If the winning conditions are satisfied, then D^{ans} outputs 1 (accepts), otherwise it outputs 0 (rejects).

Now assume the conditions of Theorem 2.32; 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. $\mathsf{TIME}_C(n) \le Q(n)$, and
3. $\mathsf{TIME}_D(n) \le T(n)$.

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 2.32.

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 2.5, 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 $\text{poly}(|D|, Q(n), \log T(n), \log n)$ to compute a clause. Computing the $\eta(\cdot)$ and $\lambda(\cdot)$ maps also take time at most $\text{poly}(\log T(n))$ (because it requires computing $T(n)$). Thus, in total, the complexity of the answer-reduced verifier is $\text{poly}(|D|, |C|, Q(n), \log T(n), \log n) = \text{poly}(|D|, |C|, \beta, \log^{\beta} n)$.

Completeness and Soundness. Completeness follows from Theorem 2.34. Soundness follows from Theorem 2.35.

This completes the proof of Theorem 2.32.

2.6 Compressions of nonlocal games and their applications

In this section we describe the compression theorems and some of their applications.

2.6.1 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 2.3 from the introduction.

Theorem 2.38 (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 $n \geq n_0$,*

$$\max\left\{\mathsf{TIME}_C(n), \mathsf{TIME}_D(n)\right\} \leq n^\alpha , \tag{2.6.1}$$

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*

$$\omega_t^s(G_n) < 1 \Longrightarrow \omega_t^s(G'_n) < 1 \ .$$

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 2.4 and 2.5. 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 2.27.

```
**Input**: $D, C$.
Compute $(D^{\mathrm{intro}}, C^{\mathrm{intro}}) = \mathcal{A}QuestionReduction_{\alpha}(D, C)$.
Compute $(D', C') = \mathcal{A}AnswerReduction_{\beta}(D^{\mathrm{intro}}, C^{\mathrm{intro}})$.
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 (2.6.1) is satisfied. Then, the complexity bounds on $(D^{\mathrm{intro}}, C^{\mathrm{intro}})$ given by the conclusion of Theorem 2.27 are exactly those that satisfy the conditions of Theorem 2.32. Thus, the output (D', C') of $\mathcal{A}AnswerReduction_{\beta}(D^{\mathrm{intro}}, C^{\mathrm{intro}})$

satisfy the conclusions of Theorem 2.32 (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 $\beta = \mathrm{poly}(\alpha)$,$n_0^{\text{intro}} = \mathrm{poly}(\beta, n_0)$ as given by Theorem 2.27. Then, define the integers $\gamma = \mathrm{poly}(\beta)$, $n_0^{\text{ans}} = \mathrm{poly}(\gamma^\gamma, n_0^{\text{intro}}) = \mathrm{poly}(\gamma^\gamma, n_0)$ as given by Theorem 2.32. Define $n_0' = \max\{n_0, n_0^{\text{intro}}, n_0^{\text{ans}}\}$.

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

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

Then, by the completeness of Answer Reduction, there is an oracularizable synchronous strategy $\mathscr{S}'$ for G_n' such that

$$\omega(G_n', \mathscr{S}') \geq \frac{1}{2} + \frac{1}{2}\omega(G_n^{\text{intro}}, \mathscr{S}^{intro}) \geq \frac{1}{2} + \frac{1}{2}\omega(G_n, \mathscr{S}) \ .$$

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

We establish the soundness property of $\mathscr{V}'$ by combining the soundness guarantees of Question Reduction and Answer Reduction:

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

Finally, we establish the entanglement bound property by combining the entanglement bounds from Question Reduction and Answer Reduction

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

□

2.6.2 Super compression

The gapless compression procedure of Theorem 2.38 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 2.39 (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 $n \geq n_0$,*

$$\max\left\{\mathsf{TIME}_C(n), \mathsf{TIME}_D(n)\right\} \leq n^\alpha , \tag{2.6.2}$$

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)*

$$\max\{\mathsf{TIME}_{C^{\text{super}}}(\kappa), \mathsf{TIME}_{D^{\text{super}}}(\kappa)\} \leq \kappa^{\lambda}\ .$$

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 2.38, the conclusions of Theorem 2.39 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 2.38. 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. (2.6.1) 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 $\mathcal{A}SuperCompress_\alpha$ 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. [71, 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 2.38 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 $n \in \mathbb{N}$,

$$\max\{\mathsf{TIME}_{D'}(n), \mathsf{TIME}_{C'}(n)\} \leq \log^\gamma n \ .$$

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 $n \geq \kappa$,* *the Turing machines $D^{\text{super}}_{\lambda^*}, C^{\text{super}}_{\lambda^*}$ when given index n never reject due to exceeding the n^{λ^*} timeout.*

Proof. Next, the time complexity of $D^{\text{super}}_{\lambda}$ (resp. $C^{\text{super}}_{\lambda}$) *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. (2.6.1). The algorithm $\mathcal{A}GaplessCompress_{\lambda}$ runs in time $\text{poly}(|D^{\text{super}}_{\lambda}|, |C^{\text{super}}_{\lambda}|, \lambda) = \text{poly}(|D|, |C|, \lambda)$. Putting this together with the complexity bounds on D' (resp. C'), we have that the complexity of $D^{\text{super}}_{\lambda}$ (resp. $C^{\text{super}}_{\lambda}$), without the automatic timeout, is at most

$$\sigma(n^{\alpha} \cdot |D| \cdot |C| \cdot \lambda \cdot \log^{\gamma} n)^{\sigma} \tag{2.6.3}$$

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 (2.6.3) 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 $\gamma = \text{poly}(\lambda^*)$, 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 $D^{\text{super}}_{\lambda^*}$ and $C^{\text{super}}_{\lambda^*}$ 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 $(D^{\text{super}}_{\lambda^*}, C^{\text{super}}_{\lambda^*})$. The algorithm clearly runs in polynomial time.

By construction the Turing machines $(D^{\text{super}}_{\lambda^*}, C^{\text{super}}_{\lambda^*})$ 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 $(D^{\text{super}}, C^{\text{super}}) = (D^{\text{super}}_{\lambda^*}, C^{\text{super}}_{\lambda^*})$.

Fix $t \in \{q, co\}$. Since the Turing machines $D^{\text{super}}, C^{\text{super}}$ never reject due to the time-out, we have that the verifier in the game G^{super}_n 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

$$\sup_{\text{finite-dim osync } \mathscr{S}_n} \omega(G_n, \mathscr{S}_n) = 1. \tag{2.6.4}$$

Define

$$c_n = \sup_{\text{finite-dim osync } \mathscr{S}^{\text{super}}_n} \omega(G^{\text{super}}_n, \mathscr{S}^{\text{super}}_n)$$

and define $c = \inf_{n \geq \kappa} c_n$. We aim to prove that $c = 1$; this would imply that $\omega^s_q(G^{\text{super}}_n) = 1$ 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 $\mathscr{S}^{\text{super}}_m$ denote a finite-dim osync strategy for G^{super}_m 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 2.38, whose value satisfies

$$\omega(G'_m, \mathscr{S}'_m) \geq \frac{1}{2} + \frac{1}{2}\omega(G_m^{\text{super}}, \mathscr{S}_m^{\text{super}}) \geq \frac{1+c}{2} \,. \tag{2.6.5}$$

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

$$\omega(G_n^{\text{super}}, \mathscr{T}_n) \geq \frac{1}{2} + \frac{1}{4}\omega(G_n, \mathscr{S}_n) + \frac{1}{4}\omega(G'_{n+1}, \mathscr{S}'_{n+1}) \geq \frac{5+c}{8} + \frac{1}{4}\omega(G_n, \mathscr{S}_n) \tag{2.6.6}$$

where the second inequality follows from eq. (2.6.5). 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. (2.6.6) over finite-dim osync strategies $\mathscr{S}_n$ for G_n and using eq. (2.6.4), 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 2.38, 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 2.38, 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 2.38 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. □

2.6.3 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 [13] using very different techniques based on group theory.

Theorem 2.40. *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 [44, 45] 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 2.39.

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 [58], 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 [38].[13] Again, the proof approaches are quite different: his proof uses techniques from approximate representation theory as well as group

[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 $\{A_a^x\}, \{B_b^y\}$.

theory.

Corollary 2.41 ([38])**.** *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 2.40, by Theorem 2.39, 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.

□

2.6.4 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 2.1.1, we combine our gapless compression theorem with a consequence of the $\mathsf{MIP}^* = \mathsf{RE}$ theorem from [14], 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 2.42 ([14])**.** *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*

$$\sup_{\textit{finite-dim osync } \mathscr{S}} \omega(G, \mathscr{S}) = 1.$$

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 [14, 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 [14, 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 $\mathrm{poly}(|S|)$ time, we obtain a checker C for the game G that runs in $\mathrm{poly}(|S|)$ time. Thus, on input S, the algorithm $\mathcal{A}HaltingGame$ 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 2.43. *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 $\mathcal{A}HaltingGame$ we construct the sequence of games $\mathcal{G}_\phi = (G_n)_{n\in\mathbb{N}}$ with verifier $\mathcal{V} = (D, C)$. Let

$$c_n = \sup_{\text{finite-dim osync } \mathcal{S}_n} \omega(G_n, \mathcal{S}_n),$$

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 $\mathcal{A}HaltingGame(S_n)$.
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 $\mathcal{A}HaltingGame(S_n)$.
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 $\mathcal{G}_\phi$: 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 $\mathcal{G}^{\text{super}} = (G_n^{\text{super}})_{n\in\mathbb{N}}$ 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 2.39.

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 2.44. *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 [72]. 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 2.45. *The exact q-value problem is complete for* Π_2.

2.6.5 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 2.1. In particular we construct *super compression* procedures (procedures that map families of games to a single equivalent game).

The following theorem was proved in [54]:

Theorem 2.46. *Assume that the approximate q-value problem is Σ_1-hard. Then there exists a computable map $\mathcal{A}GapCompress_q$ 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 2.47. *Assume that the approximate co-value problem is Π_1-hard. Then there exists a computable map $\mathcal{A}GapCompress_{co}$ 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 [44] 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 2.48. *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 2.49. *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 $\mathscr{G} = (G_n)_{n\in\mathbb{N}}$ 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 $T^q_{\mathscr{G}}$: it takes in as input a precision parameter ε and an integer m, and it searches for a finite-dimensional strategy $\mathscr{S}$ (specified with precision ε) such that the game G_m in the sequence $\mathscr{G}$ has $\omega(G_m, \mathscr{S}) \geq 1 - 2\varepsilon$. 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 $\mathscr{S}$ over an $\varepsilon$-net of quantum strategies of dimension $d$, such
      that $\omega(G_m, \mathscr{S}) > 1 - 2\varepsilon$, then halt.
end
```

Pseudocode 13: Specification of $T^q_{\mathscr{G}}$

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: "$\forall k, m\, \exists n\, T^q_{\mathscr{G}}$ 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 $m \in \mathbb{N}$.

□

2.7 Appendix A: The pasting lemma

We now prove Theorem 2.18, which is reproduced below for convenience. Recall that $\mathscr{A}$ is a von Neumann algebra with a normal tracial state τ.

Lemma 2.50 (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*

$$M^{(i)}_a M^{(j)}_b \approx_\varepsilon M^{(j)}_b M^{(i)}_a$$

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 $i \in [K]$,

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

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

$$P^s_{\vec{a}} = A^{(s_1)}_{\vec{a}_1} \cdot A^{(s_2)}_{\vec{a}_2} \cdots A^{(s_k)}_{\vec{a}_k}.$$

Note that $P^s = \{P^s_{\vec{a}}\}_{a \in \mathcal{A}^k}$ 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 2.51. *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

$$\begin{aligned} \|P^{s,t} \cdot A^{(i)} - A^{(i)} \cdot P^{s,t}\|_\tau &= \|P^s \cdot A^{(t)} \cdot A^{(i)} - A^{(i)} \cdot P^s \cdot A^{(t)}\|_\tau \\ &\leq \left\| P^s \cdot \left(A^{(t)} \cdot A^{(i)} - A^{(i)} \cdot A^{(t)} \right) \right\|_\tau + \left\| \left(P^s \cdot A^{(i)} - A^{(i)} \cdot P^s \right) \cdot A^{(t)} \right\|_\tau \end{aligned} \tag{2.7.1}$$

where the inequality follows from the triangle inequality of the τ-norm on operator sets (Theorem 2.10).

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

$$\begin{aligned} &= \sum_{\substack{\vec{a} \in \mathcal{A}^k \\ b,c \in \mathcal{A}}} \mathrm{TR} \left(\left(A_b^{(t)} \cdot A_c^{(i)} - A_c^{(i)} \cdot A_b^{(t)} \right)^* (P_{\vec{a}}^s)^* P_{\vec{a}}^s \left(A_b^{(t)} \cdot A_c^{(i)} - A_c^{(i)} \cdot A_b^{(t)} \right) \right) \\ &= \sum_{b,c \in \mathcal{A}} \mathrm{TR} \left(\left(A_b^{(t)} \cdot A_c^{(i)} - A_c^{(i)} \cdot A_b^{(t)} \right)^* \left(A_b^{(t)} \cdot A_c^{(i)} - A_c^{(i)} \cdot A_b^{(t)} \right) \right) \end{aligned}$$

where we used the fact that $\sum_{\vec{a} \in \mathcal{A}^k} (P_{\vec{a}}^s)^* P_{\vec{a}}^s = 1$.

The second term in (2.7.1) 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 (2.7.1) 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

$$Q_{\vec{a}} = P_{\vec{a}}^s (P_{\vec{a}}^s)^* \ .$$

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 $A_a^{(i)}$ operators are projections).

We now calculate the closeness of $Q_{[\vec{a}\mapsto\vec{a}_i|b]}$ to the individual $A^{(i)}_b$'s:

$$\begin{aligned}
\sum_{b\in\mathcal{A}} \|Q_{[\vec{a}\mapsto\vec{a}_i|b]} - A^{(i)}_b\|^2_\tau &= \sum_{b\in\mathcal{A}} \tau\Big(\Big(Q_{[\vec{a}\mapsto\vec{a}_i|b]} - A^{(i)}_b\Big)^2\Big) \\
&\leq 2 - 2\sum_{b\in\mathcal{A}} \tau\Big(Q_{[\vec{a}\mapsto\vec{a}_i|b]} A^{(i)}_b\Big) \\
&= 2 - 2\sum_{\vec{a}} \tau\Big(Q_{\vec{a}} A^{(i)}_{\vec{a}_i}\Big)
\end{aligned}$$

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

$$\begin{aligned}
\sum_{\vec{a}} \tau\Big(Q_{\vec{a}} A^{(i)}_{\vec{a}_i}\Big) &= \sum_{\vec{a}} \tau\Big(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot P^{s_{>i}}_{\vec{a}_{>i}} \cdot (P^{s_{>i}}_{\vec{a}_{>i}})^* \cdot A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^* \cdot A^{(i)}_{\vec{a}_i}\Big) \\
&= \sum_{\vec{a}_{<i},\vec{a}_i} \tau\Big(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^* \cdot A^{(i)}_{\vec{a}_i}\Big) \\
&= \sum_{\vec{a}_{<i},\vec{a}_i} \tau\Big(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^*\Big) + \tau\Big(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot \Big((P^{s_{<i}}_{\vec{a}_{<i}})^* \cdot A^{(i)}_{\vec{a}_i} - A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^*\Big)\Big) \\
&= 1 + \sum_{\vec{a}_{<i},\vec{a}_i} \tau\Big(P^{s_{<i}}_{\vec{a}_{<i}} \cdot A^{(i)}_{\vec{a}_i} \cdot \Big((P^{s_{<i}}_{\vec{a}_{<i}})^* \cdot A^{(i)}_{\vec{a}_i} - A^{(i)}_{\vec{a}_i} \cdot (P^{s_{<i}}_{\vec{a}_{<i}})^*\Big)\Big)
\end{aligned}$$

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 2.51. Thus we deduce that

$$\sqrt{\sum_{b\in\mathcal{A}} \|Q_{[\vec{a}\mapsto\vec{a}_i|b]} - A_b^{(i)}\|_\tau^2} \leq \sqrt{2M\varepsilon}\ . \tag{2.7.2}$$

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

$$\begin{aligned}
\sum_{\vec{a}} \tau\Big(Q_{\vec{a}} - Q_{\vec{a}}^2\Big) &= \sum_{\vec{a}} \tau\Big(P^s_{\vec{a}} - Q_{\vec{a}}^2\Big)\\
&= \sum_{\vec{a}} \tau\Big(P^s_{\vec{a}} - P^s_{\vec{a}}\cdot Q_{\vec{a}}\Big) + \tau((P^s_{\vec{a}} - Q_{\vec{a}})\cdot Q_{\vec{a}})\\
&= \sum_{\vec{a}} \tau\Big(P^s_{\vec{a}} - P^s_{\vec{a}}\cdot (P^s_{\vec{a}})^*\Big) + \tau((P^s_{\vec{a}} - Q_{\vec{a}})\cdot Q_{\vec{a}}) + \tau(((P^s_{\vec{a}})^* - Q_{\vec{a}})\cdot P^s_{\vec{a}})\\
&= \sum_{\vec{a}} \tau((P^s_{\vec{a}} - Q_{\vec{a}})\cdot Q_{\vec{a}}) + \tau(((P^s_{\vec{a}})^* - Q_{\vec{a}})\cdot P^s_{\vec{a}})
\end{aligned}$$

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 $\sum_{\vec{a}} \|P^s_{\vec{a}}\|_\tau^2$ and $\sum_{\vec{a}} \|Q_{\vec{a}}\|_\tau^2$ are most 1, this last line is at most $2\sqrt{\sum_{\vec{a}} \|P^s_{\vec{a}} - Q_{\vec{a}}\|_\tau^2}$. To bound this, we note that we can express $P^s_{\vec{a}}$ and $Q_{\vec{a}}$ as longer products

$$P^t_{\vec{b}} = P^{(s_1)}_{\vec{a}_1}\cdot P^{(s_1)}_{\vec{a}_1}\cdots P^{(s_k)}_{\vec{a}_k}\cdot P^{(s_k)}_{\vec{a}_k}\ , \qquad P^u_{\vec{c}} = P^{(s_1)}_{\vec{a}_1}\cdots P^{(s_k)}_{\vec{a}_k}\cdots\cdot P^{(s_1)}_{\vec{a}_1}$$

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 2.17) 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 2.14 that

$$R_{\vec{a}} \simeq_\eta Q_{\vec{a}}.$$

Using the Data Processing Lemma for consistency (Theorem 2.12), 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 2.13) 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

$$R_{[\vec{a}\mapsto\vec{a}_i|b]} \approx_{\sqrt{2\eta}+\sqrt{2M\varepsilon}} A^{(i)}_{b} \ .$$

Setting $\delta_{pasting}(M, \mathcal{A}, \varepsilon) = \sqrt{2\eta} + \sqrt{2M\varepsilon}$ proves the Lemma.

2.8 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 [15].

Theorem 2.52. *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:

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

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 2.53. *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. $A_a^x, B_b^y \succeq 0$ (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 2.54. *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 2.54. Σ_1-hardness follows from Proposition 2.53 and the Σ_1-hardness of approximating ω_q [14].

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 $1 \le a, b \le d$ 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 $q_i \succeq 0$ 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 $\omega_{\text{fin}}(P) \ge c$ 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 2.52.

□

Theorem 2.55. *Deciding if $\omega_{\text{fin}}(P) \geq c$ is complete for Π_2.*

Proof. Π_2-hardness follows from Proposition 2.53 and Theorem 2.45.

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 2.56. *Deciding if $\omega_{\infty}(P) \geq c$ is complete for Π_1.*

Proof. Π_1-hardness follows from Proposition 2.53 and Theorem 2.40. The inclusion is due to the NPA-hierarchy of [73]. More precisely [73] 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 3: Rigidity and Sum of Squares

This chapter is taken verbatim from our paper "A generalization of CHSH and the algebraic structure of optimal strategies" [74]. All authors of this work contributed equally.

3.1 Introduction

In 1964, Bell showed that local hidden-variable theories, which are classical in nature, cannot explain all quantum mechanical phenomena [75]. 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 [76]. Self-testing has wide reaching applications in areas of theoretical computer science including complexity theory [77, 78, 79], certifiable randomness [80], device independent quantum cryptography [81, 82], and delegated quantum computation [83]. See [84] 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 [20] 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 [85].

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 [86, 87] 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 $\mathbb{Z}_2$ [88]. 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 3.1. *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 [89] 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 [90].

The sum of squares (SOS) decomposition technique in [91] 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 [92]. 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 [88].

Question 3.2. *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 [93].

Self-tests for measurements in higher dimensions have been primarily focused on self-testing n-fold tensor-products of σ_X and σ_Z [94, 95, 96]. 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 [97]. Our games provides another example that is neither Pauli nor Clifford. Since our games are LCS this resolves the question, first posed by [98], in the affirmative.

Question 3.3. *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 [99] 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 [98] 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 [100, 101] from approximate representation theory.

Question 3.4. *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 [102], 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 3.5. *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 [89].

3.1.1 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 3.4, we give a lower-bound on the *quantum value* of this family of games. Specifically in Theorem 3.4.9, 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 [103]. 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 3.5, 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 3.4.

In section 3.7, 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 3.1. This game also answers Question 3.2 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 3.6, we introduce the sum of squares framework, using an important lemma proven in Section 3.2.4, that gives a streamlined method for proving self-testing. We then use this framework to prove self-testing for our games. Furthermore, in Section 3.8, we show that when restricted to pseudo-telepathic games, the SOS framework reduces to the solution group formalism of Cleve, Liu, and Slofstra [99].

In section 3.9, we construct an LCS game that is obtained from "gluing" two copies of the magic square game together. This game is summarized in Figure 3.1. We exhibit two inequivalent perfect strategies and thus provide an answer to Question 3.5.

$$\begin{array}{ccccccccc}
e_1 & — & e_2 & — & e_3 & & & & \\
| & & | & & \| & & & & \\
e_4 & — & e_5 & — & e_6 & & & & \\
| & & | & & \| & & & & \\
e_7 & — & e_8 & — & e_9 & & & & \\
 & & & & \| & & & & \\
 & & & & e_{10} & — & e_{11} & — & e_{12} \\
 & & & & \| & & | & & | \\
 & & & & e_{13} & — & e_{14} & — & e_{15} \\
 & & & & \| & & | & & | \\
 & & & & e_{16} & — & e_{17} & — & e_{18}
\end{array}$$

Figure 3.1: 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.

3.1.2 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 3.2.4 that encapsulates the use of GH in proving self-testing. In Section 3.2.4, 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 $v^*(\mathcal{G}_n)$). 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 $\lambda = 4nv^*(\mathcal{G}) - 4$, 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.

3.1.3 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 [104], which was then investigated also by Bavarian and Shor [105] and later extended in [106]. The game we present in section 3.3 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 [107], 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 [108], a family of Bell inequalities, which includes the I_{3322} game, is shown to self-test the maximally entangled state but no measurement operators.

3.1.4 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 3.5, 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 $J \to \omega_5^m I_5$. 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 3.4.

4. One drawback of mod 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

$$x_0x_1 = g_1$$

$$x_0x_1 = g_2.$$

   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 3.9, 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. [109] 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 [108], these positively resolve a question asked in [84] in the context of non-local games.

3.1.5 Organization of paper

In section 3.2, 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 3.3, 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 3.4, 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 3.5, we give a presentation for the groups generated by Alice and Bob's observables. In Section 3.6, we present the SOS framework and give a basic example of its application in proving self-testing. In section 3.7, 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 3.8, we show that the SOS framework reduces to the solution group formalism in the case of pseudo-telepathic LCS games. Finally, in Section 3.9 we provide an example of a non-rigid game.

3.2 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 [110, 111, 112].

3.2.1 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 $\{n, n + 1, \dots, m\}$ 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 $|\psi\rangle = U_A \otimes U_B |\Phi_n\rangle$.

3.2.2 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 3.2.1. A non-local game $\mathcal{G}$ is a tuple $(\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B, \pi, V)$ where $\mathcal{I}_A$ and $\mathcal{I}_B$ are finite question sets, $\mathcal{O}_A$ and $\mathcal{O}_B$ are finite answer sets, π denotes the probability distribution on the set $\mathcal{I}_A \times \mathcal{I}_B$ and $V : \mathcal{I}_A \times \mathcal{I}_B \times \mathcal{O}_A \times \mathcal{O}_B \to \{0, 1\}$ 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 $a \in \mathcal{O}_A$ and Bob with $b \in \mathcal{O}_B$. The players win if and only if $V(i, j, a, b) = 1$.

A *classical strategy* is defined by a pair of functions $f_A : \mathcal{I}_A \to \mathcal{O}_A$ for Alice and $f_B : \mathcal{I}_B \to \mathcal{O}_B$

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*, $\nu(\mathcal{G})$, 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 $\nu(\mathcal{G},\mathcal{S})$ is therefore

$$\nu(\mathcal{G},\mathcal{S}) = \sum_{i,j,a,b} \pi(i,j)\langle\psi|E_{i,a} \otimes F_{j,b}|\psi\rangle V(i,j,a,b).$$

The quantum value of a game, written $\nu^*(\mathcal{G})$, is the supremum of the winning probability over all quantum strategies.

The famous CHSH game [20] 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 $\frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.85$ [20].

A strategy $\mathcal{S}$ is optimal if $\nu(\mathcal{G}, \mathcal{S}) = \nu^*(\mathcal{G})$. 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 $\{E_0, \ldots, E_{n-1}\}$ 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 $\{E_0, \ldots, E_{n-1}\}$ 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 $\delta : \text{real}^+ \longrightarrow \text{real}^+$ 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 3.6, we give as an example the proof of exact rigidity of the CHSH game.

3.2.3 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* [88].

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 [99, 98]. 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 3.7. When restriced to psuedo-telepathic LCS games, our SOS approach is identical to the solution group formalism. We present this in section 3.8 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 $g_1, \ldots, g_s, J$, 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. $\prod_{j\in V_i} g_j^{A_{ij}} = J^{b_i}$.

3.2.4 Gowers-Hatami theorem and its application to self-testing

In order to precisely state our results about self-testing in Section 3.7, we recall the Gowers-Hatami theorem and $(\varepsilon, |\psi\rangle)$-representation [100, 98, 101].

Definition 3.2.2. 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 $f : G \longrightarrow U_n(\mathbb{C})$ such that

$$\mathbb{E}_{x,y} \Re \left(\langle f(x)^* f(y), f(x^{-1}y) \rangle_\sigma \right) \geq 1 - \varepsilon. \tag{3.2.1}$$

In the case of $\varepsilon = 0$, we abbreviate and call such a map a $|\psi\rangle$-representation, in which case the condition 3.2.1 simplifies to

$$\langle f(x)^* f(y), f(x^{-1}y) \rangle_\sigma = 1,$$

or equivalently

$$f(y)^* f(x) f(x^{-1}y) |\psi\rangle = |\psi\rangle, \tag{3.2.2}$$

for all $x, y \in G$. In Condition (3.2.2), 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 $\mathcal{H}_0 = \mathrm{span}\{f(g)|\psi\rangle : g \in G\}$, i.e., the Hilbert space generated by the image of f acting on $|\psi\rangle$.

To see this, we first rewrite (3.2.2) 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

$$f(x)f(y)|\psi\rangle = f(xy)|\psi\rangle \text{ for all } x, y \in G. \tag{3.2.3}$$

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 (3.2.3), 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 [101]. 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 3.2.3 (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 [101], 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 3.2.4 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 3.2.2. 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 3.2.4. *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 $V_A : \mathbb{C}^{d_A} \to \mathbb{C}^{d_A|G_A|}$, $V_B : \mathbb{C}^{d_B} \to \mathbb{C}^{d_B|G_B|}$, 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 $\mathcal{S} = (\{A_i\}, \{B_j\}, |\psi\rangle)$

$$\nu(\mathcal{G}, \mathcal{S}) = \langle\psi| \left(\sum_{i\in I_A, j\in I_B} \lambda_{ij} A_i \otimes B_j + \sum_{i\in I_A} \lambda_i A_i \otimes I + \sum_{j\in I_B} \lambda_j I \otimes B_j + \lambda I \otimes I \right) |\psi\rangle. \tag{3.2.4}$$

As argued earlier, by GH, we have

$$f_A^{\widetilde{S}}(x) \otimes I|\widetilde{\psi}\rangle = V_A^* g_A(x) V_A \otimes I|\widetilde{\psi}\rangle, \tag{3.2.5}$$

$$I \otimes f_B^{\widetilde{S}}(x)|\widetilde{\psi}\rangle = I \otimes V_B^* g_B(x) V_B|\widetilde{\psi}\rangle, \tag{3.2.6}$$

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 3.2.3, $V_{A,\rho}$ 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

$$\begin{aligned} p_{\rho,\sigma} &= \|V_{A,\rho} \otimes V_{B,\sigma} |\widetilde{\psi}\rangle\|^2, \\ |\widetilde{\psi}_{\rho,\sigma}\rangle &= \begin{cases} \frac{1}{\sqrt{p_{\rho,\sigma}}} V_{A,\rho} \otimes V_{B,\sigma} |\widetilde{\psi}\rangle & p_{\rho,\sigma} > 0, \\ 0 & p_{\rho,\sigma} = 0, \end{cases} \end{aligned}$$

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 (3.2.4), 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

$$|\widetilde{\psi}_{\rho,\sigma}\rangle = \begin{cases} |\text{junk}'\rangle|\psi\rangle & (\rho, \sigma) = (\bar{\rho}, \bar{\sigma}), \\ 0 & \text{otherwise.} \end{cases} \tag{3.2.7}$$

Now using (3.2.5), 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 (3.2.7), 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 3.2.5. *If in addition to the assumptions of Lemma 3.2.4, 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 3.2.5 as seen in Sections 3.6 and 3.7.

3.3 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 [88]. 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 3.4, 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 3.5, we present the group G_n generated by the operators in $\mathcal{S}_n$. In Section 3.7, 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 $\mathbb{Z}_n = \{1, \omega_n, \dots, \omega_n^{n-1}\}$, 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 3.3.1. *Given the strategy $\mathcal{S}$ above, it holds that $v(\mathcal{G}_n, \mathcal{S}) = \frac{1}{4n}\langle\psi|\mathcal{B}_n|\psi\rangle + \frac{1}{n}$.*

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

$$\nu(\mathcal{G}, \mathcal{S}) = \frac{1}{4} \langle \psi | \left(\sum_{a=0}^{n-1} E_{0,a} F_{0,a} + E_{0,a} F_{1,-a} + E_{1,a} F_{0,a} + E_{1,a} F_{1,1-a} \right) | \psi \rangle.$$

□

3.4 Strategies for $\mathcal{G}_n$

In this section, we present quantum strategies $\mathcal{S}_n$ for $\mathcal{G}_n$ games. In Section 3.4.2, 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 3.7, 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.

3.4.1 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 $D_{n,j} = I_n - 2e_je_j^*$ 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., $X_ne_i = e_{\sigma_n(i)}$. 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 $\gamma_n = \sqrt{2n + \frac{2}{\sin\left(\frac{\pi}{2n}\right)}}$ is the normalization factor. The generalized observables in $\mathcal{S}_n$ are

$$A_0 = X$$

$$A_1 = z^2D_0X$$

$$B_0 = X$$

$$B_1 = z^2D_0X^*.$$

Example 3.4.1. 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 3.4.2. 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 3.3.1, we have $\nu^*(\mathcal{G}_3) \geq \frac{5}{6}$.

3.4.2 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 3.4.3. *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 3.4.4. *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 3.4.5. *$X^i D_j = D_{\sigma^i(j)} X^i$, 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 $k \in [n]$.

$$XD_j e_k = (-1)^{\delta_{j,k}} e_{\sigma(k)} = (-1)^{\delta_{\sigma(j),\sigma(k)}} e_{\sigma(k)} = D_{\sigma(j)}Xe_k$$

□

Now we prove the strategy defined in section 3.4.1 is a valid quantum strategy.

Proposition 3.4.6. *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 3.4.4 in the third equality.

□

Lemma 3.4.7. *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 $2n - 4 + \frac{2}{\sin\left(\frac{\pi}{2n}\right)}$.*

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

$$\begin{aligned}\mathcal{B}|\varphi\rangle &= \left(\sum_{j=1}^{n-1} A_0^j \otimes B_0^{-j} + A_0^j \otimes B_1^j + A_1^j \otimes B_0^{-j} + z^{-4j} A_1^j \otimes B_1^j\right)|\varphi\rangle \\ &= \left(\sum_{j=1}^{n-1} (X \otimes X^*)^j + z^{2j}\,(X \otimes D_0 X^*)^j + z^{2j} (D_0 X \otimes X^*)^j + (D_0 X \otimes D_0 X^*)^j\right)|\varphi\rangle.\end{aligned}$$

Lemma 3.4.8. *$(X \otimes D_0 X^*)^j\,|\varphi\rangle = (D_0 X \otimes X^*)^j|\varphi\rangle$ and $(X \otimes X^*)^j\,|\varphi\rangle = (D_0 X \otimes D_0 X^*)^j|\varphi\rangle$.*

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

$$(X \otimes D_0 X^*)\,|\sigma^i(0), \sigma^{-i}(0)\rangle = (D_0 X \otimes X^*)|\sigma^i(0), \sigma^{-i}(0)\rangle,$$

$$(X \otimes X^*)\,|\sigma^i(0), \sigma^{-i}(0)\rangle = (D_0 X \otimes D_0 X^*)|\sigma^i(0), \sigma^{-i}(0)\rangle.$$

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

$$\begin{aligned}(X \otimes D_0 X^*)\,|\sigma^i(0), \sigma^{-i}(0)\rangle &= (I \otimes D_0)\,|\sigma^{i+1}(0), \sigma^{-i-1}(0)\rangle \\ &= (D_0 \otimes I)\,|\sigma^{i+1}(0), \sigma^{-i-1}(0)\rangle \\ &= (D_0 X \otimes X^*)|\sigma^i(0), \sigma^{-i}(0)\rangle.\end{aligned}$$

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 3.4.5, 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

$$\mathcal{B}|\varphi\rangle = 2\sum_{i=0}^{n-1}\left(\sum_{r=i+1}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)|\sigma^r(0), \sigma^{-r}(0)\rangle\right.$$
$$\left. + \sum_{r=n}^{n+i-1}\left(1 - z^{2i+n+1}\right)\left(1 - z^{2(r-i)}\right)|\sigma^r(0), \sigma^{-r}(0)\rangle\right).$$

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

$$\begin{aligned}
\mathcal{B}|\varphi\rangle = 2\sum_{i=0}^{n-1}&\left(\sum_{r=i+1}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)|\sigma^r(0), \sigma^{-r}(0)\rangle\right. \\
&\left. + \sum_{r=0}^{i-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)|\sigma^r(0), \sigma^{-r}(0)\rangle\right) \\
= 2\sum_{i=0}^{n-1}&\left(\sum_{r=0}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)|\sigma^r(0)\sigma^{-r}(0)\rangle - 2\left(1 - z^{2i+n+1}\right)|\sigma^i(0)\sigma^{-i}(0)\rangle\right) \\
= 2\sum_{i=0}^{n-1}&\left(\sum_{r=0}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)|\sigma^r(0)\sigma^{-r}(0)\rangle\right) - 4|\varphi\rangle \\
= 2\sum_{r=0}^{n-1}&|\sigma^r(0)\sigma^{-r}(0)\rangle\left(\sum_{i=0}^{n-1}\left(1 - z^{2i+n+1}\right)\left(1 + z^{2(r-i)}\right)\right) - 4|\varphi\rangle.
\end{aligned}$$

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 3.4.3 and 3.4.4, respectively. Putting these together, we obtain

$$\begin{aligned}\mathcal{B}|\varphi\rangle &= 2\left(n+\frac{1}{\sin(\frac{\pi}{2n})}\right)\sum_{r=0}^{n-1}(1-z^{2r+n+1})|\sigma^{r}(0)\sigma^{-r}(0)\rangle - 4|\varphi\rangle \\ &= \left(2n-4+\frac{2}{\sin(\frac{\pi}{2n})}\right)|\varphi\rangle.\end{aligned}$$

□

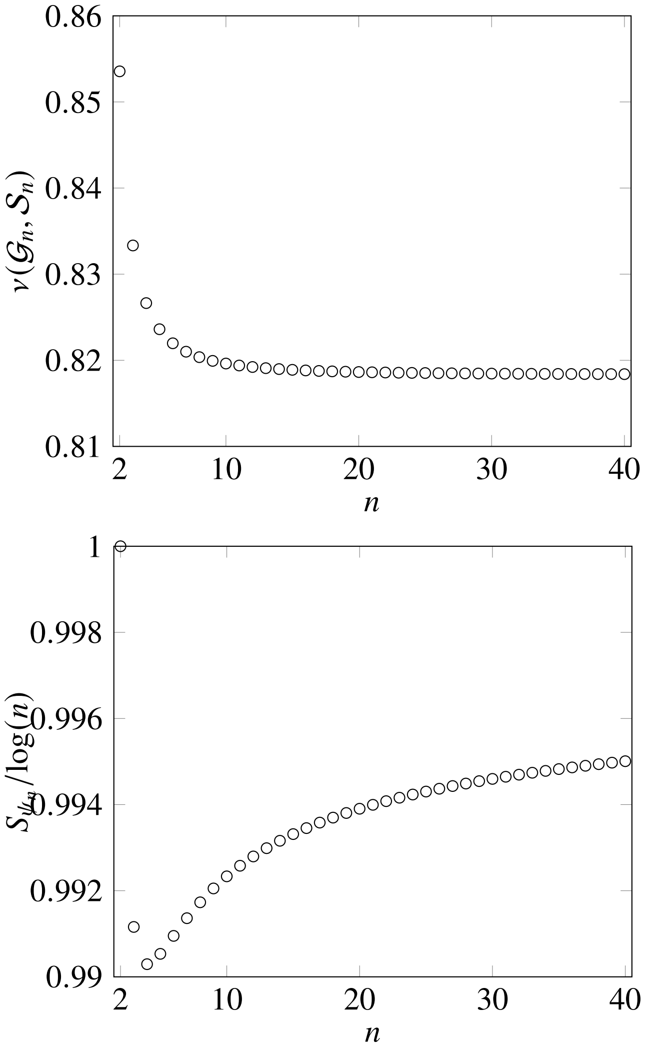

Figure 3.2: The figure on the left illustrates the fast convergence rate of the winning probabilities as they approach the limit $1/2 + 1/\pi$. The figure on the right illustrates the ratio of the entanglement entropy to the maximum entanglement entropy of the states for $n \leq 40$.

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 3.2.

Theorem 3.4.9. $\nu(\mathcal{G}_n, \mathcal{S}_n) = \frac{1}{2} + \frac{1}{2n\sin\left(\frac{\pi}{2n}\right)}$.

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 3.4.10. *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 3.4.11. *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 $\lim_{n\to\infty} \frac{S_{\psi_n}}{\log(n)} = 1$.

□

3.5 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 3.7, we prove this for $n = 3$.

Remark 3.5.1. 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 3.5.2. *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 3.5.3. *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

$$\begin{aligned}
g &= J^i P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_{k-2}} P_0^{j_{k-1}} P_1^{j_k} \\
&= J^i P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_{k-2}} P_0^{j_{k-1}} P_0^{j_k} \big(P_0^{-j_k} P_1^{j_k}\big) \\
&= J^i P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_{k-2}} P_1^{j_{k-1}+j_k} \big(P_1^{-(j_{k-1}+j_k)} P_0^{j_{k-1}+j_k}\big) \big(P_0^{-j_k} P_1^{j_k}\big) \\
&= J^{i-(j_{k-1}+j_k)} P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_{k-2}+j_{k-1}+j_k} \big(P_0^{-(j_{k-1}+j_k)} P_1^{j_{k-1}+j_k}\big) \big(P_0^{-j_k} P_1^{j_k}\big) \\
&= \cdots \\
&= J^{i-s} P_0^{-s_1} \big(P_0^{s_2} P_1^{-s_2}\big) \cdots \big(P_0^{s_{k-1}} P_1^{-s_{k-1}}\big) \big(P_0^{s_k} P_1^{-s_k}\big),
\end{aligned}$$

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 3.5.2 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 3.5.4. $|G_n| \leq n^2 2^{n-1}$ *for all* $n \in \mathbb{N}$.

Proof. Follows from lemma 3.5.3. □

Lemma 3.5.5. $|H_n| \geq n^2 2^{n-1}$ *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 3.4.5. 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 3.5.6. *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:

$$\begin{aligned}\widetilde{f}(J^i(P_0^i P_1^{-i})^2) &= z^{4i}(A_0^i A_1^{-i})^2 \\ &= z^{4i}(X^i z^{-2i}(D_0 X)^{-i})^2 \\ &= (X^i X^{-i} D_{[i]})^2 \\ &= D_{[i]}^2 \\ &= I.\end{aligned}$$

The homomorphism f is surjective because A_0, A_1 generate the group H_n. □

Theorem 3.5.7. $H_n \cong G_n$ *for all* $n \in \mathbb{N}$.

Proof. Since f is surjective, then $n^2 2^{n-1} \le |H_n| \le |G_n| \le n^2 2^{n-1}$. Thus $|H_n| = |G_n|$, so the homomorphism is also injective. □

Remark 3.5.8. 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 3.5.7 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.

3.6 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., [103, 91]. 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 3.3.1, 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

$$2\sqrt{2}I - (A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1) \succeq 0,$$

for any observables A_0, A_1, B_0, B_1. This immediately follows from the following SOS decomposition

$$2\sqrt{2}I - (A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1) = \frac{\sqrt{2}}{4}(A_0 + A_1 - \sqrt{2}B_0)^2 + \frac{\sqrt{2}}{4}(A_0 - A_1 - \sqrt{2}B_1)^2. \tag{3.6.1}$$

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 3.4.1. We learned in Section 3.5 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 (3.6.1)

$$\widetilde{B}_0|\widetilde{\psi}\rangle = \frac{1}{\sqrt{2}}(\widetilde{A}_0 + \widetilde{A}_1)|\widetilde{\psi}\rangle,$$
$$\widetilde{B}_1|\widetilde{\psi}\rangle = \frac{1}{\sqrt{2}}(\widetilde{A}_0 - \widetilde{A}_1)|\widetilde{\psi}\rangle.$$

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

$$\begin{aligned}f_A(J^i P_0^j P_1^k) &= (-1)^i \widetilde{A}_0^j \widetilde{A}_1^k, \\ f_B(J^i P_0^j P_1^k) &= (-1)^i \widetilde{B}_0^j \widetilde{B}_1^k,\end{aligned}$$

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 3.5). 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

$$\begin{aligned}
f_A(J^{i_1}P_0^{j_1}P_1^{k_1})f_A(J^{i_2}P_0^{j_2}P_1^{k_2})|\psi\rangle &= ((-1)^{i_1}\widetilde{A}_0^{j_1}\widetilde{A}_1^{k_1})((-1)^{i_2}\widetilde{A}_0^{j_2}\widetilde{A}_1^{k_2})|\psi\rangle \\
&= (-1)^{i_1+i_2+k_2j_2}\widetilde{A}_0^{j_1}\widetilde{A}_1^{k_1+k_2}\widetilde{A}_0^{j_2}|\psi\rangle \\
&= (-1)^{i_1+i_2+k_1j_2}\widetilde{A}_0^{j_1+j_2}\widetilde{A}_1^{k_1+k_2}|\psi\rangle \\
&= f_A(J^{i_1+i_2+k_1j_2}P_0^{j_1+j_2}P_1^{k_1+k_2})|\psi\rangle,
\end{aligned}$$

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 3.2.5.

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 3.2.5 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, 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

$$H_n = H_n(A_0, A_1) = \omega \sum_{i=0}^{n-1} A_0^i A_1 A_0^{(n-i-1)}. \tag{3.6.2}$$

[1] In Section 3.5, we gave a presentation for G_n using three generators, but in fact one could obtain a presentation using only two generators.

[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 $\mathbb{C}[G_B]/\langle S_j(Q_0, Q_1)\rangle$.

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 3.8, we show that in the special case of pseudo-telepathic games, this framework reduces to the solution group formalism of Cleve, Liu, and Slofstra [99]. The group derived from 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.

3.7 Optimality and rigidity for $\mathcal{G}_3$

In this section, we show that $\mathcal{S}_3$ is optimal, and therefore $v^*(\mathcal{G}_3) = 5/6$. 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 $\mathcal{B}_3$.

[3] Interestingly, cousin games of $\mathcal{G}_5$, defined using systems of equation $x_0 x_1 = 1, x_0, x_1 = \omega^i$ 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 $J \mapsto \omega_5^i I_5$.

3.7.1 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:

$$
\begin{aligned}
&6I - A_0B_0^* - A_0^*B_0 - A_0B_1 - A_0^*B_1^* - A_1B_0^* - A_1^*B_0 - \omega^*A_1B_1 - \omega A_1^*B_1^* \\
&\quad = \lambda_1(S_1^*S_1 + S_2^*S_2) + \lambda_2(T_1^*T_1 + T_2^*T_2) + \lambda_3(T_3^*T_3 + T_4^*T_4) + \lambda_4(T_5^*T_5 + T_6^*T_6),
\end{aligned}
\tag{3.7.1}
$$

where

$$
\begin{aligned}
S_1 &= A_0 + \omega A_1 + \omega^* B_0 + \omega B_1^*, \\
S_2 &= A_0^* + \omega^* A_1^* + \omega B_0^* + \omega^* B_1, \\
T_1 &= A_0B_0^* + aiA_0^*B_0 - aA_0B_1 + iA_0^*B_1^* + aA_1B_0^* - iA_1^*B_0 - \omega^*A_1B_1 - ai\omega A_1^*B_1^*, \\
T_2 &= A_0B_0^* + aiA_0^*B_0 + aA_0B_1 - iA_0^*B_1^* - aA_1B_0^* + iA_1^*B_0 - \omega^*A_1B_1 - ai\omega A_1^*B_1^*, \\
T_3 &= A_0B_0^* - aiA_0^*B_0 - aA_0B_1 - iA_0^*B_1^* + aA_1B_0^* + iA_1^*B_0 - \omega^*A_1B_1 + ai\omega A_1^*B_1^*, \\
T_4 &= A_0B_0^* - aiA_0^*B_0 + aA_0B_1 + iA_0^*B_1^* - aA_1B_0^* - iA_1^*B_0 - \omega^*A_1B_1 + ai\omega A_1^*B_1^*, \\
T_5 &= A_0B_0^* + bA_0^*B_0 - bA_0B_1 - A_0^*B_1^* - bA_1B_0^* - A_1^*B_0 + \omega^*A_1B_1 + b\omega A_1^*B_1^*, \\
T_6 &= 6I - A_0B_0^* - A_0^*B_0 - A_0B_1 - A_0^*B_1^* - A_1B_0^* - A_1^*B_0 - \omega^*A_1B_1 - \omega A_1^*B_1^*,
\end{aligned}
$$

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 $\mathcal{B}_3 \preceq 6I$ in positive semidefinite order. So from Theorem 3.3.1, it holds that $\nu^*(\mathcal{G}_3) \leq 5/6$. Combined with Theorem 3.4.9, 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.

3.7.2 Algebraic relations

As in Section 3.6, we derive group and ring relations for optimal strategies of $\mathcal{G}_3$ from the SOS (3.7.1). 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

$$A_0B_0^*|\psi\rangle = \omega^* A_1B_1|\psi\rangle, \quad A_0^*B_0|\psi\rangle = \omega A_1^*B_1^*|\psi\rangle,$$
$$A_0B_1|\psi\rangle = A_1B_0^*|\psi\rangle, \qquad A_0^*B_1^*|\psi\rangle = A_1^*B_0|\psi\rangle. \tag{3.7.2}$$

Now from these four relations and the fact that A_i, B_j are generalized observables satisfying $[A_i, B_j] = 0$, we obtain

$$\omega^* A_0^*A_1|\psi\rangle = B_1^*B_0^*|\psi\rangle \tag{3.7.3}$$
$$\omega A_0A_1^*|\psi\rangle = B_1B_0|\psi\rangle \tag{3.7.4}$$
$$A_0^*A_1|\psi\rangle = B_0B_1|\psi\rangle \tag{3.7.5}$$
$$A_0A_1^*|\psi\rangle = B_0^*B_1^*|\psi\rangle \tag{3.7.6}$$
$$A_1^*A_0|\psi\rangle = \omega^* B_0B_1|\psi\rangle \tag{3.7.7}$$
$$A_1A_0^*|\psi\rangle = \omega B_0^*B_1^*|\psi\rangle \tag{3.7.8}$$
$$A_1^*A_0|\psi\rangle = B_1^*B_0^*|\psi\rangle \tag{3.7.9}$$
$$A_1A_0^*|\psi\rangle = B_1B_0|\psi\rangle. \tag{3.7.10}$$

From the pair of relations (3.7.3) and (3.7.9) as well as the pair of relations (3.7.4) and (3.7.10), we obtain the following relations between Alice's observables acting on the state $|\psi\rangle$:

$$A_0^*A_1|\psi\rangle = \omega A_1^*A_0|\psi\rangle, \tag{3.7.11}$$
$$A_1A_0^*|\psi\rangle = \omega A_0A_1^*|\psi\rangle. \tag{3.7.12}$$

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 (3.6.2).

Proposition 3.7.1. $(H + H^*)|\psi\rangle = -2|\psi\rangle$

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

$$(B_0 B_1^* + B_1^* B_0)|\psi\rangle = (2A_0^* + 2\omega^* A_1^* + \omega A_0 A_1 + \omega A_1 A_0)|\psi\rangle. \tag{3.7.13}$$

Similarly we have

$$(B_1 B_0^* + B_0^* B_1)|\psi\rangle = (2A_0 + 2\omega A_1 + \omega^* A_0^* A_1^* + \omega^* A_1^* A_0^*)|\psi\rangle. \tag{3.7.14}$$

We proceed by simplifying $T_6|\psi\rangle = 0$ using relations (3.7.2) 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

$$\begin{aligned} 0 &= \big(3I - A_0B_0^* - A_0^*B_0 - A_0B_1 - A_0^*B_1^*\big)^*\big(3I - A_0B_0^* - A_0^*B_0 - A_0B_1 - A_0^*B_1^*\big)|\psi\rangle \\ &= \big(13I - 5P + A_0^*(B_1B_0^* + B_0^*B_1) + A_0(B_0B_1^* + B_1^*B_0) + B_0^*B_1^* + B_0B_1 + B_1B_0 + B_1^*B_0^*\big)|\psi\rangle \\ &= (-2I + A_0^*(B_1B_0^* + B_0^*B_1) + A_0(B_0B_1^* + B_1^*B_0) + B_0^*B_1^* + B_0B_1 + B_1B_0 + B_1^*B_0^*)|\psi\rangle, \quad (3.7.15) \end{aligned}$$

where in the last line, we used $(3I - P)|\psi\rangle = 0$. Using identities (3.7.13) and (3.7.14)

$$\begin{aligned} &\big(A_0^*(B_1B_0^* + B_0^*B_1) + A_0(B_0B_1^* + B_1^*B_0)\big)|\psi\rangle \\ &\quad = \big(4I + \omega A_0A_1A_0 + \omega^*A_0^*A_1^*A_0^* + 2\omega A_0^*A_1 + \omega^*A_0A_1^* + 2\omega^*A_0A_1^* + \omega A_0^*A_1\big)|\psi\rangle. \end{aligned}$$

Transferring Bob's operators to Alice using identities (3.7.3-3.7.6)

$$\big(B_0^*B_1^* + B_0B_1 + B_1B_0 + B_1^*B_0^*\big)|\psi\rangle = \big(A_0A_1^* + A_0^*A_1 + \omega A_0A_1^* + \omega^*A_0^*A_1\big)|\psi\rangle.$$

Plugging these back in (3.7.15)

$$\begin{aligned} 0 &= (2I + \omega A_0A_1A_0 + \omega^*A_0^*A_1^*A_0^* + (3\omega + \omega^* + 1)A_0^*A_1 + (3\omega^* + \omega + 1)A_0A_1^*)|\psi\rangle \\ &= (2I + \omega A_0A_1A_0 + \omega^*A_0^*A_1^*A_0^* + 2\omega A_0^*A_1 + 2\omega^*A_0A_1^*)|\psi\rangle \\ &= (2I + \omega A_0A_1A_0 + \omega^*A_0^*A_1^*A_0^* + \omega A_0^*A_1 + \omega^*A_1^*A_0 + \omega^*A_0A_1^* + \omega A_1A_0^*)|\psi\rangle. \\ &= (2I + H + H^*)|\psi\rangle, \end{aligned}$$

where in the first line we used $1 + \omega + \omega^* = 0$, and in the second line we used identities (3.7.11) and (3.7.12). □

Proposition 3.7.2. $(H + I)|\psi\rangle = (H^* + I)|\psi\rangle = 0$.

Proof. First note

$$\begin{aligned}\langle\psi|H^*H|\psi\rangle = \langle\psi|(3I + A_0^*A_1^*A_0A_1 + A_1^*A_0^*A_1A_0 + A_1^*A_0A_1A_0^* + A_0A_1^*A_0^*A_1 \\ + A_0^*A_1^*A_0^*A_1A_0^* + A_0A_1^*A_0A_1A_0)|\psi\rangle.\end{aligned} \tag{3.7.16}$$

Using (3.7.11) and (3.7.12), 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 (3.7.5) and (3.7.7)

$$\langle\psi|A_0^*A_1^*A_0A_1|\psi\rangle = \langle\psi|A_0^*A_1A_1A_0^*A_0^*A_1|\psi\rangle = \omega\langle\psi|B_1^*B_0^*A_1A_0^*B_0B_1|\psi\rangle = \omega\langle\psi|A_1A_0^*|\psi\rangle,$$

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 (3.7.16), 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 3.7.1. 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 3.7.3. $A_0A_1A_0|\psi\rangle = \omega A_0^*A_1^*A_0^*|\psi\rangle$.

Proof. By Proposition 3.7.2, $H|\psi\rangle = H^*|\psi\rangle$, and by identities (3.7.11), (3.7.12), $(\omega A_0^*A_1 + \omega A_1A_0^*)|\psi\rangle = (\omega^* A_1^*A_0 + \omega^* A_0A_1^*)|\psi\rangle$. Putting these together, we obtain $A_0A_1A_0|\psi\rangle = \omega A_0^*A_1^*A_0^*|\psi\rangle$. □

Proposition 3.7.4. *$A_0A_1^*A_0^*A_1|\psi\rangle = A_0^*A_1A_0A_1^*|\psi\rangle$ in other words $A_0A_1^*$ 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 3.7.11, in the third line we used 3.7.3, and in the fifth line we used 3.7.12.

□

3.7.3 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 3.5.7, we know that the optimal operators of Alice defined in section 3.4.1 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 3.5.8. We apply Corollary 3.2.5 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 3.7.5. *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 3.5.3. 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

$$\begin{aligned} &f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})f_A(J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'})|\psi\rangle \\ &\quad = f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2}J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'})|\psi\rangle \end{aligned} \tag{3.7.17}$$

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 3.5.3, 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 3.5.2, $P_0 P_1^{-1}$ and $P_0^{-1} P_1$ commute. So the right-hand-side of (3.7.17) 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 (3.7.5) and (3.7.6) and the fact that Alice and Bob's operators commute.

Also since Alice and Bob's operators commute

$$\begin{aligned}
f_A(J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'})|\psi\rangle &= \omega^{i'}A_0^{j'}(A_0A_1^*)^{q_1'}(A_0^*A_1)^{q_2'}|\psi\rangle \\
&= (B_0B_1)^{q_2'}\omega^{i'}A_0^{j'}(A_0A_1^*)^{q_1'}|\psi\rangle \\
&= (B_0B_1)^{q_2'}(B_0^*B_1^*)^{q_1'}\omega^{i'}A_0^{j'}|\psi\rangle \\
&= (B_0B_1)^{q_2'}(B_0^*B_1^*)^{q_1'}f_A(J^{i'}P_0^{j'})|\psi\rangle.
\end{aligned}$$

Therefore the left-hand-side of (3.7.17) can be written as

$$\begin{aligned}
&f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})f_A(J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'})|\psi\rangle \\
&\quad = (B_0B_1)^{q_2'}(B_0^*B_1^*)^{q_1'}f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})f_A(J^{i'}P_0^{j'})|\psi\rangle
\end{aligned}$$

Since B_0, B_1 are unitaries, (3.7.17) 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

$$f_A((P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})f_A(P_0^{j'})|\psi\rangle = f_A((P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2}P_0^{j'})|\psi\rangle \tag{3.7.18}$$

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 (3.7.11).

- $q_1 = 1, q_2 = 0$:

$$(P_0P_1^{-1})P_0 = J^2P_0(P_0^{-1}P_1)$$

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 (3.7.11).

- $q_1 = q_2 = 1$:

$$(P_0P_1^{-1})(P_0^{-1}P_1)P_0 = J(P_0P_1^{-1})(P_1^{-1}P_0)P_0 = JP_0(P_1P_0^{-1}) = J^2P_0(P_0P_1^{-1}).$$

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 3.7.3 and in the second last line we used (3.7.12).

The proof that f_B is a $|\psi\rangle$-representation follows similarly. □

Theorem 3.7.6. *$\mathcal{G}_3$ 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 $g_1' = Ug_1U^*$ where $U = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Now $\widetilde{A}_0 = g_1(P_0), \widetilde{A}_1 = g_1(P_1), \widetilde{B}_0 = g_1'(P_0)^*, \widetilde{B}_1 \coloneqq g_1'(P_1)$ is the same strategy defined in example 3.4.2.

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 $\nu(\mathcal{G}_3, \mathcal{S}_{g_1,g_1',|\psi\rangle})$. 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 3.2.5.

□

Remark 3.7.7. 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.

3.8 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 [99] 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 3.2.3 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:

$$\sum_{x:x\in S_i} E_{i,x} = \frac{1}{2}\left(I + (-1)^{b_i} \prod_{k\in V_i} A_k^{(i)}\right) \tag{3.8.1}$$

$$\sum_{x:y=x_j} E_{i,x} = \frac{1}{2}\left(I + yA_j^{(i)}\right) \tag{3.8.2}$$

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 3.8.1 and 3.8.2 we have

$$\begin{aligned}
\left(1 - \sum_{\substack{x,y:\\ x\in S_i\\ y=x_j}} E_{i,x}F_{j,y}\right) &= I - \sum_{y} F_{j,y} \sum_{\substack{x:\\ x\in S_i\\ y=x_j}} E_{i,x} \\
&= I - \frac{1}{4}\sum_{y} F_{j,y}\left((I + yA_j^{(i)})(I + (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)})\right) \\
&= I - \frac{1}{4}\sum_{y} F_{j,y}\left(I + yA_j^{(i)} + (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)} + y(-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)}\right) \\
&= I - \frac{1}{4}F_{j,1}\left(I + A_j^{(i)} + (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)} + (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)}\right) \\
&\qquad\qquad - \frac{1}{4}F_{j,-1}\left(I - A_j^{(i)} + (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)} + -(-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)}\right) \\
&= I - \frac{1}{4}I - \frac{1}{4}B_jA_j^{(i)} - \frac{1}{4}(-1)^{b_i}\prod_{k\in v_i} A_k^{(i)} - \frac{1}{4}B_j(-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)} \\
&= \frac{1}{8}\left((I - B_jA_j^{(i)})^2 + (I - (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)})^2 + (I - (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}A_j^{(i)}B_j)^2\right).
\end{aligned}$$

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 $j \in V_i$,

$$B_j|\psi\rangle = A_j^{(i)}|\psi\rangle \tag{3.8.3}$$

$$|\psi\rangle = (-1)^{b_i}\prod_{k\in v_i} A_k^{(i)}|\psi\rangle \tag{3.8.4}$$

Using identities 3.8.3 and 3.8.4 it is possible to define a $|\psi\rangle$-representation for the solution group

$G_{A,b}$.

3.9 A non-rigid pseudo-telepathic LCS game

The canonical example of a pseudo-telepathic LCS games is the Mermin-Peres magic square game [89] 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 3.3: 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 [113].

$$\begin{array}{lll} A_1 = I \otimes \sigma_Z, & A_2 = \sigma_Z \otimes I, & A_3 = \sigma_Z \otimes \sigma_Z \\ A_4 = \sigma_X \otimes I, & A_5 = I \otimes \sigma_X, & A_6 = \sigma_X \otimes \sigma_X \\ A_7 = \sigma_X \otimes \sigma_Z, & A_8 = \sigma_Z \otimes \sigma_X, & A_9 = \sigma_Y \otimes \sigma_Y, \end{array}$$

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 3.4.

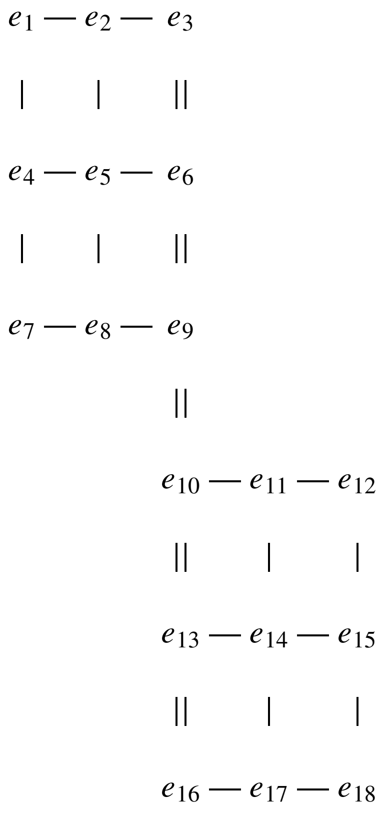

Figure 3.4: This describes a LCS game with 18 variables $e_1, e_2, \ldots, e_{18}$. Each single-line indicates that the variables along the line multiply to 1, and the double-line indicates that the variables along the line multiply to -1.

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 3.9.1. *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

$$(U_A E_1 \otimes U_B)|\psi_1\rangle = ((A_1 \otimes I)|\psi\rangle)|\text{junk}_1\rangle \tag{3.9.1}$$

$$(U_A E_5 \otimes U_B)|\psi_1\rangle = ((A_5 \otimes I)|\psi\rangle)|\text{junk}_1\rangle \tag{3.9.2}$$

$$(V_A F_1 \otimes V_B)|\psi_2\rangle = ((A_1 \otimes I)|\psi\rangle)|\text{junk}_2\rangle \tag{3.9.3}$$

$$(V_A F_5 \otimes V_B)|\psi_2\rangle = ((A_5 \otimes I)|\psi\rangle)|\text{junk}_2\rangle. \tag{3.9.4}$$

From relation (3.9.2), 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 (3.9.1), 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 (3.9.1) and (3.9.3), 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 3.8 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 4: On Synchronous Strategies

This chapter is taken verbatim from our paper “Synchronous Values of Games” [32]. All authors of this work contributed equally.

4.1 Introduction

Nonlocal games have been the central object of study in many areas of computer science and quantum information [6, 4, 114, 3, 2]. They play a central role in our understanding of entanglement. Such games were vital to the recent resolution of the Connes’ Embedding Problem [14] and to answering the Tsirelson Problems [38, 14] about the relationships between the different mathematical models for entanglement.

The *value* of a nonlocal game is the supremum of the probability of winning the game over all allowed strategies. The value of a game can vary depending on the types of strategies or probability densities that are allowed, and there has been considerable interest in how the value of a game can change when one is allowed to use quantum assisted strategies versus classically defined distributions [20, 115, 85, 116, 117, 118]. In addition, the proofs of the separation of the various mathematical models for entanglement involved finding games whose quantum assisted values depended on the particular mathematical model used to describe entanglement. Thus, separating the values of games for the various models has been the most successful tool in showing that these various models of quantum densities are different [14, 13, 38, 119, 120, 121, 122].

In this paper we are interested in how values of games behave when one puts on the restriction that the probability densities derived from the various models must also be *synchronous*, a term we define later. There are several reasons for this interest. First, it has been shown that the study of synchronous densities is related to the study of traces on C*-algebras [58, 60]. For this reason, finding synchronous values of games turns into problems about optimizing the trace of an element of a C*-algebra over certain types of traces on the C*-algebra, which lends a totally different flavour to the theory of values of games.

Second, the Connes' Embedding Problem in its original form is a question about the behaviour of traces. So studying synchronous values of games provides a much more direct link between this problem and games.

Finally, there is a family of games known as *synchronous games* that has been very useful in delineating the separations between the different models for quantum densities. In fact, the separations between the different models for entanglement have all been shown using synchronous games. For synchronous games, it is very natural to restrict the allowed strategies to also be synchronous.

Thus, hopefully, the study of synchronous values of synchronous games could lead to a clearer understanding of the negative resolution of the Connes' Embedding Problem.

In section 2, we delineate these ideas and definitions more clearly.

In section 3, we turn our attention to the graph colouring game. In this game the players are given c colours with c smaller than the chromatic number of the graph. The value of this game is in some sense a measure of how nearly they can convince someone that they have successfully coloured the graph with only c-colours. Remarkably the quantum assisted value can be much higher than the classical value of these games.

We show that for a particular density on inputs, the synchronous local value of this game is a function of the max c-cut of the graph, while the ordinary local value is related to the max cut problem for a bipartite extension of the graph. This leads us to introduce a quantum version of max cut that is motivated by the quantum assisted synchronous value of the 2-colouring game and we prove that this value is given by an SDP. There are many SDP relaxations of max cut, and our results show that one of these relaxations corresponds to the synchronous value of this game. For an introduction to this literature see [123]. We give a formula for the quantum assisted synchronous value of the 2-colouring game of a graph with any density on inputs in terms of an SDP and compute this value for some graphs.

In section 4, we turn our attention to a family of games that has been studied extensively in the literature, called XOR games. For XOR games, their ordinary value and their synchronous value are shown to be optimization problems over two different spectrahedra.

In section 5, we return to the graph colouring game and study the problem of 2-colouring an odd cycle. Even though this game is synchronous, we show that often there are non-synchronous strategies that out perform any synchronous strategy. In fact, we show that as one varies the prior distributions on pairs of vertices, which are the inputs of this game, then there are various regimes where the synchronous values are smaller than the non-synchronous values and other regimes where they are the same.

In section 6, we turn our attention to parallel repetition of games. A famous result in game theory says that unless the classical value of a game is 1, then the value of playing n parallel copies of the game tends to 0 as n grows. In contrast, we give an example of a game whose synchronous value is strictly increasing under parallel repetition. The *bias* of the XOR of two XOR games is known to be multiplicative. We show that in contrast the synchronous bias need not be multiplicative.

Finally, each synchronous strategy for a game corresponds to a certain arrangement of projections in a tracial C*-algebra. In section 7, we derive conditions that are necessarily met by any arrangement of projections that yield a correlation that attains the synchronous value of the game. For the CHSH game we show that these relations force all of the projections to commute, and that, consequently, for the CHSH game the quantum-assisted synchronous value is equal to the classical value of the game. More generally, we give conditions which must hold whenever the max value of a game occurs with a finite dimensional synchronous strategy.

4.2 Values of Games

The types of games that we shall be interested in are *two player nonlocal games*. These are *cooperative games* in which two players referred to as Alice and Bob cooperate to give correct pairs of answers to pairs of questions posed by a third party often called the *Referee* or *Verifier*. The nonlocality condition is that once the game starts the players cannot communicate with one another. In particular, Alice does not know what question Bob has received and vice versa. Whether the pair of answers returned by the players is satisfactory or not depends not just on the individual answers but on the 4-tuple consisting of the question-answer pairs.

More formally a nonlocal game is described by two input sets I_A, I_B, two output set O_A, O_B, a function

$$\lambda : I_A \times I_B \times O_A \times O_B \to \{0, 1\},$$

often called the *rules* or *verification function*, and a **prior distribution** (or distribution for short) on input pairs, i.e.,

$$\pi : I_A \times I_B \longrightarrow [0,1],$$

with $\sum_{x,y} \pi(x,y) = 1$. Throughout, we let

$$W := \{(x,y,a,b) : \lambda(x,y,a,b) = 1\},$$

be the set of *correct* or *winning* 4-tuples and

$$N := \{(x,y,a,b) : \lambda(x,y,a,b) = 0\},$$

be the set of *incorrect* or *losing* 4-tuples. We sometimes refer to N as the *null set*. Each *round* of the game consists of Alice and Bob receiving an input pair (x,y) with probability $\pi(x,y)$ and returning an output pair (a,b). Thus, a game G is specified by $(I_A, I_B, O_A, O_b, \lambda, \pi)$.

Intuitively, if Alice and Bob have some *strategy* for such a game, then it would yield a **conditional probability density**[1],

$$p(a,b|x,y),\ x \in I_A,\ y \in I_B,\ a \in O_A,\ b \in O_B,$$

which gives the conditional probability that Alice and Bob return output pair (a,b), given that they received input pair (x,y).

A *deterministic strategy* corresponds to a pair of functions, $f_A : I_A \rightarrow O_A$ and $f_B : I_B \rightarrow O_B$ such that any time Alice and Bob receive input pair (x,y) they reply with output pair $(a,b) =$

[1] Some authors refer to conditional probability densities as correlations.

$(f_A(x), f_B(y))$. In this case $p(a, b|x, y)$ is always 0 or 1.

We often use **density** to refer to conditional probability density. We generally identify strategies with the conditional densities that they produce. Since $0 \leq p(a, b|x, y) \leq 1$, $\forall a, b, x, y$, it is natural to identify densities with points in the m-cube, $[0, 1]^m$ where $m = n_A n_B k_A k_B$ is the product of the cardinalities, $n_A = |I_A|$, $n_B = |O_B|$, $k_A = |O_A|$, $k_B = |O_B|$.

A strategy p is called *non-signaling* if

- for every $a \in O_A, x \in I_A$ and $y, y' \in I_B$ we have

$$\sum_b p(a, b|x, y) = \sum_b p(a, b|x, y'),$$

- for every $b \in O_B, y \in I_B$ and $x, x' \in I_A$ we have

$$\sum_a p(a, b|x, y) = \sum_a p(a, b|x', y).$$

Intuitively, this is a restatement of the nonlocality condition that states that Alice's answer is not dependent on Bob's question and vice versa. Every strategy in this paper is non-signalling. For a density $p(a, b|x, y)$ we denote Alice's marginal density by p_A. This is defined to be $p_A(a|x) = \sum_b p_A(a, b|x, y)$ where y is any question for Bob (the choice of y does not matter because p is non-signalling). One can similarly define Bob's marginal density p_B.

In a two-player nonlocal game, the probability of winning, i.e., the *expected value* of a given strategy $p(a, b|x, y)$ is given by

$$\begin{aligned} \omega(G, \pi, p) &= \sum_{x,y,a,b} \pi(x, y)\lambda(x, y, a, b)p(a, b|x, y) \\ &= \sum_{(x,y,a,b)\in W} \pi(x, y)p(a, b|x, y). \end{aligned}$$

Given a set S of conditional probability densities the **S-value** of the pair (G, π) is

$$\omega_S(G, \pi) := \sup\{\omega(G, \pi, p) : p \in S\}.$$

Identifying $S \subseteq [0, 1]^m$, since the value is clearly a convex function of p, the value will always be attained at one of the extreme points of the closed convex hull of S.

There are many sets of conditional probability densities for which researchers attempt to compute the S-value. Among these, in particular, are the **local, quantum**, and **quantum commuting** densities, denoted by

$$C_{loc}(n_A, n_B, k_A, k_B), C_q(n_A, n_B, k_A, k_B), \text{ and } C_{qc}(n_A, n_B, k_A, k_B),$$

respectively. We refer to [59, 60] for the precise definitions of these sets. To simplify notation, we generally suppress the set sizes. For fixed numbers of inputs and outputs these are convex sets, with C_{loc} and C_{qc} closed, while C_q is not generally closed. In fact, in [119] it was shown that $C_q(n, n, k, k)$ is not closed for all $n \geq 5, k \geq 2$. The closure of C_q is often denoted by C_{qa}. These sets satisfy

$$C_{loc} \subseteq C_q \subseteq C_{qa} \subseteq C_{qc}.$$

We remark that C_{loc} is a convex polytope whose extreme points are generated by the $\{0,1\}$ densities arising from deterministic strategies.

To simplify notation, we set

$$\omega_t(G,\pi) = \omega_{C_t}(G,\pi),\ \ t = loc, q, qa, qc.$$

Note that, since the value is a convex function of the densitiy, we have that

$$\omega_{loc}(G,\pi) = \sup \left\{ \sum_{\substack{x,y \\ (x,y,f_A(x),f_B(y))\in W}} \pi(x,y) \right\},$$

where the supremum is over all pairs of functions $f_A : I_A \to O_A,\ f_B : I_B \to O_B$.

Also, since the value is a continuous function of the density, we have $\omega_q(G,\pi) = \omega_{qa}(G,\pi)$. An often interesting question for $\omega_q(G,\pi)$ is whether or not the value is actually attained by an element of C_q. For $t = loc, qa, qc$ the value is always attained, since the corresponding sets of densities are closed and hence compact.

Computing these values for various games generated a great deal of interest in the operator algebras community when it was shown by [124] that if *Connes' embedding problem* had an affirmative answer, then

$$\omega_q(G,\pi) = \omega_{qc}(G,\pi),$$

for all games and densities.

Recently, [14] proved the existence of a game for which

$$\omega_q(G,\pi) < 1/2 < \omega_{qc}(G,\pi) = 1,$$

thus refuting Connes' embedding problem.

4.2.1 Synchronous Games

The games that we shall be interested in have the property that Alice and Bob's question sets and answer sets are the same, i.e., $I_A = I_B =: I$ and $O_A = O_B =: O$. So such a game is given as $G = (I, O, \lambda, \pi)$. If $n = |I|$ and $k = |O|$, then we say that the game has n inputs and k outputs and write $C_t(n, k)$, $t = loc, q, qc$ for the corresponding sets of densities.

For such games it is natural to impose some conditions on λ. We call G **synchronous** if

$$\lambda(x, x, a, b) = 0, \ \forall a \neq b,$$

i.e., if Alice and Bob are asked the same question they must give the same reply, although their answer to this question could vary with rounds. The game constructed in [14] that refutes the embedding problem is synchronous.

We call a game **symmetric** if

$$\lambda(x, y, a, b) = \lambda(y, x, b, a),$$

so that interchanging Alice and Bob has no effect on the rules.

In addition to imposing these conditions on the rules of a game, it is natural to impose them on the allowed densities. A density $p(a, b|x, y)$ is called **synchronous** if

$$p(a, b|x, x) = 0, \ \forall a \neq b.$$

We let $C_t^s(n,k) \subseteq C_t(n,k),\ t = loc, q, qc$ denote the corresponding subsets of synchronous densities.

Given a game $G = (I, O, \lambda, \pi)$, we set

$$\omega_t^s(G,\pi) = \omega_{C_t^s}(G,\pi),\ t = loc, q, qc.$$

These are the values that we are interested in computing in this paper.

In [58], which introduced the concept of synchronous games and densities, and [60] each of the sets $C_t^s(n,k), t = loc, q, qa, qc$ were characterized in terms of traces.

Given a C*-algebra $\mathcal{A}$ with unit, by a **trace** on $\mathcal{A}$ we mean a linear functional $\tau : \mathcal{A} \to \mathbb{C}$ satisfying $\tau(I) = 1,\ p \geq 0 \implies \tau(p) \geq 0$ and $\tau(xy) = \tau(yx)$. The first two conditions characterize **states** on $\mathcal{A}$. When $\mathcal{A} = M_m$, the set of $m \times m$ matrices, it is known that there is a unique trace, namely,

$$tr_m((a_{i,j})) = \frac{1}{m}\sum_i a_{i,i} = \frac{1}{m}Tr((a_{i,j})).$$

Given a C*-algebra $\mathcal{A}$ with unit I, a **k-outcome projection valued measure(k-PVM)** is a set of k projections, $E_a = E_a^2 = E_a^*$ such that $\sum_{a=0}^{k-1} E_a = I$. A family of n k-PVM's is a set of projections $\{E_{x,a} : 1 \leq x \leq n, 0 \leq a \leq k-1\}$ with $\sum_a E_{x,a} = I, \forall x$.

The following is a restatement of the results of [58] and [60] characterizing elements of $C_t^s(n,k)$ in terms of traces.

Theorem 4.2.1 ([58, 60]). *We have that $p \in C_{qc}^s(n,k)$ if and only if there is a family of n k-outcome PVM's $\{E_{x,a} : 1 \leq x \leq n, 0 \leq a \leq k-1\}$ in a unital C*-algebra $\mathcal{A}$ with a trace τ such* *that*

$$p(a, b|x, y) = \tau(E_{x,a}E_{y,b}).$$

Moreover,

- $p \in C^s_{loc}(n, k)$ *if and only if* $\mathcal{A}$ *can be taken to be abelian,*

- $p \in C^s_q(n, k)$ *if and only if* $\mathcal{A}$ *can be taken to be finite dimensional,*

- $p \in C^s_{qa}(n, k)$ *if and only if* $\mathcal{A}$ *can be taken to be an ultrapower of the hyperfinite* II_1*-factor.*

Let $\mathcal{A}$ be a C*-algebra and τ a trace. Let $\pi_\tau : \mathcal{A} \longrightarrow B(H)$ be the corresponding GNS representation and $h \in H$ the GNS state. We say that τ is of **type loc** if $\pi_\tau(\mathcal{A})$ is abelian. We say that τ is of **type q** if $\pi_\tau(\mathcal{A})$ is finite dimensional. We say that τ is of **type qa** if τ is *amenable* in the sense of [60, Definition 3.1]. By the preceding theorem, together with [60, Theorem 3.2], whenever $\{E_{x,a}\}$ are PVM's in a fixed C*-algebra $\mathcal{A}$ and τ is a trace on $\mathcal{A}$, then $p(a, b|x, y) = \tau(E_{x,a}E_{y,b})$ defines a density $p \in C^s_{loc}(n, k)$ (resp., $C^s_q(n, k), C^s_{qa}(n, k)$) whenever τ is of type $t = loc$ (resp. $t = q, t = qa$).

Note that if $p(a, b|x, y)$ is a synchronous density, then

$$p(a, b|x, y) = \tau(E_{x,a}E_{y,b}) = \tau(E_{y,b}E_{x,a}) = p(b, a|y, x).$$

In other words every synchronous density is **symmetric**.

The above result translates into the following result about synchronous values.

Theorem 4.2.2. *Let* $G = (I, O, \lambda, \pi)$ *be an n input k output game. Then*

1.

$$\omega^s_{loc}(G,\pi) = \sup\left\{ \sum_{\substack{x,y \\ (x,y,f(x),f(y))\in W}} \pi(x,y) \right\},$$

where the supremum is over all functions, $f : I \to O$ from inputs to outputs,

2.

$$\omega^s_q(G,\pi) = \omega^s_{qa}(G,\pi) = \sup\left\{ \sum_{(x,y,a,b)\in W} \pi(x,y) tr_m(E_{x,a}E_{y,b}) \right\},$$

where the supremum is over all families of n k-PVM's in M_m and over all m,

3.

$$\omega^s_{qc}(G,\pi) = \sup\left\{ \sum_{(x,y,a,b)\in W} \pi(x,y)\tau(E_{x,a}E_{y,b}) \right\},$$

where the supremum is over all unital C-algebras $\mathcal{A}$, traces τ, and families of n k-PVM's in $\mathcal{A}$.*

As we remarked earlier, the second supremum may not be attained.

4.2.2 A Universal C*-algebra Viewpoint

We let $\mathbb{F}(n,k)$ denote the group that is the free product of n copies of the cyclic group of order k. The full C*-algebra of this group $C^*(\mathbb{F}(n,k))$ is generated by n unitaries u_x, $1 \le x \le n$ each of order k, i.e., $u_x^k = I$. Given any unital C*-algebra $\mathcal{A}$ with n unitaries $U_x \in \mathcal{A}, 1 \le x \le n$ of order k, there is a *-homomorphism from $C^*(\mathbb{F}(n,k))$ mapping $u_x \to U_x$. If we decompose each u_x in terms of its spectral projections,

$$u_x = \sum_{a=0}^{k-1} \alpha^a e_{x,a},$$

where $\alpha = e^{2\pi i/k}$, then $\{e_{x,a} : 1 \leq x \leq n, 0 \leq a \leq k-1\}$ is a universal family of n k-PVM's, in the sense that given any set of n k-PVM's $\{E_{x,a}\}$ in a unital C*-algebra $\mathcal{A}$, there is a unital *-homomorphism from $C^*(\mathbb{F}(n,k))$ to $\mathcal{A}$ sending $e_{x,a} \to E_{x,a}$.

Values of games can be interpreted in terms of properties of the maximal and minimal C*-tensor product of this algebra with itself.

It follows from the work of [124](see also [125]) that

- $p(a,b|x,y) \in \overline{C_q(n,k)} = C_{qa}(n,k)$ if and only if there exits a state

  $$s : C^*(\mathbb{F}(n,k)) \otimes_{min} C^*(\mathbb{F}(n,k)) \to \mathbb{C}$$

  such that

  $$p(a,b|x,y) = s(e_{x,a} \otimes e_{y,b}),$$

- $p(a,b|x,y) \in C_{qc}(n,k)$ if and only if there exists a state

  $$s : C^*(\mathbb{F}(n,k)) \otimes_{max} C^*(\mathbb{F}(n,k)) \to \mathbb{C}$$

  such that

  $$p(a,b|x,y) = s(e_{x,a} \otimes e_{y,b}).$$

Given a game G and prior distribution π we set

$$P_{G,\pi} = \sum_{(x,y,a,b)\in W} \pi(x,y) e_{x,a} \otimes e_{y,b}.$$

Using the fact that norms of positive elements are attained by taking the supremum over states, we have:

Proposition 4.2.3. *Given an n input, k output game $G = (I, O, \lambda, \pi)$,*

$$\omega_q(G, \pi) = \|P_{G,\pi}\|_{C^*(\mathbb{F}(n,k)) \otimes_{min} C^*(\mathbb{F}(n,k))},$$

and

$$\omega_{qc}(G, \pi) = \|P_{G,\pi}\|_{C^*(\mathbb{F}(n,k)) \otimes_{max} C^*(\mathbb{F}(n,k))}.$$

The example of [14] gave the first proof that the minimal and maximal norms are different. Similar results to Proposition 4.2.3 can be found in Section 4.1 of [126] where the value of a game is described as the norm of an operator in a tensor product of operator spaces.

We now turn to the synchronous case. The element $e_{x,a}e_{y,b}$ is not positive, but for any trace we have that

$$\tau(e_{x,a}e_{y,b}) = \tau(e_{x,a}e_{y,b}e_{x,a}),$$

and $e_{x,a}e_{y,b}e_{x,a} \geq 0$.

We set

$$R_{G,\pi} = \sum_{(x,y,a,b) \in W} \pi(x, y) e_{x,a}e_{y,b}e_{x,a}.$$

We also set $C \subseteq C^*(\mathbb{F}(n, k))$ equal to the closed linear span of all commutators, $xy - yx$.

Given any C*-algebra $\mathcal{A}$ we let $T(\mathcal{A})$ denote the set of traces on $\mathcal{A}$ and let $T_{fin}(\mathcal{A})$ denote the set of traces that *factor through matrix algebras,* i.e., are of the form

$$\tau(a) = tr_m(\pi(a)),$$

for some m and some unital *-homomorphism $\pi : \mathcal{A} \to M_m$.

Theorem 4.2.4. *Let $G = (I, O, \lambda, \pi)$ be an n input, k output game. Then*

1.

$$\omega^s_{qc}(G, \pi) = \sup\{\tau(R_{G,\pi}) : \tau \in T(C^*(\mathbb{F}(n, k))\}$$

$$= \inf\{\|R_{G,\pi} - C\| : C \in \mathcal{C}\},$$

2.

$$\omega^s_q(G, \pi) = \sup\{\tau(R_{G,\pi}) : \tau \in T_{fin}(C^*(\mathbb{F}(n, k))\}.$$

Two of the equalities are direct applications of the above facts. The equality of the value with the distance to the space of commutators follows from [127, Theorem 2.9] where it is shown that for positive elements of a C*-algebra, the supremum over all traces is equal to the distance to the space $\mathcal{C}$.

For the example of a game constructed in [14], it is known that

$$\omega^s_q(G, \pi) < 1/2 < \omega^s_{qc}(G, \pi) = 1,$$

and consequently, their results also give the first proof that $T_{fin}(C^*(\mathbb{F}(n, k))$ is not dense in $T(C^*(\mathbb{F}(n, k))$. Perhaps even more remarkable is that this difference is witnessed by the element $R_{G,\pi}$ for some game, which only involves words in the generators of order three. However, the game of [14] is mostly given implicitly and estimates on the values of n and k to achieve their example are very large.

In summary, we see that the theory of values and synchronous values of these games gives us interesting information about C*-algebras. Thus, we are led to study these values for interesting sets of games.

4.3 The Graph Colouring Game

In this section we study the synchronous value of the game we get by trying to colour the vertices of a graph using c-colours, especially when c is smaller than the least number of colours needed for an actual colouring. By a graph we mean a pair $G = (V, E)$, where V denotes the vertices and $E \subseteq V \times V$ denotes the edge set. Our graphs are undirected, i.e., $(x, y) \in E \implies (y, x) \in E$ and loopless, i.e., $(x, x) \notin E$. A *c-colouring* is any function $f : V \to \{1, ..., c\}$ such that $(x, y) \in E$ implies that $f(x) \neq f(y)$.

Note that since $(x, y) \in E \implies (y, x) \in E$, and these both represent the same edge, then the cardinality of the set E is equal to twice the number of edges.

Before recalling the graph colouring game it helps to recall the **graph homomorphism game**.

Given two graphs $G_i = (V_i, E_i)$ a *graph homomorphism* is a function $f : V_1 \to V_2$ such that $(x, y) \in E_1 \implies (f(x), f(y)) \in E_2$. If we let K_c denote the complete graph on c vertices, then a c-colouring of G is just a graph homomorphism from G to K_c.

The **graph homomorphism game,** $Hom(G_1, G_2)$ is the synchronous game with inputs $I = V_1$, outputs $O = V_2$ and rule $\lambda : V_1 \times V_1 \times V_2 \times V_2 \to \{0, 1\}$ with null set

$$N = \{(x, y, a, b) : (x, y) \in E_1,\ (a, b) \notin E_2\} \cup \{(x, x, a, b) : x \in V_1,\ a \neq b\}.$$

Note that λ is symmetric.

The **graph c-colouring game** is the game $Hom(G, K_c)$. We use $\{1, ..., c\}$ for the vertex set of K_c. We also usually assume that $c < \chi(G)$ (where $\chi(G)$ is the chromatic number of G) since otherwise

$$\omega_t^s(Hom(G, K_c)) = 1, \text{ for } t = loc, q, qa, qc.$$

4.3.1 The Relation Between Max c-Cut and the Synchronous Local Value

Given a graph $G = (V, E)$ the *max c-cut* of G, is the maximum number of edges that can be coloured “correctly" using c-colours, i.e.,

$$Cut_c(G) := \frac{\max\{|\{(x, y) \in E : x \in S_i,\ y \in S_j,\ i \neq j\}|\}}{2},$$

where the maximum is over all partitions of V into c disjoint subsets, $S_1, ..., S_c$ and the absolute value signs denote cardinality. Equivalently, a partition into c disjoint subsets is defined by a function $f : V \to \{1, ..., c\}$ with $S_i = f^{-1}(\{i\})$, so that

$$Cut_c(G) = \frac{\max\{|\{(x, y) \in E : f(x) \neq f(y)\}|\}}{2},$$

where now the maximum is over all functions. Note that G has a c-colouring precisely when $\frac{|E|}{2} = Cut_c(G)$.

The max 2-cut is generally referred to as simply the max cut. Computing the max cut is known to be NP-hard [128].

The following result shows that from the point of view of max cut problems, the synchronous value of the graph colouring game is more meaningful.

Proposition 4.3.1. *Let $G = (V, E)$ be a graph on n vertices and let $Hom(G, K_c)$ be the graph c-colouring game and let π be the uniform density on E. Then*

$$\omega_{loc}^{s}(Hom(G, K_c), \pi) = \frac{2Cut_c(G)}{|E|}.$$

Proof. Each synchronous deterministic strategy corresponds to a function $f : V \to \{1, ..., c\}$. The number of input pairs for which this strategy will win is equal to $2Cut_c(G)$ and the result follows. □

In contrast, one can see that $\omega_{loc}(Hom(G, K_c), \pi)$ is related to the max c-cut of a bipartite graph over G, since Alice and Bob are allowed different functions for their deterministic strategy. Given a graph $G = (V, E)$ we define a new graph $G_b = (V_b, E_b)$ with $V_b = V \times \{0, 1\}$ and $((x, i), (y, j)) \in E_b$ if and only if $i \neq j$ and $(x, y) \in E$. This graph is the usual bipartite graph defined over G.

Proposition 4.3.2. *Let $G = (V, E)$ be a graph, let $G_b = (V_b, E_b)$ be the bipartite graph defined over G as above, and consider the c-colouring game with π the uniform probability density on E. Then*

$$\omega_{loc}(Hom(G, K_c), \pi) = \frac{Cut_c(G_b)}{|E|}.$$

Proof. Each deterministic strategy is given by a pair of functions $f, g : V \to \{1, ..., c\}$. Such pairs of functions are in one-to-one correspondence with functions $F : V_b \to \{1, ..., c\}$ by setting $f(x) = F((x, 0))$ and $g(x) = F((x, 1))$.

The number of times that this strategy will win is equal to

$$|\{(x,y) \in E : f(x) \neq g(y)\}| = |\{((x,0),(y,1)) \in E_b : F(x,0) \neq F(y,1)\}|.$$

Note that when we chose f, g to maximize this number, we are obtaining $Cut_c(G_b)$ the actual number of edges since we are not counting ordered pairs of the form $((x,1),(y,0))$, and the result follows. □

Thus, there is a clean relationship between the synchronous local value of the graph colouring game and the cut numbers, while the usual local value is related to the cut numbers of the bipartite graph constructed from the original graph. This relationship makes it natural to define *quantum cut numbers of graphs* as follows.

Definition 4.3.3. Given a graph $G = (V, E)$, a natural number $c \geq 2$ and for $t \in \{q, qc\}$ we define the *t-quantum max c-cut number of G* to be

$$Cut_{t,c}(G) = \frac{|E|}{2} \cdot \omega_t^s(Hom(G, K_c), \pi),$$

where π is the uniform density on E.

Using our characterizations of these synchronous values, we have that for a graph $G = (V, E)$

on n vertices,

$$\begin{aligned}
Cut_{qc,c}(G) &= \frac{1}{2}\sup\left\{\sum_{(x,y)\in E, a\neq b}\tau(e_{x,a}e_{y,b}) : \tau \in T(C^*(\mathbb{F}(n,c))\right\} \\
&= \frac{|E|}{2} - \frac{1}{2}\inf\left\{\sum_{(x,y)\in E}\sum_{a=1}^{c}\tau(e_{x,a}e_{y,a}) : \tau \in T(C^*(\mathbb{F}(n,c))\right\} \\
&= \frac{1}{2}\inf\left\{\|\sum_{(x,y)\in E, a\neq b} e_{e,a}e_{y,b} - C\| : C \in C\right\},
\end{aligned}$$

while

$$\begin{aligned}
Cut_{q,c}(G) = \frac{1}{2}\sup_{m}\left\{\sum_{(x,y)\in E, a\neq b} tr_m(E_{x,a}E_{y,b}) : \{E_{x,a}\} \text{ an (n,c)-PVM in } M_m\right\} \\
= \frac{|E|}{2} - \frac{1}{2}\inf_{m}\left\{\sum_{(x,y)\in E}\sum_{a=1}^{c} tr_m(E_{x,a}E_{y,a}) : \{E_{x,a}\} \text{ an (n,c)-PVM in } M_m\right\},
\end{aligned}$$

where tr_m denotes the normalized trace on M_m.

In a later section on XOR games we show that $Cut_{q,2}(G) = Cut_{qc,2}(G)$ and that this value is given by an SDP. There is a significant body of literature of semidefinite relaxations of max cut, for an introduction see [123].

4.3.2 The Graph Correlation Function

This function, with a slightly different notation, was introduced and studied in [119] where it was used to give a proof of the non-closure of $C_q^s(n,k)$ for all $n \geq 5, k \geq 2$. Given any graph $G = (V, E)$ and a C*-algebra with a trace $(\mathcal{A}, \tau)$ and a set of projections, $P_x \in \mathcal{A}$, $x \in V$, then the

correlation of these projections is

$$\sum_{(x,y)\in E} \tau(P_x P_y).$$

Then for each $t \in \{loc, q, qa, qc\}$ the **graph correlation function** $f_{G,t}(r)$ is defined as:

$$f_{G,t}(r) = \inf\left\{ \sum_{(x,y)\in E} \tau(P_x P_y) : \tau(P_x) = r, \forall x \in V \right\},$$

where the infimum is over all sets of projections $\{P_x : x \in V\}$ in the C*-algebra and all traces of type t. Note that the C*-algebra is fixed and the optimization is over choices of projections and traces. So clearly,

$$0 \le f_{G,qc}(r) \le f_{G,qa}(r) = f_{G,q}(r) \le f_{G,loc}(r),$$

and there will exist projections and traces of type t attaining these values except, possibly, in the case q.

In [119], it was shown that for the complete graph on 5 vertices, K_5, the value of the function $f_{K_5,q}(r)$ is not attained for any irrational value of r in a certain interval, which was then shown to imply that $C_q(5,2)$ is not closed.

In [58] it was shown that if we set

$$r_{G,t} = \sup\{r : f_{G,t}(r) = 0\},$$

then

$$r_{G,t}^{-1} \le \chi_t(G),$$

where these *quantum chromatic numbers* $\chi_t(G)$ of type $t \in \{loc, q, qa, qc\}$ is the least value of c

for which there exists a perfect strategy of type t for the graph c-colouring game. In [58] it is also shown that $r^{-1}_{G,loc}$ is equal to the fractional chromatic number of the graph G, while $r^{-1}_{G,q}$ agrees with the quantum fractional chromatic number introduced by D. Roberson [35].

In [119] it is shown that if the infimum of the graph correlation function is attained by a set of projections $\{P_x : x \in V\}$, then for each $x \in V$, P_x commutes with $\sum_{y:(x,y)\in E} P_y$. In Section 7, we adapt their technique to obtain relations that must be satisfied by the projections that attain the synchronous value for other games.

We continue our study of the synchronous values of the c-colouring game by obtaining estimates in terms of the graph correlation function, which we will show are sharp for the case $c = 2$.

4.3.3 The Uniform Synchronous Density

The uniform distribution for n inputs and c outputs is given by $p(a, b|x, y) = 1/c^2$, but this density is not synchronous. We wish to introduce a synchronous analogue.

The **uniform synchronous density on** n **inputs and** c **outputs** is given by the formula,

$$p(a, b|x, y) = \begin{cases} 1/c^2, & x \neq y, \\ 1/c, & x = y, a = b, \\ 0, & x = y, a \neq b. \end{cases}$$

Proposition 4.3.4. *The uniform synchronous density on n inputs and c outputs is a local density, i.e., is in $C^s_{loc}(n, c)$.*

Proof. Let $S = \{(a_1, ..., a_n) : 0 \leq a_i \leq c - 1,\ a_i \in \mathbb{Z}\}$ and define $S_{x,a} \subseteq S$ to be the n-tuples that are equal to a in the x-th coordinate. Note that $\cup_{a=0}^{c-1} S_{x,a} = S$. Consider the uniform distribution P

on S so that each point has probability $\frac{1}{|S|} = \frac{1}{c^n}$.

On question pair (x, y), Alice and Bob, using classical shared randomness, sample a tuple $(a_1, ..., a_n)$ from S according to P. Alice responds with a_x and Bob responds with a_y. This classical strategy generates the synchronous local density given by

$$p(a, b|x, y) = \int_S \chi_{S_{x,a}} \chi_{S_{y,b}} dP = \frac{|S_{x,a} \cap S_{y,b}|}{c^n},$$

where χ_T denotes the characteristic function of the set T. It is easily checked that this is the uniform synchronous density. □

Somewhat surprisingly, another representation of the uniform synchronous density is given by the canonical trace on the free group $\mathbb{F}(n, c)$. Recall that the canonical trace on the algebra of a group $\mathbb{C}(G)$ is given by setting $\tau(u_e) = 1$, where e is the group identity, so that u_e is the identity of $\mathbb{C}(G)$ and $\tau(u_g) = 0, \forall g \neq e$, and extending linearly. If $U_1, ..., U_n$ are the order c unitaries that generate $\mathbb{F}(n, c)$, then the canonical projections are given by

$$e_{x,a} = \frac{1}{c} \sum_{j=0}^{c-1} \alpha^{-aj} U_x^j,$$

where $\alpha = e^{2\pi i/c}$. Thus, $\tau(e_{x,a}) = 1/c$. These projections and the canonical trace yield a synchronous density

$$p(a, b|x, y) = \tau(e_{x,a} e_{y,b}),$$

which is easily seen to be the uniform synchronous density. It is somewhat remarkable that the trace arising from this free non-abelian group agrees on the generators, up to order two, with a trace arising from an abelian setting.

This density gives us a bound on the graph correlation function.

Proposition 4.3.5. *Let $G = (V, E)$be a graph on n vertices. Then*

$$f_{G,loc}(1/c) \leq \frac{|E|}{c^2}.$$

Proof. Let $E_{x,a}$ be the projections yielding the uniform synchronous density, then we have that

$$f_{G,loc}(1/c) \leq \sum_{(x,y)\in E} \tau(E_{x,1}E_{y,1}) = \frac{|E|}{c^2}.$$

□

Theorem 4.3.6. *Let $G = (V, E)$ be a graph on n vertices and consider the c-colouring game $Hom(G, K_c)$ played with the uniform distribution π on E. Then for $t \in \{loc, q, qc\}$,*

$$max \left\{1 - \frac{1}{c},\ 1 - \frac{2}{|E|} f_{G,t}(1/2)\right\} \leq \omega_t^s(Hom(G, K_c), \pi) \leq 1 - \frac{c}{|E|} f_{G,t}(1/c). \tag{4.3.1}$$

Proof. First, assume that our density is synchronous so that there exist PVM's $\{E_{x,a} : 0 \leq a \leq c-1\}$ such that $p(a, b|x, y) = \tau(E_{x,a}E_{y,b})$ for some C*-algebra and trace $\tau : \mathcal{A} \to \mathbb{C}$ of type t. Then we have that

$$\sum_{a=0}^{c-1} \sum_{(x,y)\in E} p(a, a|x, y) \quad = \quad \sum_{(x,y)\in E} \sum_{a=0}^{c-1} \tau(E_{x,a}E_{y,a}) \quad = \quad c \sum_{(x,y)\in E} \tau^{(c)}(P_x P_y), \tag{4.3.2}$$

where we set $\mathcal{A}^{(c)} = \mathcal{A} \oplus \cdots \oplus \mathcal{A}$ (c times) and let $\tau^{(c)} : \mathcal{A}^{(c)} \to \mathbb{C}$ be the unital trace $\tau^{(c)}(X_0 \oplus \cdots \oplus X_{c-1}) = \sum_{a=0}^{c-1} \tau(X_a)/c$ and let $P_x = E_{x,0} \oplus \cdots \oplus E_{x,c-1}$. Note that in this case, for every x, we have that

$$\tau^{(c)}(P_x) = \sum_{a=0}^{c-1} \tau(E_{x,a})/c = 1/c.$$

This proves that

$$\omega_t^s(Hom(G, K_c), \pi) \leq 1 - \frac{c}{|E|} f_{G,t}(1/c).$$

For the other inequality, we see that the value of any synchronous density $p(a, b|x, y) \in C_t^s(n, k)$ is given by

$$\omega(Hom(G, K_c), \pi, p) = 1 - \frac{1}{|E|} \sum_{a=0}^{c-1} \sum_{(x,y) \in E} p(a, a|x, y).$$

If we use the uniform synchronous density, then this becomes,

$$1 - \frac{1}{|E|} \sum_{a=0}^{c-1} \sum_{(x,y) \in E} 1/c^2 = 1 - \frac{1}{c}.$$

Now suppose that we are given projections, $\{P_x : x \in V\} \subseteq \mathcal{A}$ and a trace τ of type t with $\tau(P_x) = 1/2$. Then we set $E_{x,0} = P_x$, $E_{x,1} = I - P_x$ and $E_{x,a} = 0$, $a \neq 0, 1$. For the corresponding synchronous correlation, we have that

$$\begin{aligned} 1 - \omega_t^s(Hom(G, K_c), \pi) &\leq \frac{1}{|E|} \sum_{(x,y) \in E} \sum_a \tau(E_{x,a} E_{y,a}) \\ &= \frac{1}{|E|} \sum_{(x,y) \in E} \tau(P_x P_y + (I - P_x)(I - P_y)) \\ &= \frac{1}{|E|} \sum_{(x,y) \in E} \tau(2P_x P_y + I - P_x - P_y) \\ &= \frac{2}{|E|} \sum_{(x,y) \in E} \tau(P_x P_y), \end{aligned}$$

and the other inequality follows. □

Corollary 4.3.7. *Let G be a graph on n vertices. Then for the 2-colouring game, with uniform distribution π on E, we have that*

$$\omega_t^s(Hom(G, K_2), \pi) = 1 - \frac{2}{|E|} f_{G,t}(1/2).$$

In particular, $\omega_q^s(Hom(G, K_2), \pi) = \omega_{qc}^s(Hom(G, K_2), \pi)$ and $Cut_{q,2}(G) = \frac{|E|}{2} - f_{G,q}(1/2)$.

Proof. The first result follows from the above inequalities. The second follows from [119, Proposition 3.10] where it is shown that for any graph, $f_{G,q}(1/2) = f_{G,qc}(1/2)$. □

There are similar inequalities, with different constants, for each of the three types of densities discussed at the beginning of the section.

In general for $c \neq 2$, we do not expect that the upper bound is sharp. For example, suppose that we had a graph such that

$$r_{G,t}^{-1} \leq c < \chi_t(G).$$

Then $f_{G,t}(1/c) = 0$, but since $c < \chi_t(G)$ there is no perfect t-strategy and hence,

$$\omega_t^s(Hom(G, K_c), \pi) < 1 = 1 - \frac{c}{n^2} f_{G,t}(1/c).$$

Unfortunately, we do not know an example of a graph with this particular separation, so we cannot say definitely that $\omega_t^s(Hom(G, K_c), \pi) \neq 1 - \frac{c}{n^2 f_{G,t}(1/c)}$, for some c.

It is a consequence of Tsirelson's work that for any graph $f_{G,q}(1/2) = f_{G,qc}(1/2)$, this is mentioned in [119] and we provide another proof in Section 4.4. Consequently, for the uniform distribution π,

$$\omega_q^s(Hom(G,K_2),\pi) = \omega_{qc}^s(Hom(G,K_2),\pi).$$

In fact, Tsirelson's work tells us quite a bit more in the 2-colouring case, since 2-colouring games, with appropriately chosen distributions on questions, belong to a family of games known as XOR games, which is the topic of our next section.

First, we consider the value of the game of c-colouring a complete graph on n vertices when $n > c$.

4.3.4 c-Colouring the Complete Graph on n Vertices

We now turn our attention to the case that $G = K_n$. We begin by computing the graph correlation function in this case. In addition to the graph correlation functions, $f_{G,t}(r), t = loc, q, qc$, the paper [119] also introduces a function $f_{G,vect}(r)$ that satisfies, $f_{G,vect}(r) \leq f_{G,qc}(r)$. We use this fact in the proof of the following theorem.

Theorem 4.3.8. *For the complete graph K_n, $n \geq 5$ and $\frac{n-\sqrt{n^2-4n}}{2n} \leq r \leq \frac{n+\sqrt{n^2-4n}}{2n}$ we have that*

$$f_{K_n,q}(r) = f_{K_n,qc}(r) = nr(nr-1).$$

Proof. In [119, Proposition 4.1] it is shown that for the complete graph $f_{K_n,vect}(r) = nr(nr-1)$ for $\frac{1}{n} \leq r \leq \frac{n-1}{n}$. Note that $\frac{1}{n} \leq \frac{n-\sqrt{n^2-4n}}{2n}$ and $\frac{n+\sqrt{n^2-4n}}{2n} \leq \frac{n-1}{n}$.

In [129], it is proven that for any rational r in this smaller interval there exist n projection matrices in M_m for some m, $Q_x, 0 \leq x \leq n-1$ such that $\sum_{x=0}^{n-1} Q_x = (nr)I_m$. Let

$$P_x = \oplus_{j=0}^{n-1} Q_{j+x},$$

where the index is modulo n. Then $\sum_{x=0}^{n-1} P_x = (nr)I_{nm}$. Moreover, if we let τ denote the normalized trace on M_{mn} then $\tau(P_x) = r$ for every x. Thus we can write

$$nr(nr-1) = f_{K_n,vect}(r) \leq f_{K_n,qc}(r) \leq f_{K_n,q}(r) \leq \sum_{(x,y)\in E} \tau(P_x P_y).$$

Now notice that

$$\begin{aligned}\sum_{(x,y)\in E} \tau(P_x P_y) &= \sum_{x=0}^{n-1} \sum_{y\neq x} \tau(P_x P_y) \\ &= \sum_{x=0}^{n-1} \tau(P_x((nr)I_{nm} - P_x)) \\ &= \sum_{x=0}^{n-1} (nr-1)\tau(P_x) \\ &= nr(nr-1).\end{aligned}$$

The result follows by observing that the functions $f_q = f_{qa}$ and f_{qc} are continuous. □

4.4 Synchronous Values of XOR Games

In [21] quantum values of XOR games were studied extensively. In this section, we recall their results, study synchronous values of XOR games, explain how to calculate the synchronous values using semidefinite programming, and compare the two sets of results. Later, we will consider several specific examples of synchronous values of XOR games and study their properties. For XOR games the output set is always $\mathbb{Z}_2$.

Definition 4.4.1. A game $G = (I, \{0,1\}, \lambda)$ is an **XOR game** if there exists a function $f : I \times I \to \{0,1\}$ such that $\lambda(x,y,a,b) = 1$ if and only if $a \oplus b = f(x,y)$, where $a \oplus b$ denotes addition in the binary field.

Note that an XOR game is synchronous if and only if $f(x,x) = 0$ for all $x \in I$, and symmetric if and only if $f(x,y) = f(y,x)$.

Computing values of XOR games is especially straightforward, because of the following observation together with the Tsirelson's theory.

Proposition 4.4.2. *Let G be an XOR game with $|I| = n$ and prior distribution π, and let $t \in \{loc, qa, qc\}$. Then there exists a strategy $p \in C_t(n,2)$ such that $\omega_t(G,\pi) = \omega(G,\pi,p)$, where $p_A(0|x) = p_B(0|y) = 1/2$ for each $x, y \in I$.*

Proof. Since $C_t(n,2)$ is closed for each $t \in \{loc, qa, qc\}$, there exists $p \in C_t(n,2)$ such that $\omega_t(G,\pi) = \omega(G,\pi,p)$. Given such a density p, there exist a Hilbert space H, operators

$P_1, \ldots, P_n, Q_1, \ldots, Q_n \in B(H)$, and a unit vector $h \in H$ such that

$$p(0,0|x,y) = \langle P_x Q_y h, h\rangle$$

for each $x, y \in I$. For each $x \in I$, define $P_i' = P_i \oplus (I - P_i)$ and $h' = \frac{1}{\sqrt{2}}(h \oplus h)$. Let $p' \in C_t(n,2)$ be the unique density satisfying

$$p'(0,0|x,y) = \langle P_x' Q_y' h', h'\rangle$$

for each $x, y \in I$. Note that $p'(a, b|x, y) = \frac{1}{2}(p(a, b|x, y) + p(a \oplus 1, b \oplus 1|x, y))$. Then

$$\begin{aligned}
\omega(G, \pi, p) &= \sum_{x,y \in I, a,b \in \{0,1\}} \pi(x, y) p(a, b|x, y) \lambda(x, y, a, b) \\
&= \sum_{x,y \in I, a \oplus b = f(x,y)} \pi(x, y) p(a, b|x, y) \\
&= \sum_{x,y \in I, a \oplus b = f(x,y)} \pi(x, y) \frac{1}{2}(p(a, b|x, y) + p(a \oplus 1, b \oplus 1|x, y)) \\
&= \sum_{x,y \in I, a \oplus b = f(x,y)} \pi(x, y) p'(a, b|x, y) \\
&= \omega(G, \pi, p')
\end{aligned}$$

where we have used the fact that $a \oplus b = (a \oplus 1) \oplus (b \oplus 1)$. Since $p'_A(0|x) = p'_B(0|y) = 1/2$ and since $\omega_t(G, \pi) = \omega_t(G, \pi, p) = \omega_t(G, \pi, p')$, the statement is proven. □

Two-outcome densities satisfying $p_A(0|x) = p_B(0|y) = 1/2$ for all $x, y \in I$ are called **unbiased** densities in the literature. The following theorem is a restatement of Tsirelson's characterisation of quantum observables [130] in terms of unbiased densities. For those unfamiliar with the similarities and differences between quantum observables and quantum densities, see [131, Theorem 11.8].

Theorem 4.4.3 (Tsirelson). *Let $p(i, j|s, t)$ be a density such that $p_A(0|s) = p_B(0|t) = 1/2$ for all s, t. Then the following statements are equivalent:*

1. *$p(i, j|s, t) \in C_{qc}(n, 2)$.*

2. *There exist real unit vectors $x_s, y_t \in \mathbb{R}^m$ for $1 \leq s, t \leq n$ such that $p(i, j|s, t) = \frac{1}{4}(1 + (-1)^{i+j}\langle x_s, y_t \rangle)$.*

3. *$p(i, j|s, t) \in C_q(n, 2)$.*

A similar statement can be made in the synchronous case.

Theorem 4.4.4. *Let $p(i, j|s, t)$ be a synchronous density such that $p(0, 0|s, s) = p(1, 1|s, s)$ for all s. Then the following statements are equivalent:*

1. *$p(i, j|s, t) \in C^s_{qc}(n, 2)$.*
2. *There exist real unit vectors $x_s \in \mathbb{R}^m$ for $1 \leq s \leq n$ such that $p(i, j|s, t) = \frac{1}{4}(1 + (-1)^{i+j}\langle x_s, x_t\rangle)$.*
3. *$p(i, j|s, t) \in C^s_q(n, 2)$.*

Proof. Suppose the first statement is true. By Theorem 4.4.3, there exist unit vectors x_s, y_t for $1 \leq s, t \leq n$ such that $p(i, j|s, t) = \frac{1}{4}(1 + (-1)^{i+j}\langle x_s, y_t\rangle)$. Since $p(i, j|s, s) = 0$ whenever $i \neq j$, we have $\langle x_s, y_s\rangle = 1$ for every s. By Cauchy-Schwarz, $x_s = y_s$ for every s. The other implications are straightforward. □

Remark 4. *Given projections P_x in a C*-algebra with a trace $(\mathcal{A}, \tau)$ such that $\tau(P_x) = 1/2$, set $E_{x,0} = P_x$ and $E_{x,1} = I - P_x$. Then $\tau(E_{x,i}E_{y,j}) := p(i, j|x, y)$ is a density in C_{qc} with marginals equal to $1/2$. Hence by the above result $p(i, j|x, y) \in C_q$. Given a graph $G = (V, E)$, to compute $f_{G,qc}(1/2)$ we are minimizing*

$$\sum_{(x,y)\in E} \tau(P_x P_y) = \sum_{(x,y)\in E} p(0, 0|x, y),$$

over all sets of projections with $\tau(P_x) = 1/2$ and, hence, $f_{G,qc}(1/2) = f_{G,q}(1/2)$. This is essentially the proof given in [119, Proposition 3.10].

We will use the theorems above, together with Proposition 4.4.2, to calculate the values of certain XOR games. For now, we will only provide a general formulation for these values in terms of semidefinite programs.

Remark 5. *Let $G = (I, \{0,1\}, \lambda)$ be an XOR game with $n := |I|$, and suppose $f : I \times I \to \{0,1\}$ is a function satisfying $f(x,y) = a \oplus b$ if and only if $\lambda(x,y,a,b) = 1$ for all $a, b \in \{0,1\}$ and $x, y \in I$. Let $\pi(x,y)$ be a prior distribution on I, and let $\mathcal{G} = (G, \pi)$ denote the game G with questions asked according to the distribution π. Following [21], we define the matrix $A_{\mathcal{G}} \in M_n$ by $A_{\mathcal{G}} = ((-1)^{f(x,y)}\pi(x,y))$, which [21] call the* **cost matrix***. They also study a matrix*

$$B_{\mathcal{G}} := \frac{1}{2}\begin{pmatrix} 0 & A_{\mathcal{G}} \\ A_{\mathcal{G}}^T & 0 \end{pmatrix} \in M_{2n}.$$

For synchronous values, the matrix,

$$A_{\mathcal{G}}^s := \frac{1}{2}(A_{\mathcal{G}} + A_{\mathcal{G}}^T) \in M_n$$

plays a similar role to the cost matrix and we will refer to this matrix as the **symmetrized cost matrix**.

Let $\mathcal{E}_n \subseteq M_n$ denote the $n \times n$ **elliptope** defined by

$$\mathcal{E}_n := \{P \in M_n(\mathbb{R}) : diag(P) = I_n \text{ and } P \geq 0\}. \tag{4.4.1}$$

The following formula for the value of an XOR game is a restatement of results in [21]. The formula for the synchronous value is new.

Theorem 4.4.5. *Let $G = (I, \{0,1\}, \lambda, \pi)$ be an XOR game with $n := |I|$ and $\pi(x,y)$ a prior distribution on I. Then*

$$\omega_{qc}(G,\pi) = \omega_q(G,\pi) = \frac{1}{2} + \frac{1}{2}\max_{P\in\mathcal{E}_{2n}} Tr(B_{\mathcal{G}}P)$$

and

$$\omega^s_{qc}(G,\pi) = \omega^s_q(G,\pi) = \frac{1}{2} + \frac{1}{2}\max_{P\in\mathcal{E}_n} Tr(A^s_{\mathcal{G}}P).$$

Proof. Suppose $f : I \times I \to \{0,1\}$ is a function satisfying $f(x,y) = a \oplus b$ if and only if $\lambda(x,y,a,b) = 1$ for all $a, b \in \{0,1\}$.

We first consider the claim concerning $\omega_{qc}(G,\pi)$. By Proposition 4.4.2, there exists $p \in C_q(n,2)$ such that $\omega_{qc}(G,\pi) = \omega(G,\pi,p)$ and $p_A(0|x) = p_B(0|y) = 1/2$ for every $x, y \in I$. Since $\lambda(x,y,a,b) = 1$ if and only if $a \oplus b = f(x,y)$, we have that

$$\omega_{qc}(G,\pi) = \sum_{x,y\in I, a\oplus b = f(x,y)} \pi(x,y)p(a,b|x,y).$$

By Theorem 4.4.3 this implies

$$\begin{aligned}\omega_{qc}(G,\pi) &= \sum_{x,y\in I, a\oplus b=f(x,y)} \frac{1}{4}\pi(x,y)(1+(-1)^{a+b}\langle v_x, w_y\rangle) \\ &= \frac{1}{4}\left(\sum_{x,y\in I, a\oplus b=f(x,y)} \pi(x,y) + \sum_{x,y\in I}\pi(x,y)(-1)^{f(x,y)}\langle v_x, w_y\rangle\right)\end{aligned}$$

where the v_x's and w_y's are real unit vectors. Since every expression of the form $p(a,b|x,y) =$

$\frac{1}{4}(1 + (-1)^{a+b}\langle v_x, w_y\rangle)$ defines an element of $C_{qc}(n, 2)$, we have

$$\omega_{qc}(G, \pi) = \frac{1}{4}\left(\sum_{x,y \in I, a \oplus b = f(x,y)} \pi(x, y) + \max_{v_x, w_y} \sum_{x,y \in I} \pi(x, y)(-1)^{f(x,y)}\langle v_x, w_y\rangle \right)$$

where the maximization is over all sets of real unit vectors v_x and w_y. Since $\pi(x, y)$ is a probability distribution and $a \oplus b = f(x, y)$ for exactly two choices of pairs (a, b), we have that

$$\sum_{x,y \in I, a \oplus b = f(x,y)} \pi(x, y) = 2.$$

Also, notice that an $n \times n$ matrix has the form $(\langle v_x, w_y\rangle)_{x,y}$ for unit vectors v_x and w_y if and only if it is the upper right (or lower left) $n \times n$ corner of a matrix $P \in \mathcal{E}_{2n}$, since every element $P \in \mathcal{E}_{2n}$ has a Gram decomposition

$$P = (v_1 \dots v_n w_1 \dots w_n)^*(v_1 \dots v_n w_1 \dots w_n).$$

A computation yields the expression

$$\omega_{qc}(G, \pi) = \omega_q(G, \pi) = \frac{1}{2} + \frac{1}{2} \max_{P \in \mathcal{E}_{2n}} Tr(B_{\mathcal{G}} P).$$

To verify the claims concerning $\omega_{qc}^s(G, \pi)$, first note that by the above argument we have

$$\omega_{qc}^s(G, \pi) = \omega_q^s(G, \pi) = \frac{1}{2} + \frac{1}{2} \max_{P' \in \mathcal{E}_{2n}'} Tr(B_{\mathcal{G}} P').$$

where $\mathcal{E}_{2n}' \subseteq \mathcal{E}_{2n}$ is taken to be the set of $P \in \mathcal{E}_{2n}$ whose upper right $n \times n$ corner has the form

$(\langle v_x, v_y \rangle)_{x,y}$ for a single set of real unit vectors $\{v_1, \ldots, v_n\}$, by Theorem 4.4.4. Because of the form of $B_{\mathcal{G}}$, we may assume any $P' \in \mathcal{E}'_{2n}$ has the form

$$P' = \begin{pmatrix} P & P \\ P & P \end{pmatrix}, \quad P \in \mathcal{E}_n,$$

and a computation shows that $Tr(B_{\mathcal{G}} P') = Tr(A^s_G P)$. Thus

$$\omega^s_{qc}(G, \pi) = \omega^s_q(G, \pi) = \frac{1}{2} + \frac{1}{2} \max_{P \in \mathcal{E}_n} Tr(A^s_{\mathcal{G}} P).$$

This proves the claims. □

4.5 Two Colourings

The 2-colouring game for a graph $G = (V, E)$ is not formally an XOR game, since whenever $x \neq y$ and $(x, y) \notin E$ we have that $\lambda(x, y, a, b) = 1$ for all pairs a, b, while an XOR game requires that $a \oplus b = f(x, y) \in \{0, 1\}$ to win, for every $x, y \in V$. However, if the prior distribution on inputs has the property that $\pi(x, y) = 0$, whenever $x \neq y$ and $(x, y) \notin E$, then we may arbitrarily set $f(x, y)$ to be 0 or 1, without altering the corresponding value of the game. Thus, when we restrict to prior distributions with this property, we may apply the results on synchronous XOR games to compute the value of 2-colouring games.

Proposition 4.5.1. *Let $G = (V, E)$ be a graph on n vertices and let A_G denote its adjacency matrix. Then*

$$Cut_{q,2}(G) = Cut_{qc,2}(G) = \frac{|E|}{4} - \frac{1}{4} \min_{P \in \mathcal{E}_n} Tr(A_G P).$$

Proof. Recall that to compute this value we must consider the game $\mathcal{G} = (Hom(G, K_2), \pi)$ where π is the uniform density on E. In this case we have an XOR game with $f(x, y) = 1$, $\forall (x, y) \in E$ and 0 otherwise. Thus, $A^s_{\mathcal{G}} = \big((-1)^{f(x,y)}\pi(x, y)\big) = -\frac{1}{|E|}A_G$ and the result follows by Theorem 4.4.5. □

It is not hard to see that if we let $\mathcal{P}_n \subset \mathcal{E}_n$ be the set of all rank one positives all of whose entries are ±1, then the ordinary max cut is given by

$$Cut_2(G) = \frac{|E|}{4} - \frac{1}{4} \min_{P \in \mathcal{P}_n} Tr(A_G P).$$

This gives another way to see $Cut_{q,2}(G)$ as a relaxation of the usual max cut.

We now turn our attention to studying 2 colourings for odd cycles. Let C_{2k+1} be an odd cycle. We will index the vertices by $\mathbb{Z}_{2k+1}$ so that vertices are adjacent if and only if they are the pair $(j, j \pm 1)$, $0 \leq j \leq 2k$ where $2k + 1 = 0$. We consider the game $\mathcal{G} = (Hom(C_{2k+1}, K_2), \pi)$ with several different prior distributions π on $\mathbb{Z}_{2k+1} \times \mathbb{Z}_{2k+1}$. We first consider a non-symmetric uniform distribution, first studied by Cleve-Hoyer-Toner-Watrous [132], in order to compare the synchronous and non-synchronous values of the game. We then consider a natural family of symmetric distributions. We will show that for both non-symmetric and symmetric distributions, the synchronous quantum value of the game can be strictly smaller than the quantum value of the game, though in some cases these values may coincide. In all cases, the q and qc values of the game will coincide.

4.5.1 Non-symmetric uniform distribution

We now compute the synchronous q-value of $\mathcal{G} = (Hom(C_{2k+1}, K_2), \pi)$ with the prior distribution given by

$$\pi(x,y) = \begin{cases} \frac{1}{2n} & x = y \text{ or } x+1 = y \mod n \\ 0 & \text{else} \end{cases}$$

where $n = 2k+1$. The game $Hom(C_{2k+1}, K_2)$ with the distribution π was studied in Subsection 3.2 of [132], where it was show that

$$\omega_{qc}(\mathcal{G}) = \omega_q(\mathcal{G}) = \cos^2(\pi/4n) = \frac{1}{2} + \frac{1}{2}\cos(\pi/2n).$$

We will show that $\omega^s_{qc}(\mathcal{G}) = \omega^s_q(\mathcal{G}) = \frac{1}{2} + \frac{1}{2}\cos^2(\pi/2n)$, which is strictly less than $\omega_{qc}(\mathcal{G})$.

Theorem 4.5.2. *Let $n = 2k+1$. Then $\omega^s_{qc}(\mathcal{G}) = \omega^s_q(\mathcal{G}) = \frac{1}{2} + \frac{1}{2}\cos^2(\pi/2n)$.*

Proof. By Theorem 4.4.5, we have

$$\omega^s_{qc}(\mathcal{G}, \pi) = \omega^s_q(\mathcal{G}, \pi) = \frac{1}{2} + \frac{1}{2}\max_{P \in \mathcal{E}_n} Tr(A^s_{\mathcal{G}} P)$$

where

$$A^s_{\mathcal{G}} = \begin{pmatrix} \frac{1}{2n} & -\frac{1}{4n} & 0 & \dots & -\frac{1}{4n} \\ -\frac{1}{4n} & \frac{1}{2n} & -\frac{1}{4n} & \dots & 0 \\ & \ddots & \ddots & \ddots & \\ 0 & & -\frac{1}{4n} & \frac{1}{2n} & -\frac{1}{4n} \\ -\frac{1}{4n} & \dots & 0 & -\frac{1}{4n} & \frac{1}{2n} \end{pmatrix}$$

and $\mathcal{E}_n$ denotes the $n \times n$ elliptope defined in Equation (4.4.1). Thus, it suffices to calculate

$$\max_{P \in \mathcal{E}_n} Tr(A^s_{\mathcal{G}} P).$$

The dual of this semidefinite program is

$$\min_{D \in \mathcal{D}_n} Tr(D) \quad \text{subject to} \quad D - A^s_{\mathcal{G}} \geq 0$$

where $\mathcal{D}_n$ denotes the set of $n \times n$ diagonal real matrices. Since the feasible region $\mathcal{E}_n$ is convex and includes positive definite matrices, and since $\mathcal{D}_n$ is non-emepty, Slater's conditions [133] are satisfied and strong duality holds. By the symmetry of $A^s_{\mathcal{G}}$, it suffices to minimize $Tr(D)$ over all constant diagonal matrices. This is because if D is diagonal and satisfies $D - A^s_{\mathcal{G}} \geq 0$, then $U^*(D - A^s_{\mathcal{G}})U = U^* D U - A^s_{\mathcal{G}} \geq 0$ where U is the cyclic shift

$$U = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & \ddots & \ddots & \ddots & \\ 0 & & 0 & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

Averaging $(U^j)^* D U^j$ over all $j \in \{0, 1, \dots, n-1\}$ yields a constant matrix with the same trace as D. Hence, we only need to calculate

$$\min_{y \in \mathbb{R}} ny \quad \text{subject to} \quad yI_n - A^s_{\mathcal{G}} \geq 0.$$

Since the matrix $yI_n - A^s_{\mathcal{G}}$ is circulant, its eigenvalues have the form

$$\lambda_j = \left(y - \frac{1}{2n}\right) + \frac{1}{4n}\omega_n^j + \frac{1}{4n}\omega_n^{(n-1)j},$$

where $\omega_n = e^{2\pi i/n}$ is the primitive n-th root of unity[2] (c.f. Exercise 2.2P10 of [134]). Observe that λ_j is real since $\omega_n^{-j} = \omega_n^{(n-1)j}$ and thus $\omega_n^j + \omega_n^{(n-1)j} = 2\mathrm{Re}(\omega_n^j)$. The smallest value of y for which $\lambda_j \geq 0$ for every j is

$$y = \frac{1}{2n} + \frac{1}{2n}\cos(\pi/n).$$

It follows that

$$\max_{P \in \mathcal{E}_n} Tr(A^s_{\mathcal{G}}P) = \frac{1}{2}\left(1 + \cos(\pi/n)\right).$$

Consequently,

$$\begin{aligned}
\omega^s_{qc}(\mathcal{G}, \pi) &= \frac{1}{2} + \frac{1}{4}\left(1 + \cos(\pi/n)\right) \\
&= \frac{1}{2} + \frac{1}{4}\left(1 + 2\cos^2(\pi/2n) - 1\right) \\
&= \frac{1}{2} + \frac{1}{2}\cos^2(\pi/2n)
\end{aligned}$$

as desired. □

4.5.2 Symmetric distributions

The above shows that the synchronous q-value of a game is sometimes strictly smaller than the q-value of the game. In that case, the gap between these values is aided by the fact that the

[2] This can be seen directly by checking that $\begin{pmatrix} 1 & \omega_n^j & \ldots & \omega_n^{j(n-1)} \end{pmatrix}^T$ is an eigenvector for each $j \in \{0, 1, \ldots, n-1\}$.

prior distribution is not symmetric. We will now show that even when the prior distribution is symmetric, there may still be a gap between the synchronous q-value of the game and the q-value of the game.

Let $p, q \geq 0$ with $p + q = 1$. Consider the symmetric prior distribution

$$\pi(x, y) = \begin{cases} \frac{p}{2n} & x + 1 = y \mod n \\ \frac{p}{2n} & y + 1 = x \mod n \\ \frac{q}{n} & x = y \\ 0 & \text{else} \end{cases} \tag{4.5.1}$$

where $n = 2k + 1$. We first calculate the q-value of the two-colouring game, which is again equal to the qc-value of the game.

Theorem 4.5.3. *Let $p, q \geq 0$ with $p + q = 1$, and let π be the prior distribution given in equation (4.5.1), where $n = 2k + 1$. Then*

$$\omega_{qc}(\mathcal{G}) = \omega_q(\mathcal{G}) = \begin{cases} p & p > \frac{1}{2-\cos^2(\pi/2n)} \\ q + p\cos^2(\pi/2n) & \textit{else}. \end{cases}$$

Moreover, $\omega_{qc}(\mathcal{G}) = \omega_{loc}(\mathcal{G})$ whenever $p > \frac{1}{2-\cos^2(\pi/2n)}$.

Proof. By Theorem 4.4.5, we have

$$\omega_{qc}(\mathcal{G}, \pi) = \omega_q(\mathcal{G}, \pi) = \frac{1}{2} + \frac{1}{2} \max_{P \in \mathcal{E}_{2n}} Tr(B_{\mathcal{G}} P)$$

where

$$B_{\mathcal{G}} := \frac{1}{2}\begin{pmatrix} 0 & A_{\mathcal{G}} \\ A_{\mathcal{G}}^T & 0 \end{pmatrix} \in M_{2n}, \quad A_{\mathcal{G}} = \begin{pmatrix} \frac{q}{n} & -\frac{p}{2n} & 0 & \dots & -\frac{p}{2n} \\ -\frac{p}{2n} & \frac{q}{n} & -\frac{p}{2n} & \dots & 0 \\ & \ddots & \ddots & \ddots & \\ 0 & & -\frac{p}{2n} & \frac{q}{n} & -\frac{p}{2n} \\ -\frac{p}{2n} & \dots & 0 & -\frac{p}{2n} & \frac{q}{n} \end{pmatrix}$$

and $\mathcal{E}_{2n}$ denotes the $2n \times 2n$ elliptope. We will now calculate

$$\max_{P \in \mathcal{E}_{2n}} Tr(B_{\mathcal{G}} P).$$

The value of this semidefinite program is equal to the value of the dual program

$$\min_{D \in \mathcal{D}_{2n}} Tr(D) \quad \text{subject to} \quad D - B_{\mathcal{G}} \geq 0$$

where $\mathcal{D}_{2n}$ denotes the set of $2n \times 2n$ diagonal real matrices. Following arguments in the previous section, it suffices to minimize $Tr(D)$ over all constant diagonal matrices. Hence, we only need to calculate

$$\min_{y \in \mathbb{R}} 2ny \quad \text{subject to} \quad yI_{2n} - B_{\mathcal{G}} \geq 0.$$

It follows from Lemma 3.1 of [135] that the value of this semidefinite program is

$$2n\|B_{\mathcal{G}}\| = n\|A_{\mathcal{G}}\|.$$

Since $A_{\mathcal{G}}$ is symmetric, its norm is equal to $\max_j |\lambda_j|$, where $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$ are the eigenvalues of $A_{\mathcal{G}}$. Since $A_{\mathcal{G}}$ is circulant, its eigenvalues have the form

$$\lambda_j = \frac{q}{n} - \frac{p}{2n}\omega_n^j - \frac{p}{2n}\omega_n^{(n-1)j}$$

where $\omega_n = e^{2\pi i/n}$ is the n-th root of unity. Thus, the smallest eigenvalue of $A_{\mathcal{G}}$ is $\lambda_0 = \frac{q-p}{n}$, while the largest eigenvalue is $\lambda_{(n-1)/2} = \frac{q}{n} + \frac{p}{n}\cos(\pi/n)$. A calculation shows that

$$\frac{p-q}{n} > \frac{q}{n} + \frac{p}{n}\cos(\pi/n) \quad \text{if and only if} \quad p > \frac{2}{3-\cos(\pi/n)} = \frac{1}{2-\cos^2(\pi/2n)}$$

using $q = 1-p$. Thus

$$n\|A_{\mathcal{G}}\| = \begin{cases} p-q & p > \frac{1}{2-\cos^2(\pi/2n)} \\ q + p\cos(\pi/n) & \text{else} \end{cases}$$

and thus

$$\omega_{qc}(\mathcal{G},\pi) = \begin{cases} \frac{1}{2} + \frac{1}{2}(p-q) & p > \frac{1}{2-\cos^2(\pi/2n)} \\ \frac{1}{2} + \frac{1}{2}(q + p\cos(\pi/n)) & \text{else} \end{cases}.$$

Since

$$\frac{1}{2} + \frac{1}{2}(p-q) = \frac{1}{2}(p+q) + \frac{1}{2}(p-q) = p$$

and

$$\begin{aligned}\frac{1}{2}+\frac{1}{2}(q+p\cos(\pi/n)) &= \frac{1}{2}+\frac{1}{2}(1-p)+\frac{p}{2}(\cos(\pi/n))\\ &= 1-\frac{p}{2}+\frac{p}{2}(2\cos^2(\pi/2n)-1)\\ &= 1-p+p\cos^2(\pi/2n)\\ &= q+p\cos^2(\pi/2n),\end{aligned}$$

the first statement is proven. That $\omega_{loc}(\mathcal{G},\pi)=p$ when $p>\frac{1}{2-\cos^2(\pi/2n)}$ follows from the observation that the value p is obtained when Alice and Bob employ the deterministic strategy of always returning opposite colors. □

We remark that whenever $p>(2-\cos^2(\pi/2n))^{-1}$, the winning deterministic strategy of always returning opposite colors (e.g. Alice always answers with $a=0$ and Bob with $b=1$) is not a synchronous strategy. Let us now consider the synchronous value of this game.

Theorem 4.5.4. *Let $p,q\geq 0$ with $p+q=1$, and let π be the prior distribution given in equation (4.5.1), where $n=2k+1$. Then*

$$\omega_{qc}^s(\mathcal{G})=\omega_q^s(\mathcal{G})=q+p\cos^2(\pi/2n).$$

Consequently, $\omega_{qc}^s(\mathcal{G})<\omega_{qc}(\mathcal{G})=\omega_{loc}(\mathcal{G})$ whenever $p>\frac{1}{2-\cos^2(\pi/2n)}$.

Proof. The proof is similar to the proof of Theorem 4.5.2, so we just outline the main points. By Theorem 4.4.5,

$$\omega_{qc}^s(\mathcal{G},\pi)=\omega_q^s(\mathcal{G},\pi)=\frac{1}{2}+\frac{1}{2}\max_{P\in\mathcal{E}_n}Tr(A_{\mathcal{G}}^sP).$$

The value $\max_{P \in \mathcal{E}_n} Tr(A^s_{\mathcal{G}} P)$ is obtained by considering the eigenvalues of the circulant matrix $A^s_{\mathcal{G}} = A_{\mathcal{G}}$. These eigenvalues have the form

$$\lambda_j = \frac{q}{n} - \frac{p}{2n}\omega_n^j - \frac{p}{2n}\omega_n^{(n-1)j}$$

where $\omega_n = e^{2\pi i/n}$ is the n-th root of unity. In particular, the largest eigenvalue of $A_{\mathcal{G}}$ is $\frac{q}{n} + \frac{p}{n}\cos(\pi/n)$. Thus, the value of

$$\min_{D \in \mathcal{D}_n} Tr(D) \quad \text{subject to} \quad D - A^s_{\mathcal{G}} \geq 0,$$

which is equal to

$$\min_{y \in \mathbb{R}} ny \quad \text{subject to} \quad yI_n - A^s_{\mathcal{G}} \geq 0$$

is given by

$$n\left(\frac{q}{n} + \frac{p}{n}\cos(\pi/n)\right) = q + p\cos(\pi/n).$$

Finally, repeating the calculations from the proof of Theorem 4.5.3 yields the result. □

4.6 Products of Games

There is a great deal of research concerning products of games and especially their behaviour when one does many iterations of a fixed game [56, 57, 52]. Many of these results are false for synchronous values of games.

Given two games $G_i = (X_i, O_i, \lambda_i), i = 1, 2$ their product $G_1 \times G_2$ is the game with input set

$X := X_1 \times X_2$, output set $O := O_1 \times O_2$ and rule function,

$$\lambda : X \times X \times O \times O \to \{0, 1\} = \mathbb{Z}_2,$$

given by

$$\lambda((x_1, x_2), (y_1, y_2), (a_1, a_2), (b_1, b_2)) = \lambda_1(x_1, y_1, a_1, b_1)\lambda_2(x_2, y_2, a_2, b_2),$$

where the product is in $\mathbb{Z}_2$. Thus, they win if and only if $\lambda_1(x_1, y_1, a_1, b_1) = 1$ and $\lambda_2(x_2, y_2, a_2, b_2) = 1$, that is if and only if they win both games. It is customary to write $\lambda = \lambda_1 \times \lambda_2$.

Given prior distributions $\pi_1 : X_1 \times X_1 \to [0, 1]$ and $\pi_2 : X_2 \times X_2 \to [0, 1]$ it is easy to see that by defining,

$$\pi : X \times X \to [0, 1],\ \pi((x_1, x_2), (y_1, y_2)) := \pi_1(x_1, y_1) \cdot \pi_2(x_2, y_2),$$

we obtain a distribution on $X \times X$, which is denoted by $\pi_1 \times \pi_2$.

If $\mathcal{G}_i = (G_i, \pi_i)$ denotes the game with distribution π_i then we set $\mathcal{G}_1 \times \mathcal{G}_2 = (G_1 \times G_2, \pi_1 \times \pi_2)$.

These definitions clearly extend to products of more than two games. Given a game with distribution $\mathcal{G} = (G, \pi)$ we let $\mathcal{G}^n = (G^n, \pi^n)$ denote the n-fold product of a game with itself.

Here are a few of the results that are known for the values of such games:

1. (Supermultiplicativity) $\omega_t(\mathcal{G} \times \mathcal{H}) \geq \omega_t(\mathcal{G})\omega_t(\mathcal{H})$, and examples exist for which the inequality is strict,

2. $\omega_t(\mathcal{G} \times \mathcal{H}) \leq min\{\omega_t(\mathcal{G}), \omega_t(\mathcal{H})\}$

3. $G \times H$ has a perfect t-strategy $\iff$ G and H each have a perfect t-strategy for $t = loc, qa, qc$.

4. if $\omega_{loc}(\mathcal{G}) < 1$, then $\omega_{loc}(\mathcal{G}^n) \to 0$.

Thus, when the value is not 1, even though it is possible that $\omega_{loc}(\mathcal{G}^n) > \omega_{loc}(\mathcal{G})^n$, we still have that it tends to 0.

The analogues of (1) and (3) were shown to hold for synchronous values in [136], where an example is also given to show that the inequality can be strict.

The example below shows that (2) and (4) can fail for synchronous values.

Example 4.6.1. Let $\mathcal{G} = (G, \pi)$ be the game where Alice's and Bob's question and answer sets are $\{0, 1\}$ and let the distribution π be given by $\pi(0, 1) = \pi(1, 1) = 1/2$. The players win if their answer pair is $(1, 1)$ when asked question pair $(0, 1)$. They also win if their answer pair is $(0, 1)$ when they receive question pair $(1, 1)$. They lose in all other cases. Note that Bob receives 1 with probability 1 while Alice receives 0, 1 with equal probability.

This game has a perfect non-synchronous strategy, namely, for Bob to always return 1 and for Alice given input $x \in \mathbb{Z}_2$ to always return $x + 1$. Thus,

$$\omega_{loc}(\mathcal{G}) = \omega_{qc}(\mathcal{G}) = 1,$$

and consequently,

$$\omega_{loc}(\mathcal{G}^n) = \omega_{qc}(\mathcal{G}^n) = 1.$$

Theorem 4.6.2. *Let $\mathcal{G} = (G, \pi)$ be the game with distribution of Example 4.6.1. Then*

$$\omega^s_{loc}(\mathcal{G}^n) = \omega^s_{qc}(\mathcal{G}^n) = 1 - \frac{1}{2^n}.$$

Proof. The synchronous value of this game is at most $1/2$, since on question $(1, 1)$ a synchronous strategy will require them to return the same answer and lose. On the other hand, the deterministic strategy of Alice and Bob always returning 1 has a value of $1/2$. Hence, $\omega^s_{loc}(\mathcal{G}) = \omega^s_q(\mathcal{G}) = \frac{1}{2}$. In terms of traces and projections, this is given by setting $E_{0,1} = E_{1,1} = I$ and $E_{0,0} = E_{1,0} = 0$.

Now for the n-fold parallel repetition the questions are pairs $x, y \in \{0, 1\}^n$ and the answers are pairs $a, b \in \{0, 1\}^n$. But $\pi^n(x, y) = 0$ unless $y = (1, ..., 1) := 1^n$, while $\pi(x, 1^n) = \frac{1}{2^n}$, $\forall x \in \{0, 1\}^n$.

The only question pair where the synchronous restriction can be enforced is therefore $(1^n, 1^n)$, and on this question any synchronous strategy loses as before. Thus, $\omega^s_{qc}(\mathcal{G}^n) \leq 1 - \frac{1}{2^n}$.

On the other hand, consider the deterministic strategy where when the input string is 1^n they return 1^n but for every other input string $x \neq 1^n$, they return the output string $\overline{x} = x + 1^n$, where addition is in the vector space $\mathbb{Z}_2^n$, i.e., each bit of x is flipped. For every string $x \neq 1^n$ that Alice receives this strategy wins. Hence, $\omega^s_{loc}(\mathcal{G}^n) \geq 1 - \frac{1}{2^n}$. Therefore the synchronous value of the parallel repeated game is $\omega^s_{loc}(\mathcal{G}^n) = \omega^s_{qc}(\mathcal{G}^n) = 1 - \frac{1}{2^n}$.

Alternatively, this is the strategy that corresponds to choosing PVM's,

$$E_{1^n,1^n} = E_{x,\overline{x}} = I, \ \forall x \neq 1^n,$$

and all other projections equal to 0. □

Thus, not only does the synchronous value not tend to 0, but it is monotonically increasing. Also, we have that

$$\omega_t^s(\mathcal{G}^2) > \min\{\omega_t(\mathcal{G}), \omega_t^s(\mathcal{G})\},$$

so that this example violates the synchronous analogues of properties (2) and (4).

Two objections can be raised to this example. The game itself is not synchronous and the distribution is not symmetric. It is natural to wonder if this pathology persists even when restricting attention to this smaller family of synchronous games with symmetric prior densities. This is formalized in the following problems.

Problem 4.6.3. If $\mathcal{G}_i = (G_i, \pi_i), i = 1, 2$ are symmetric synchronous games with symmetric densities, then is $\omega_t^s(\mathcal{G}_1 \times \mathcal{G}_2) \leq \min(\omega_t^s(\mathcal{G}_1), \omega_t^s(\mathcal{G}_2))$?

Problem 4.6.4. If $\mathcal{G}$ is a symmetric, synchronous game with symmetric distribution, can $\omega_t^s(\mathcal{G}^n)$ be monotone increasing?

We next return our attention to XOR games.

First note that the product of two XOR games is not an XOR game. In fact the product is not even a game with binary answers. Our first step is to recall an operation on XOR games, studied in [21], that unlike the product, produces an XOR game. The **XOR of XOR games** G_1 and G_2 with densities π_1, π_2 and rule functions f_1 and f_2, denoted by $G_1 \oplus G_2$, is the XOR game $(I_1 \times I_2, \{0, 1\}, \lambda)$ with distribution $\pi_1 \times \pi_2$ and rule function λ defined so that $\lambda((x_1, x_2), (y_1, y_2), a, b) = 1$ iff $a + b = f_1(x_1, y_1) + f_2(x_2, y_2)$ in $\mathbb{Z}_2$. The XOR of more than two games is defined inductively.

The following result shows why this is an interesting operation on XOR games.

Proposition 4.6.5. *Let $\mathcal{G}_i = (I_i, \{0, 1\}, \lambda_i, \pi_i), i = 1, 2$ be XOR games with densities and cost* *matrices $A_{\mathcal{G}_i}, i = 1, 2$. Then the cost matrix of their direct sum satisfies*

$$A_{\mathcal{G}_1 \oplus \mathcal{G}_2} = A_{\mathcal{G}_1} \otimes A_{\mathcal{G}_2}.$$

The **bias** of a game with distribution is defined by the formulas

$$\varepsilon_t(\mathcal{G}) = 2\omega_t(\mathcal{G}) - 1, \;\; t = loc, q, qc,$$

and corresponds to the probability of winning minus the probability of losing. Similarly, we have the **synchronous bias**,

$$\varepsilon_t^s(\mathcal{G}) = 2\omega_t^s(\mathcal{G}) - 1, \;\; t = loc, q, qc.$$

In [21, Theorem 1] it was proven that the quantum bias of XOR games is multiplicative for the direct sum operations, i.e.,

$$\varepsilon_q(\mathcal{G}_1 \oplus \mathcal{G}_2) = \varepsilon_q(\mathcal{G}_1)\varepsilon_q(\mathcal{G}_2).$$

In what follows we show that this fails for the synchronous bias, even for a family of games that is very well behaved.

Definition 4.6.6. An XOR game with distribution π will be called a **synchronous XOR game**, provided that the game is synchronous, i.e., $f(x,x) = 0$, symmetric, $f(x,y) = f(y,x)$ and the distribution is symmetric, $\pi(x,y) = \pi(y,x)$.

Note that when $\mathcal{G}$ is a synchronous XOR game, we have that the cost matrix $A_{\mathcal{G}} = ((-1)^{f(x,y)}\pi(x,y)) = A_{\mathcal{G}}^T$ and hence,

$$A_{\mathcal{G}}^s = A_{\mathcal{G}}.$$

In what follows we first show that the perfect parallel repetition does not hold for the synchronous bias of synchronous XOR games. We then identify a subclass of XOR games for which the synchronous value satisfies the perfect parallel repetition.

Restating Theorem 4.4.5 in terms of biases yields:

Theorem 4.6.7. *Let $G = (I, \{0,1\}, \lambda)$ be an XOR game with $n := |I|$, and suppose $f : I \times I \to \{0,1\}$ is a function satisfying $f(x,y) = a \oplus b$ for all $a, b \in \{0,1\}$. Let $\pi(x,y)$ be a prior distribution on I. Then for $\mathcal{G} = (G, \pi)$,*

$$\varepsilon_{qc}(\mathcal{G}) = \varepsilon_q(\mathcal{G}) = \max_{P \in \mathcal{E}_{2n}} Tr(B_{\mathcal{G}} P)$$

and

$$\varepsilon^s_{qc}(\mathcal{G}) = \varepsilon^s_q(\mathcal{G}) = \max_{P \in \mathcal{E}_n} Tr(A^s_{\mathcal{G}} P).$$

Fix the question set to be $I = \{1, \ldots, m\}$ and we can equivalently write the above optimization problem for the bias of a synchronous XOR game as the primal-dual semidefinite programs

$$\begin{array}{lll} (\mathcal{P}) & \text{maximize:} & \langle A, P \rangle \\ & \text{subject to:} & \text{diag}(P) = 1, \\ & & P \geq 0, \end{array} \qquad \begin{array}{lll} (\mathcal{D}) & \text{minimize:} & \sum_{k=1}^{m} y_k \\ & \text{subject to:} & \text{Diag}(y) - A \geq 0, \end{array}$$

where the inner product is the trace inner product,

$$A := A^s_{\mathcal{G}} = 1/2(\pi(x,y)(-1)^{f(x,y)}) + 1/2(\pi(x,y)(-1)^{f(x,y)})^T,$$

and diag is the function that zeros out nondiagonal entries of a matrix, and Diag of a vector is the matrix where the diagonal entries are the vector entries and nondiagonal entries are zero. This primal-dual satisfies the Slater condition [133] and therefore their optimal values are attained and are equal. In fact by complementary slackness if (P^*, y^*) is an optimal solution pair for primal and dual then it holds that $P^*(\mathrm{Diag}(y^*) - A) = 0$. Now if y' is any other optimal dual solution, it holds that $P^* \mathrm{Diag}(y^* - y') = 0$. Since the diagonal entries of P are 1, this implies that $y' = y^*$. Therefore we get the following lemma

Lemma 4.1. *The dual problem $(\mathcal{D})$ has a unique optimal solution.*

In the next theorem, we show that the bias of an XOR game for which $\mathrm{Diag}(y^*) \geq A \geq -\mathrm{Diag}(y^*)$, where y^* is the unique dual optimal solution, are multiplicative. That is, for any two XOR games with this property, we have $\varepsilon_q^s(G_1 \oplus G_2) = \varepsilon_q^s(G_1)\varepsilon_q^s(G_2)$. This in particular includes all XOR games for which the game matrix is positive semidefinite. This is not true for all XOR games as is shown by the next example.

Example 4.6.8. Let $\mathcal{G}$ be the synchronous XOR game with cost matrix

$$A = \begin{bmatrix} \frac{1}{21} & -\frac{3}{21} & -\frac{3}{21} \\ -\frac{3}{21} & \frac{1}{21} & -\frac{3}{21} \\ -\frac{3}{21} & -\frac{3}{21} & \frac{1}{21} \end{bmatrix}.$$

The pair $P^* = \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & 1 & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{bmatrix}$ and $y^* = \begin{bmatrix} \frac{4}{21} \\ \frac{4}{21} \\ \frac{4}{21} \end{bmatrix}$ are easily seen to be feasible solutions of the primal and dual SDPs and they achieve the same value $\frac{4}{7}$ in the primal and dual problems, respectively.

Therefore they are optimal solutions and the optimal value and hence the synchronous quantum bias of this game is

$$\varepsilon_q^s(\mathcal{G}) = \frac{4}{7}.$$

Now the cost matrix for the game $\mathcal{G}' = \mathcal{G} \oplus \mathcal{G}$ is $A \otimes A$. Therefore the primal-dual problem for $\mathcal{G}'$ is

$$\begin{array}{llll} (\mathcal{P}) & \text{maximize:} & \langle A \otimes A, W \rangle & \qquad (\mathcal{D}) \quad \text{minimize:} \quad \sum_{k=1}^{9} u_k \\ & \text{subject to:} & \operatorname{diag}(W) = 1, & \qquad \qquad \text{subject to:} \quad \operatorname{Diag}(u) - A \otimes A \succeq 0. \\ & & W \succeq 0, & \end{array}$$

Now from a similar argument like above the pair $W^* = ee^*$ where $e \in \mathbb{C}^9$ is the all-one vector and $u = (\frac{5}{21})^2 e$ are optimal solutions for the primal and dual respectively and the optimal value is $(\frac{5}{7})^2$. So we have that

$$\varepsilon_q^s(\mathcal{G} \oplus \mathcal{G}) = (\frac{5}{7})^2 > (\frac{4}{7})^2 = \varepsilon_q^s(\mathcal{G})^2.$$

Note that the unique optimal solution y^* for the dual problem of G does not satisfy the condition

$$\operatorname{Diag}(y^*) \geq A \geq -\operatorname{Diag}(y^*)$$

because the eigenvalues of A are $4/21, 4/21, -5/21$.

Definition 4.6.9. We call a synchronous XOR game $\mathcal{G}$ and symmetrized cost matrix $A := A_{\mathcal{G}}^s$

balanced, if the unique optimal dual solution y^* satisfies

$$\mathrm{Diag}(y^*) \geq A \geq -\mathrm{Diag}(y^*).$$

Suppose that $\mathcal{G}$ is a balanced game and y^* is its unique dual optimal solution. Note that if $y^*(i) \leq 0$ for some question i, then the inequalities above imply that $y^*(i) = A(i,i) = 0$. Then again since $A + \mathrm{Diag}(y^*)$ is positive semidefinite (and its ith diagonal element is 0), it must be that the ith column and row of A are all zeros. Therefore it is true that $\pi(i,j) = \pi(j,i) = 0$ for all questions j. Therefore question i is irrelevant and can be removed from the question set of the original game. Thus without loss of generality, we can assume that $y^* > 0$ (by $y^* > 0$ we mean $y^*(i) > 0$ for all i).

Proposition 4.6.10. *Any XOR $\mathcal{G}$ game for which $A^s_{\mathcal{G}} \geq 0$ is balanced.*

Theorem 4.6.11. *If $\mathcal{G}_i, i = 1,2$ are balanced XOR games, then*

$$\varepsilon^s_q(\mathcal{G}_1 \oplus \mathcal{G}_2) = \varepsilon^s_q(\mathcal{G}_1)\varepsilon^s_q(\mathcal{G}_2)$$

and $\mathcal{G}_1 \oplus \mathcal{G}_2$ is balanced.

Proof. It is straightforward to see that $\varepsilon^s_q(\mathcal{G}_1 \oplus \mathcal{G}_2) \geq \varepsilon^s_q(\mathcal{G}_1)\varepsilon^s_q(\mathcal{G}_2)$. So we just prove the reverse inequality $\varepsilon^s_q(\mathcal{G}_1 \oplus \mathcal{G}_2) \leq \varepsilon^s_q(\mathcal{G}_1)\varepsilon^s_q(\mathcal{G}_2)$.

Let A_1 and A_2 be the symmetrized cost matrices of $\mathcal{G}_1$ and $\mathcal{G}_2$, respectively. Then the symmetrized cost matrix of $\mathcal{G} = \mathcal{G}_1 \oplus \mathcal{G}_2$ is $A = A_1 \otimes A_2$. By assumption the unique optimal dual solutions satisfy $y_1 > 0$ and $y_2 > 0$ and

$$-\operatorname{Diag}(y_1) \le A_1 \le \operatorname{Diag}(y_1),$$

$$-\operatorname{Diag}(y_2) \le A_2 \le \operatorname{Diag}(y_2).$$

We also have

$$-I \le \operatorname{Diag}(y_1)^{-1/2} A_1 \operatorname{Diag}(y_1)^{-1/2} \le I,$$

$$-I \le \operatorname{Diag}(y_2)^{-1/2} A_2 \operatorname{Diag}(y_2)^{-1/2} \le I.$$

This implies that the operator norm of

$$(\operatorname{Diag}(y_1)^{-1/2} \otimes \operatorname{Diag}(y_2)^{-1/2})(A_1 \otimes A_2)(\operatorname{Diag}(y_1)^{-1/2} \otimes \operatorname{Diag}(y_2)^{-1/2})$$

is at most 1 and therefore

$$-I \le (\operatorname{Diag}(y_1)^{-1/2} \otimes \operatorname{Diag}(y_2)^{-1/2})(A_1 \otimes A_2)(\operatorname{Diag}(y_1)^{-1/2} \otimes \operatorname{Diag}(y_2)^{-1/2}) \le I$$

which equivalently can be written as

$$-\operatorname{Diag}(y_1) \otimes \operatorname{Diag}(y_2) \le A_1 \otimes A_2 \le \operatorname{Diag}(y_1) \otimes \operatorname{Diag}(y_2).$$

Thus $y_1 \otimes y_2$ is a feasible solution of the dual problem of $G_1 \oplus G_2$. Therefore the bias of $G_1 \otimes G_2$ is at most $\varepsilon_q^s(G_1)\varepsilon_q^s(G_2)$. Therefore it must be that $\varepsilon_q^s(G_1 \oplus G_2) = \varepsilon_q^s(G_1)\varepsilon_q^s(G_2)$ and $y_1 \otimes y_2$

is the unique dual optimal solution for $G_1 \oplus G_2$. Finally, from the last inequality we derived, the game $G_1 \oplus G_2$ is balanced. □

4.7 Optimality Conditions

In this section we derive conditions that a family E of n k-PVM's in a tracial C*-algebra $(\mathcal{A}, \tau)$ must satisfy in order to give the optimal value of a game. In the second part of this section we give necessary conditions for when optimizing over **positive operator valued measures** (POVMs) has a synchronous optimizer. This POVM subsection restricts $\mathcal{A}$ to be M_m, the set of all $m \times m$ matrices.

Our main definitions are stated for both k-PVMs and k-POVMs. These both consist of operators $\{E_{x,a}\}$ which satisfy $E_{x,a} \geq 0$ and $\sum_{a=0}^{k-1} E_a = I$, however, for a PVM each $\{E_{x,a}\}$ is a projection. Given an n input, k output game and distribution, $\mathcal{G} = (G, \pi)$, and a tracial C*-algebra $(\mathcal{A}, \tau)$, we seek conditions that a family $E := \{E_{x,a} : x \in I, a \in O\}$ of k-PVM's or k-POVM's must satisfy in order to maximize the quantity

$$\phi(E) = \sum_{(x,y,a,b)\in W} \pi(x,y)\tau(E_{x,a}E_{y,b}) = \sum_{(x,y,a,b)} \pi(x,y)\lambda(x,y,a,b)\tau(E_{x,a}E_{y,b}).$$

When a family maximizes ϕ over all PVM-families (resp. PVM-families) in $\mathcal{A}$, we call it **PVM optimal (resp. POVM optimal) for** $(\mathcal{A}, \tau)$. For each fixed $(x,a) \in I \times O$ we set

$$Q_{x,a} = \sum_{\substack{y,b \\ (x,y,a,b)\in N, y\neq x}} \pi(x,y)E_{y,b} + \sum_{\substack{y,b \\ (y,x,b,a)\in N, y\neq x}} \pi(y,x)E_{y,b}.$$

Note that when λ is symmetric and the distribution is symmetric, then both sums occurring in the definition of $Q_{x,a}$ are equal.

4.7.1 Optimality over families of PVM's

We begin with a first derivative condition.

Proposition 4.7.1. *Let $(G, \pi) = (I, O, \lambda, \pi)$ be a synchronous game with distribution, let $(\mathcal{A}, \tau)$ be a faithful trace of type t, let $\{E_{x,a}\} \subseteq \mathcal{A}$ and let $p(a, b|x, y) = \tau(E_{x,a}E_{y,a})$. If $\{E_{x,a}\}$ is an optimal PVM for $(\mathcal{A}, \tau)$, then*

$$\sum_a E_{x,a}Q_{x,a} = \sum_a Q_{x,a}E_{x,a}, \ \forall x \in I.$$

Proof. Fix $x_0 \in I$. Let $H = H^* \in \mathcal{A}$ and replace the projections $E_{x_0,a}$ by $e^{iHr}E_{x_0,a}e^{-iHr}$, while leaving all the other projections fixed. Let us call the resulting density $p_r(a, b|x, y)$ and consider the function

$$f(r) = 1 - \omega(\mathcal{G}, \pi, p_r) = \sum_{(x,y,a,b)\in N} \pi(x, y)p_r(a, b|x, y).$$

Since this smooth function attains its minimum at $r = 0$ we must have that

$$\begin{aligned} 0 = f'(0) &= i \sum_{\substack{a,y,b \\ (x_0,y,a,b)\in N, y\neq x_0}} \pi(x_0, y)\tau(HE_{x_0,a}E_{y,b} - E_{x_0,a}HE_{y,b}) \\ &+ i \sum_{\substack{a,y,b \\ (y,x_0,b,a)\in N, y\neq x_0}} \pi(y, x_0)\tau(E_{y,b}HE_{x_0,a} - E_{y,b}E_{x_0,a}H) \\ &= i \sum_{\substack{a,y,b \\ (x_0,y,a,b)\in N, y\neq x_0}} \pi(x_0, y)\tau(H(E_{x_0,a}E_{y,b} - E_{y,b}E_{x_0,a})) \\ &+ i \sum_{\substack{a,y,b \\ (y,x_0,b,a)\in N, y\neq x_0}} \pi(y, x_0)\tau(H(E_{x_0,a}E_{y,b} - E_{y,b}E_{x_0,a})) \\ &= i\tau(H(\sum_a E_{x_0,a}Q_{x_0,a} - Q_{x_0,a}E_{x,a})). \end{aligned}$$

Since this is true for every $H = H^*$ and τ is faithful, we have that

$$\sum_a E_{x_0,a}Q_{x_0,a} - Q_{x_0,a}E_{x_0,a} = 0,$$

from which the result follows. □

Remark 6. *This proof is adapted from [119] where a similar idea was used to prove that for the graph correlation function, if a set of projections $\{P_x : x \in V\}$ minimized the correlation for a graph (V, E), then necessarily each P_x commuted with the sum of the projections over all vertices adjacent to x.*

Remark 7. *We will show what this result says about the CHSH game, with uniform distribution. Recall that this game has $I = O = \mathbb{Z}_2$ and the rules are that to win $a + b = xy$ where the arithmetic is in the field $\mathbb{Z}_2$. Computation shows that*

$$Q_{0,0} = E_{1,1},\ Q_{0,1} = E_{1,0},\ Q_{1,0} = E_{0,1},\ Q_{1,1} = E_{0,0}.$$

Thus, the above result tells us that for an optimum PVM strategy,

$$E_{0,0}E_{1,1} + E_{0,1}E_{1,0} = E_{1,1}E_{0,0} + E_{1,0}E_{0,1}.$$

Setting $P = E_{0,0}, Q = E_{1,0}$, this equation becomes

$$P(I - Q) + (I - P)Q = (I - Q)P + Q(I - P) \implies PQ = QP.$$

Thus, an optimal synchronous strategy for this game is an abelian strategy, which shows that

$$\omega_{qc}^{s}(CHSH) = \omega_{loc}^{s}(CHSH)$$

and we know that this latter value is the supremum over all deterministic strategies where Alice and Bob must use the same function $f : I \to O$. It is well-known that among these four functions, the optimal is for Alice and Bob to always return 0, i.e., $f(x) = 0, \forall x$, which has a value of $3/4$. *Thus, this game has no quantum advantage when we restrict to synchronous PVM strategies.*

Remark 8. *Set*

$$\Omega_x = \sum_a E_{x,a} Q_{x,a}.$$

If we have $\{E_{x,a}\}$ optimal as above, then the optimality condition in Proposition 4.7.1 is equivalent to $\Omega_x = \Omega_x^*$, $\forall x$ and it is also equivalent to $E_{x,a}Q_{x,a}E_{x,b} = E_{x,a}Q_{x,b}E_{x,b}$, $\forall a, b, x$.

One difficulty with C*-algebras is that they might contain few projections, for example the C*-algebra of continuous functions on $[0, 1]$ only contains the two trivial projections. However, von Neumann algebras are always generated by their projections. Given any C*-algebra and faithful trace $(\mathcal{A}, \tau)$ after we take the GNS representation, we may always look at the tracial von Neumann algebra generated by the image. Thus, insisting that $\mathcal{A}$ be a von Neumann algebra does not impose an undue restriction.

Lemma 4.2. *Let $(\mathcal{A}, \tau)$ be a von Neumann algebra with a faithful trace τ, let E be a projection and let $H = H^*$. If for every projection $P \leq E$ we have that $\tau(PH) \geq 0$, then $EHE \geq 0$.*

Proof. Let $\mathcal{A}$ be a concrete von Neumann subalgebra of the bounded operators on some Hilbert space. Recall that if $R \geq 0$ is a positive element of $\mathcal{A}$, then the projection P onto the range of R is an element of $\mathcal{A}$.

Decompose $EHE = R_+ - R_-$ into its positive and negative parts and let $P \leq E$ be the projection onto the range of R_-. Since

$$0 \leq \tau(PH) = \tau(PHP) = -\tau(R_-) \leq 0$$

and τ is faithful, we have that $R_- = 0$ and so $EHE \geq 0$.

□

Proposition 4.7.2. *Let $(G, \pi) = (I, O, \lambda, \pi)$ be a synchronous game with distribution, let $(\mathcal{A}, \tau)$ be a von Neumann algebra with a faithful trace. If $\{E_{x,a}\}$ is an optimal PVM for $(\mathcal{A}, \tau)$, then*

$$E_{x,a}Q_{x,b}E_{x,a} + \delta_x^b \, E_{x,a} \leq E_{x,a}Q_{x,a}E_{x,a} + \delta_x^a \, E_{x,a} \tag{4.7.1}$$

where $\delta_x^a = \pi(x,x)\lambda(x,x,a,a)$.

Proof. Fix an x_0 and a pair $a_0 \neq b_0$, and a projection, $P \leq E_{x_0,a_0}$. If we replace the family $\{E_{x,a}\}$ by the family $\{F_{x,a}\}$ defined by

- $F_{x,a} = E_{x,a}, \forall x \neq x_0$,
- $F_{x_0,c} = E_{x_0,c}, \forall c \neq a_0, b_0$,
- $F_{x_0,a_0} = E_{x_0,a_0} - P$,
- $F_{x_0,b_0} = E_{x_0,b_0} + P$,

then the value $\phi(F)$ of this new family of projections must be smaller than $\phi(E)$. Computing $\phi(E) - \phi(F)$ and applying the above lemma yields the result. □

Remark 9. *It is instructive to see what these results tell us in the case of the graph k-colouring game with uniform distribution. If a set of projections $\{E_{x,a}\}$ is optimal for this game and we write $y \sim x$ to indicate that vertices x, y are adjacent, then $Q_{x,a} = 2\sum_{y\sim x} E_{y,a}$ and the first derivative result tells us that for each a*

$$\sum_a E_{x,a}Q_{x,a} = \sum_a Q_{x,a}E_{x,a}.$$

The second result implies that

$$E_{x,a}(\sum_{y\sim x} E_{y,b})E_{x,a} \leq E_{x,a}(\sum_{y\sim x} E_{y,a})E_{x,a},$$

since $\delta_x^a = \delta_x^b$. Summing this inequality over all b, yields

$$d_x E_{x,a} \leq kE_{x,a}(\sum_{y\sim x} E_{y,a})E_{x,a}$$

where d_x is the degree of the vertex x.

Remark 10. *The necessary condition for a family to be PVM optimal for $(\mathcal{A}, \tau)$ in Proposition 4.7.1 comes from $f'(0) = 0$. An additional necessary condition for optimality comes from analyzing $f''(0) \leq 0$, which we did successfully and we found inequalities on the $E_{x,a}Q_{x,b}E_{x,a}$ which are equivalent to $f''(0) \leq 0$. Comparing these inequalities to those in Proposition 4.7.2 yields, when $\mathcal{A} = M_m$, that the conditions in Proposition 4.7.1 and Proposition 4.7.2 imply $f''(0) \leq 0$. This is unexpected, since one is derived by calculus and the other from permuting projections. We omit the proof, since as just noted it does not give a new optimality condition and the proof is not short.*

4.7.2 Optimizing over POVM's

In this second part of the section we give a set of optimality conditions for a more constrained problem than we just studied. We study optimal POVM strategies which are synchronous. In other words, these are optimal POVM strategies which are also PVM, as soon will be explained. Throughout this subsection we specialize $\mathcal{A}$ to be M_m the set of all $m \times m$ matrices and also require the extra restriction that $\lambda(x, x, a, a) = 1, \forall x, a$. With these assumptions we can use semidefinite programing theory, and get elegant optimality conditions Proposition 4.7.3 which easily imply the (weaker) conclusions of Proposition 4.7.2 and Proposition 4.7.1 restricted to finite dimensions.

The following are known properties of POVM optimization. Note that if $\{E_{x,a}\}$ are only POVM's, then setting

$$p(a, b|x, y) = \tau(E_{x,a}E_{y,b})$$

does define a density in C_{qc}, see Lemma 5.2 of [137]. But it will not necessarily be a synchronous density. In fact, assuming that τ is a faithful trace, we will have that the density is synchronous if and only if $\tau(E_{x,a}E_{x,b}) = 0$ for $a \neq b$ which is equivalent to $E_{x,a}E_{x,b} = 0$. On the other hand the fact that $\sum_a E_{x,a} = I$ and $E_{x,a}E_{x,b} = 0$ implies that each $E_{x,a}$ is a projection. Thus, the set of densities that can be obtained in this fashion is strictly larger than the synchronous densities, but it is also known to be smaller than the set of all densities in C_{qc}. For more details on this set of densities see [137].

The main result of this subsection is

Proposition 4.7.3. *Let $(\mathcal{G}, \pi) = (I, O, \lambda, \pi)$ be a synchronous game with distribution such that $\lambda(x, x, a, a) = 1$ for all a, x and let $(\mathcal{A}, \tau) = (M_m, tr_m)$ be the $m \times m$ matrices with their unique* *normalized trace. An optimizing POVM for $(\mathcal{A}, \tau)$ which is a PVM must satisfy*

1. $\Omega_x - Q_{x,b} \geq 0 \ \ for \ all \ b$

2. $(\Omega_x - Q_{x,b})E_{x,b} = 0 = E_{x,b}(\Omega_x - Q_{x,b})$ *for all b.*

Suppose the max value of the game occurs with a finite dimensional PVM strategy which is a synchronous strategy. Then the hypotheses of this proposition apply; so (1) and (2) must both hold.

Remark 11. *This can be compared to the previously derived necessary conditions, in the case that they also assume $\lambda(x, x, a, a) = 1$. That Ω_x is selfadjoint, the conclusion of Proposition 4.7.1, is immediate from Proposition 4.7.3(1), since $Q_{x,b}$ is selfadjoint. Proposition 4.7.2 also follows simply by compressing it with $E_{x,a}$.*

As an example consider the graph coloring problem. Summing Proposition 4.7.3(1) on $b = 0, 1, \ldots, k-1$ gives

$$\Omega_x \geq \frac{d_x}{k} I. \tag{4.7.2}$$

This condition when compressed by $E_{x,a}$ is the same as the one in Remark 9, so this condition is typically much stronger.

POVM proofs

Recall

$$\phi(E) = \sum_{(x,y,a,b)} \pi(x, y) \ \lambda(x, y, a, b) \ \tau(E_{x,a}E_{y,b}).$$

It will be useful to sort $\phi(E)$ according to dependence on a particular point x_0. Let E_x denote the POVM $E_x := \{E_{x,0}, \cdots, E_{x,k-1}\}$.

Lemma 4.3. *Fix τ and fix x_0. Then*

$$\phi(E) = no(x_0) + \pi(x_0, x_0)\mu(E_{x_0}) + \sum_{a,b} \pi(x_0, x_0)\lambda(x_0, x_0, a, b)\ \tau(E_{x_0,a}E_{x_0,b})$$

where $no(x_0)$ denotes a function which has no dependence on x_0 and $\mu(E_x) := \tau(\sum_a E_{x,a}Q_{x,a})$.

Proof. This is a straightfoward decomposition of the sum defining ϕ. □

We are setting about to derive the optimality conditions in Proposition 4.7.3 and wish to maximize $\phi(E)$ over E which are POVMs. In this context we are assuming that $\lambda(x_0, x_0, a, a) = 1$, that λ is synchronous, and we analyse a maximizer E_x which is a PVM, hence by Lemma 4.3 we get $\phi(E) = no(x_0) + \pi(x_0, x_0)\mu(E_{x_0}) + \pi(x_0, x_0)\tau(I)$ and emphasize that the first and last terms of ϕ are constant with respect to E_{x_0}. Thus optimality conditions for Proposition 4.7.3 are the same as for the less encumbered problem: Fix x_0

$$\max_{E_{x_0}\ a\ POVM} \mu(E_{x_0}).$$

This is equivalent to: maximize

$$\tau(\sum_{a=0}^{k-2} E_{x_0,a}(Q_{x_0,a} - Q_{x_0,k-1}) +\ \tau(\ Q_{x_0,k-1}\ )$$

over $E_{x_0,0} \geq 0, \ldots, E_{x_0,k-1} \geq 0$ subject to $E_{x_0,k-1} = I - (E_{x_0,0} + \cdots + E_{x_0,k-2}) \geq 0$. We call this the core problem.

This is a Semi Definite Program (SDP) over a domain with interior whose dual SDP is

$$\min_{R} \tau(R^{(k-1)(k-1)}) \tag{4.7.3}$$

subject to

1. $R \in \mathbb{R}^{Nk \times Nk},\ R \geq 0$ with R partitioned as

$$R =: \begin{pmatrix} R^{00} & \dots & R^{0(k-1)} \\ \vdots & \ddots & \vdots \\ R^{(k-1)0} & \dots & R^{(k-1)(k-1)} \end{pmatrix}$$

2. $R^{aa} - R^{(k-1)(k-1)} = -Q_{x_0,a} + Q_{x_0,k-1}$

The off diagonal terms of R are irrelevant and we ignore them from now on.

Here the standard Primal -Dual Optimality Conditions, see [138], have the following form.

Lemma 4.4. *If the POVM E_x and the dual optimizer R exist (i.e. the optimum is achieved) for the core problem, then these are satisfied for all a:*

1. $R^{aa} \geq 0$

2. $R^{aa} E_{x_0,a} = 0 = E_{x_0,a} R^{aa}$

3. $R^{aa} - R^{(k-1)(k-1)} = -Q_{x_0,a} + Q_{x_0,k-1}$ *for all a.*

Proof of Proposition 4.7.3 Proposition 4.7.3 follows from Lemma 4.4 as we now see. First observe that $R^{aa} - R^{bb} = -Q_{x_0,a} + Q_{x_0,b}$, because

$$R^{aa} - R^{bb} = R^{aa} - R^{(k-1)(k-1)} - (R^{bb} - R^{(k-1)(k-1)}).$$

From this we get $\Omega_{x_0} - Q_{x_0,b} = R^{bb} \geq 0$ for all b, because

$$\sum_a E_{x_0,a}(Q_{x_0,a} - Q_{x_0,b}) = -\sum_a E_{x_0,a}R^{aa} + \sum_a E_{x_0,a}R^{bb}$$
$$\Omega_{x_0} - Q_{x_0,b} = +\sum_a E_{x_0,a}R^{bb} = R^{bb}.$$

The optimality conditions have been proved.

Now we turn to the last claim in the proposition. Letting $\omega_{povm}(G, \pi)$ denote the max value of the game over all densities of the form $\tau(E_{x,a}E_{y,b})$ for POVMs $\{E_{x,a}\}$ in a finite dimensional von Neumann algebra with a trace τ, the last assertion of the proposition operates under assumptions which imply

$$\omega_q^s(G, \pi) \leq \omega_{povm}(G, \pi) \leq \omega_{qc}(G, \pi) = \omega_q(G, \pi);$$

the second inequality following from Lemma 5.2 of [137]. Thus our maximizing PVM strategy is also a POVM maximizer which amounts to the (demanding) hypothesis of Proposition 4.7.3. □

References

[1] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy, "Interactive proofs and the hardness of approximating cliques," *J. ACM*, vol. 43, no. 2, 268–292, Mar. 1996.

[2] S. Arora and S. Safra, "Probabilistic checking of proofs: A new characterization of np," *J. ACM*, vol. 45, no. 1, pp. 70–122, Jan. 1998.

[3] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, "Proof verification and the hardness of approximation problems," *J. ACM*, vol. 45, no. 3, 501–555, May 1998.

[4] L. Babai, L. Fortnow, and C. Lund, "Non-deterministic exponential time has two-prover interactive protocols," *computational complexity*, vol. 1, no. 1, pp. 3–40, 1991.

[5] R. Raz, "A parallel repetition theorem," in *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing*, ser. STOC '95, Las Vegas, Nevada, USA: Association for Computing Machinery, 1995, 447–456, ISBN: 0897917189.

[6] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson, "Multi-prover interactive proofs: How to remove intractability assumptions," in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, ser. STOC '88, Chicago, Illinois, USA: ACM, 1988, pp. 113–131, ISBN: 0-89791-264-0.

[7] L. Mančinska and D. E. Roberson, "Quantum homomorphisms," *Journal of Combinatorial Theory, Series B*, vol. 118, pp. 228–267, 2016.

[8] A. Atserias, L. Mančinska, D. E. Roberson, R. Šámal, S. Severini, and A. Varvitsiotis, "Quantum and non-signalling graph isomorphisms," *Journal of Combinatorial Theory, Series B*, vol. 136, pp. 289–328, 2019.

[9] L. Mančinska and D. E. Roberson, "Quantum isomorphism is equivalent to equality of homomorphism counts from planar graphs," in *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, 2020, pp. 661–672.

[10] P. J. Cameron, A. Montanaro, M. W. Newman, S. Severini, and A. Winter, *On the quantum chromatic number of a graph*, 2006. arXiv: `quant-ph/0608016 [quant-ph]`.

[11] G. Scarpa and S. Severini, "Kochen–specker sets and the rank-1 quantum chromatic number," *IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2524–2529, 2012.

[12] 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.

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

[14] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, "$\mathsf{MIP}^* = \mathsf{RE}$," *arXiv preprint arXiv:2001.04383*, 2020.

[15] J. Canny, "Some algebraic and geometric computations in PSPACE," ser. STOC '88, Chicago, Illinois, USA: Association for Computing Machinery, 1988, 460–467, ISBN: 0897912640.

[16] S. J. Harris, *Universality of graph homomorphism games and the quantum coloring problem*, 2023. arXiv: `2305.18116 [quant-ph]`.

[17] 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.

[18] D. Mermin, "Simple unified form for the major no-hidden-variables theorems," *Physical Review Letters*, vol. 65, no. 27, p. 3373, 1990.

[19] A. Peres, "Incompatible results of quantum measurements," *Physics Letters A*, vol. 151, no. 3-4, pp. 107–108, 1990.

[20] 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.

[21] 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.

[22] D. Cui, L. Mančinska, S. S. Nezhadi, and D. E. Roberson, *Quantum perfect matchings*, 2025. arXiv: `2502.05136 [quant-ph]`.

[23] O. Goldreich, *Introduction to Property Testing*. Cambridge University Press, 2017.

[24] T. Ito and T. Vidick, "A multi-prover interactive proof for nexp sound against entangled provers," in *Proceedings of the 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, ser. FOCS '12, Washington, DC, USA: IEEE Computer Society, 2012, pp. 243–252, ISBN: 978-0-7695-4874-6.

[25] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, "Quantum soundness of testing tensor codes," *Forthcoming draft*, 2021.

[26] 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.

[27] A. Natarajan and T. Vidick, "A quantum linearity test for robustly verifying entanglement," in *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, ser. STOC 2017, Montreal, Canada: ACM, 2017, pp. 1003–1015, ISBN: 978-1-4503-4528-6.

[28] 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.

[29] Z. Ji, *Binary constraint system games and locally commutative reductions*, 2013. arXiv: `1310.3794 [quant-ph]`.

[30] I. Holyer, "The np-completeness of edge-coloring," *SIAM Journal on Computing*, vol. 10, no. 4, pp. 718–720, 1981.

[31] E. R. Scheinerman and D. H. Ullman, *Fractional Graph Theory: a Rational Approach to the Theory of Graphs*. Minola, N.Y.: Dover Publications, 2013, ISBN: 9780486292137 0486292134.

[32] J. W. Helton, H. Mousavi, S. S. Nezhadi, V. I. Paulsen, and T. B. Russell, "Synchronous Values of Games," *Annales Henri Poincare*, vol. 25, no. 10, pp. 4357–4397, 2024. arXiv: `2109.14741 [quant-ph]`.

[33] W. T. Tutte, "The Factorization of Linear Graphs," *Journal of the London Mathematical Society*, vol. s1-22, no. 2, pp. 107–111, Apr. 1947. eprint: `https://academic.oup.com/jlms/article-pdf/s1-22/2/107/2624763/s1-22-2-107.pdf`.

[34] L. Maninska, D. E. Roberson, and A. Varvitsiotis, "On deciding the existence of perfect entangled strategies for nonlocal games," *Chic. J. Theor. Comput. Sci.*, vol. 2016, 2015.

[35] D. E. Roberson, "Variations on a theme: Graph homomorphisms," 2013.

[36] P. Lisonek, P. Badziag, J. R. Portillo, and A. Cabello, "Kochen-specker set with seven contexts," *Physical Review A*, vol. 89, no. 4, Apr. 2014.

[37] C. Berge, *Hypergraphs - combinatorics of finite sets* (North-Holland mathematical library). North-Holland, 1989, vol. 45, ISBN: 978-0-444-87489-4.

[38] W. Slofstra, "The set of quantum correlations is not closed," in *Forum of Mathematics, Pi*, Cambridge University Press, vol. 7, 2019.

[39] A. Connes, “Classification of injective factors cases II_1, II_∞, III_λ, $\lambda \neq 1$,” *Annals of Mathematics*, pp. 73–115, 1976.

[40] N. Ozawa, “About the Connes embedding conjecture: Algebraic approaches.,” *Jpn. J. Math.*, vol. 8, 147–183, 1 2013.

[41] V. B. Scholz and R. F. Werner, “Tsirelson’s problem,” *arXiv preprint arXiv:0812.4305*, 2008.

[42] T. Fritz, “Tsirelson’s problem and Kirchberg’s conjecture,” *Reviews in Mathematical Physics*, vol. 24, no. 05, p. 1 250 012, 2012.

[43] 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.

[44] 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.

[45] 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.

[46] S. Pironio *et al.*, “Random numbers certified by Bell’s theorem,” *Nature*, vol. 464, no. 7291, pp. 1021–1024, 2010.

[47] T. Netzer and A. Thom, “Hyperbolic polynomials and generalized Clifford algebras,” *Discrete & Computational Geometry*, vol. 51, no. 4, pp. 802–814, 2014.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] I. Goldbring and B. Hart, "A computability-theoretic reformulation of the Connes Embedding Problem," *arXiv preprint arXiv:1308.2638*, 2013.

[54] 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.

[55] M. Coudron and A. Natarajan, "The parallel-repeated magic square game is rigid.," Sep. 2016.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

[60] 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.

[61] B. Blackadar, *Operator algebras: theory of C^*-algebras and von Neumann algebras*. Springer Science & Business Media, 2006, vol. 122.

[62] 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.

[63] M. de la Salle, "Orthogonalization of positive operator valued measures," *arXiv preprint arXiv:2103.14126*, 2021.

[64] 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.

[65] I. Šupić and J. Bowles, "Self-testing of quantum systems: A review," *Quantum*, vol. 4, p. 337, 2020.

[66] P. Aravind, "A simple demonstration of Bell's theorem involving two observers and no probabilities or inequalities," *arXiv preprint quant-ph/0206070*, 2002.

[67] 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.

[68] V. Jones, *von Neumann Algebras*, `https://math.berkeley.edu/~vfr/VonNeumann2009.pdf`, 2009.

[69] 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.

[70] C. H. Papadimitriou, *Computational Complexity*. Addison-Wesley, 1994.

[71] N. D. Jones, *Computability and complexity: from a programming perspective*. MIT press, 1997, vol. 21.

[72] 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.

[73] 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.

[74] 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.

[75] J. S. Bell, "On the einstein-podolsky-rosen paradox.," *Physics*, vol. 1, p. 195, 1964.

[76] 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`.

[77] 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`.

[78] 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.

[79] A. Natarajan and J. Wright, "Neexp in mip," *ArXiv*, vol. abs/1904.05870, 2019, https://doi.org/10.1109/focs.2019.00039.

[80] 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.

[81] 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.

[82] 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.

[83] 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.

[84] I. Supić and J. Bowles, "Self-testing of quantum systems: A review.," https://doi.org/10.22331/q-2020-09-30-337, 2019.

[85] 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.

[86] 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.

[87] B. Tsirelson, "Some results and problems on quantum bell-type inequalities.," *Hadronis Journal Supplement*, vol. 8, pp. 320–331, 1993.

[88] 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.

[89] 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`.

[90] M. Coudron and A. Natarajan, "The parallel-repeated magic square game is rigid," arXiv:1609.06306 [quant-ph], 2016.

[91] 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`.

[92] 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`.

[93] 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`.

[94] A. Natarajan and T. Vidick, "Robust self-testing of many-qubit states.," in *STOC*, `https://doi.org/10.1038/s41534-018-0120-0`, 2017.

[95] A. Coladangelo, "Parallel self-testing of (tilted) epr pairs via copies of (tilted) chsh," *Quantum Information and Computation*, vol. 17, p. 35, 2016.

[96] M. Mckague, "Self-testing in parallel with chsh," *Quantum*, vol. 1, 2016, `https://doi.org/10.22331/q-2017-04-25-1`.

[97] 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.

[98] A. Coladangelo and J. Stark, "Robust self-testing for linear constraint system games.," in *QIP 2018*, 2018.

[99] 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`.

[100] 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`.

[101] T. Vidick, "A simplified analysis on robust self-testing of *n* epr pairs.," Available at `http://users.cms.caltech.edu/~vidick/`, 2018.

[102] 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`.

[103] 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`.

[104] 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]`.

[105] 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.

[106] 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.

[107] 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.

[108] J. Kaniewski, "Weak form of self-testing," *Physical Review Research*, vol. 2, no. 3, 2020.

[109] L. Mančinska, T. G. Nielsen, and J. Prakash, *Glued magic games self-test maximally entangled states*, 2021. arXiv: `2105.10658 [quant-ph]`.

[110] J. Watrous, *The Theory of Quantum Information.* Cambridge University Press, 2018, `https://doi.org/10.1017/9781316848142`.

[111] I. Chuang and M. Nielsen, *Quantum Computation and Quantum Information.* Cambridge University Press, 2010, `https://doi.org/10.1017/CBO9780511976667`.

[112] 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.

[113] 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`.

[114] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy, "Interactive proofs and the hardness of approximating cliques," *J. ACM*, vol. 43, no. 2, 268–292, Mar. 1996.

[115] N. D. Mermin, “Simple unified form for the major no-hidden-variables theorems.,” *Phys. Rev. Lett.*, vol. 65, no. 27, p. 3373, 1990.

[116] O. Regev and T. Vidick, “Quantum xor games,” vol. 7, no. 4, 2015.

[117] R. Cleve and R. Mittal, “Characterization of binary constraint system games.,” in *International Colloquium on Automata, Languages, and Programming (ICALP) 2012*, 2012, 320–331.

[118] R. Cleve, L. Liu, and W. Slofstra, “Perfect commuting-operator strategies for linear system games.,” *Journal of Mathematical Physics*, vol. 58, no. 012202, 2017.

[119] K. Dykema, V. I. Paulsen, and J. Prakash, “Non-closure of the Set of Quantum Correlations via Graphs,” *Communications in Mathematical Physics*, vol. 365, no. 3, pp. 1125–1142, Feb. 2019.

[120] M. Musat and M. Rørdam, “Non-closure of quantum correlation matrices and factorizable channels that require infinite dimensional ancilla (with an appendix by narutaka ozawa),” *Communications in Mathematical Physics*, vol. 375, pp. 1761 –1776, 2018.

[121] A. Coladangelo, “A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations,” *Quantum*, vol. 4, p. 282, Jun. 2020.

[122] A. Coladangelo and J. Stark, “Unconditional separation of finite and infinite-dimensional quantum correlations,” *journal=arXiv preprint arxiv:1804.05116*, 2018.

[123] M. Laurent, “Semidefinite relaxations for max-cut,” in *The sharpest cut* (MPS-SIAM series on optimization), M. Grötschel, Ed., MPS-SIAM series on optimization. Society for Industrial and Applied Mathematics, 2004, pp. 291–327, Pagination: 37, ISBN: 0898715520.

[124] 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.

[125] V. I. Paulsen and I. G. Todorov, “Quantum chromatic numbers via operator systems,” *Quarterly Journal of Mathematics*, vol. 66, pp. 677–692, 2013.

[126] C. Palazuelos and T. Vidick, “Survey on nonlocal games and operator space theory,” *Journal of Mathematical Physics*, vol. 57, no. 1, Jan. 2016.

[127] J. Cuntz and G. Kjærgård Pedersen, “Equivalence and traces on c-algebras,” *Journal of Functional Analysis*, vol. 33, no. 2, pp. 135–164, 1979.

[128] R. Karp, “Reducibility among combinatorial problems,” vol. 40, Jan. 1972, pp. 85–103, ISBN: 978-3-540-68274-5.

[129] S. A. Kruglyak, V. I. Rabanovich, and Y. S. Samoilenko, “On sums of projections,” *Functional Analysis and Its Applications*, vol. 36, no. 3, 182–195, Jul. 2002.

[130] B. Tsirelson, “Some results and problems on quantum bell-type inequalities.,” *Hadronis Journal Supplement*, vol. 8, pp. 320–331, 1993.

[131] V. I. Paulsen, *Entanglement and non-locality online course notes*.

[132] R. Cleve, P. Høyer, B. Toner, and J. Watrous, “Consequences and limits of nonlocal strategies.,” p. 25, 2004.

[133] M. Slater, “Lagrange multipliers revisited,” *Cowles Commission Discussion*, no. 403, 1950.

[134] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed. Cambridge University Press, 2012.

[135] V. Paulsen, *Completely Bounded Maps and Operator Algebras*. Feb. 2003, ISBN: 9780521816694.

[136] L. Mančinska, V. I. Paulsen, I. G. Todorov, and A. Winter, “Products of synchronous games,” *Studia Mathematica*, vol. 272, no. 3, 299–317, 2023.

[137] E. Alhajjar and T. B. Russell, “Maximally entangled correlation sets,” *arXiv: Quantum Physics*, 2020.

[138] F. Alizadeh, J.-P. Haeberly, and M. Overton, “Complementarity and nondegeneracy in semidefinite programming,” *Mathematical Programming*, vol. 77, May 1995.