Entanglement and Non-Locality in Games and Graphs

Arthur Mehta

Abstract

This thesis is primarily based on two collaborative works written by the author and several coauthors. These works, presented in Chapters 4 and 5, are on the topics of quantum graphs, and self-testing via non-local games respectively.

Quantum graph theory, also known as non-commutative graph theory, is an operator space generalization of graph theory. The independence number, and Lovász theta function were generalized to this setting by Duan, Severini, and Winter [DSW13] and two different version of the chromatic number were introduced by Stahlke [Sta16] and Paulsen [HPP16]. In Chapter 4, we introduce two new generalizations of the chromatic number to non-commutative graphs and provide an upper bound on the parameter of Stahlke. We provide a generalization of the graph complement and show the chromatic number of the orthogonal complement of a non-commutative graph is bounded below by its theta number. We also provide a generalization of both Sabidussi's Theorem and Hedetniemi's conjecture to non-commutative graphs.

The study of non-local games considers scenarios in which separated players collaborate to provide satisfying responses to questions given by a referee. The condition of separating players makes non-local games an excellent setting to gain insight into quantum phenomena such as entanglement and non-locality. Non-local games can also provide protocols known as self-tests. Self-testing allows an experimenter to interact classically with a black box quantum system and certify that a specific entangled state was present and a specific set of measurements were performed. The most studied self-test is the CHSH game which certifies the presence of a single EPR entangled state and the use of anti-commuting Pauli measurements. In Chapter 5, we introduce an algebraic generalization of CHSH and obtain a self-test for non-Pauli operators resolving an open question posed by Coladangelo and Stark (QIP 2017). Our games also provide a self-test for states other than the maximally entangled state, and hence resolves the open question posed by Cleve and Mittal (ICALP 2012).

The results of Chapter 5 make use of sums of squares techniques in the settings of group rings and $*$-algebras. In Chapter 3, we review these techniques and discuss how they relate to the study of non-local games. We also provide a weak sum of squares property for the ring of integers $\mathbb{Z}^n$. In particular we show that if $b \in \mathbb{C}[\mathbb{Z}^n]$ is hermitian and positive under all unitary representations then it must be expressible as a sum of hermitian squares.

Chapter 1

Introduction

Quantum information theory (QIT) is a study that examines the nature of information processing that is governed by quantum mechanics. As a field of study, it sits at the cross roads of many different scientific specializations including theoretical physics, theoretical computer science and pure mathematics. Each of these specializations provides unique viewpoints and can differ from one another in terms of notational conventions, style, and philosophical outlook. These differences make collaboration between experts both challenging and profitable to the study of QIT.

The goal of this thesis is to highlight collaboration across different specializations by using their differing motives and techniques to ask new questions and obtain new results. These results are largely based on two collaborative research projects, written by the author and various coauthors, on the topics of *quantum graphs* and *non-local games* [KM19], [CMMN20]. Each of these projects has been accepted for publication in reputable academic journals and they are presented in this form in Chapters 4 and 5. In Chapter 1, we give a high level introduction to *self-testing* through *non-local games* and the topic of *quantum graphs*. We discuss how each of these works connects with the goal of collaboration across different disciplines.

Providing the correct mathematical framework is one of the most important contributions mathematics can provide to the interdisciplinary study of QIT. In the absence of a complete mathematical theory related results may appear disconnected and techniques can come across as ad hoc instead of generalizable. Chapters 2 and Chapter 3 highlight this contribution. Chapter 2 is not original work but serves to provide a reference for an often overlooked discussion on the operator theory foundations of QIT. In Chapter 3, we visit the topic of *sums of squares* in the context of group algebras. Chapter 3 contains some new results and this chapter concludes by connecting the topic of sums of squares to techniques used in Chapter 5.

1.1 Non-locality and Self-testing

In May of 1935, Albert Einstein, along with his two postdoctoral students Boris Podolsky and Nathan Rosen (EPR), published their now famous paper *Can Quantum Mechanical Description of Physical Reality Be Considered Complete?* [EPR35]. This paper planted the seed for one of the most intense scientific debates of the 20-th century. Einstein, Podolsky and Rosen were motivated by the possible implications of the Heisenberg uncertainty principle. This principle claims that there are pairs of incompatible measurements of a state that cannot both be known with certainty. Mathematically, this principle was derived from an operator theory description of quantum mechanics which represents measurements as operators on a Hilbert space. This was a severe divergence from classical mechanics which presupposes that there must be an underlying "reality" of any observable quantity of a given state. Consequently, Einstein, Podolsky and Rosen argue that the prevailing operator theory formalism of quantum mechanics was an incomplete description of reality. In an effort to show this description was incomplete they propose the following thought experiment.

Two scientists, Alice and Bob, are spatially separated and each possess one of a pair of entangled particles. Alice and Bob can each make one of two possible incompatible measurements, call these measurements $M_{|0\rangle,|1\rangle}$ and $M_{|+\rangle,|-\rangle}$. A global state, $|EPR\rangle$, is used to jointly describe separated systems of Alice and Bob. If Alice first applies measurement $M_{|0\rangle,|1\rangle}$ and observes outcome $i \in \{0,1\}$ then Bob's state would have collapsed so that his measurement outcome with respect to $M_{|0\rangle,|1\rangle}$ would also be i with probability 1. Similarly, if Alice first applies the second measurement and observes outcome $j \in \{+,-\}$ then Bob's state would also measure as outcome j with certainty. Einstein et al. go on to argue that this shows that Bob's particle must have the value for each of the two measurements predetermined and the current quantum mechanical description is thus incomplete. A central assumption in this reasoning is the idea of locality, which purports that if Alice and Bob are spatially separated then measurements conducted by Alice can not affect the underlying "reality" of Bob's particle.

Is it possible to replace the prevailing operator theory formalism of quantum mechanics with a more complete model that is compatible with the assumption of locality? This was the challenge implicit in the work of Einstein, Podolsky and Rosen. At a high level, this question is concerned with the appropriate mathematical framework to describe quantum mechanics. The possibility of a framework for quantum mechanics that is also consistent with classical physics was eventually refuted by Bell in his landmark work *On the Einstein-Podolsky-Rosen paradox* [Bel64]. Bell's theorem was later simplified using *non-local games* [CHSH69].

1.1.1 Non-Local Games

In a non-local game two cooperating players, Alice and Bob, interact with a third party known as the verifier. The game consists of two sets of questions, one for each player, and two sets of possible answers, again one for each player. The rules of the game simply consists of an assignment of win or lose to each possible 4-tuple of questions and answers for each player. Prior to the start of the game the rules are known to all players and Alice and Bob are given an opportunity to agree upon a strategy. Once the game is to begin, the players are spatially separated so as to prohibit any communication between Alice and Bob. This condition of separation can be viewed as a non-locality condition. The verifier then randomly selects and provides one question to each player and receives one response from each player. The players are then determined to win or lose based upon the rules. For a more formal description of non-local games please see Section 5.2.2.

In their celebrated paper [CHSH69] Clauser, Horne, Shimony, and Holt show that the scenario described above is a compelling setting to probe the limitations of locality and the implications of quantum entanglement. They consider the following game, widely known as the CHSH game. The question and answer set for each player is simply the set $\mathbb{Z}_2$, the integers modulo 2. Suppose Alice is given question x and returns answer a, and Bob is given question y and returns answer b. The rules of the game simply state that the players win precisely when $xy = a + b$. That is, the players win if the sum of their answers is congruent modulo 2 to the product of their questions.

If Alice and Bob are using a deterministic strategy for the CHSH game then they can't hope to win with a probability greater then 0.75. If instead the players are allowed to form a strategy based on the formalism of quantum mechanics then one can ask if the players can develop a strategy that wins the CHSH game with a probability greater then 0.75. This is exactly what is shown in [CHSH69] where the authors describe a quantum strategy for the CHSH game that can win with probability of approximately 0.85.

This deep insight was able to propel the debate first started by Einstein, Podolsky and Rosen from the setting of thought experiment to the setting of experimentally verifiable science. The idea is to run a real life version of this game and try to experimentally demonstrate a strategy that wins with a higher probability than 0.75. Indeed, such experiments have been conducted and consequently demonstrated a refutation of a classical description of the quantum world, see for example [CS78].

Since the innovation of the CHSH game, many more non-local games have been studied in the context of quantum information theory. Examples include XOR games [CSUU07], linear constraint system games [CM12], graph parameter [PHMS19] and graph isomorphism games [AMR^{+}19]. The study of these games has wide ranging applications across many different fields of study that intersect with QIT. As we have already remarked, non-local games play a central role in theoretical and experimental physics as they can be used to refute the possibility of a classical description of quantum mechanics. Cryptographers can use non-local games to exploit the intrinsic randomness of quantum mechanics to certify randomness for cryptographic protocols [VV12]. Further applications are found in theoretical computer science, where non-local games can be used to define interesting complexity classes [CHTW04]. Surprisingly, non-local games have also been shown to have powerful implications for deep problems within pure mathematics. This is probably best illustrated by the recent resolution to the long standing Connes' embedding problem from the theory of von Neumann algebras [JNV^{+}20]. In this work the authors introduce a game that can distinguish between two different mathematical formalisms for quantum strategies of non-local games and hence resolve Connes' embedding problem through a sequence of equivalent conjectures. For a good discussion on the connections between these equivalent conjectures see [Vid19].

1.1.2 Self-Testing

The fact that a simple game can be used to refute the possibility for a classical description of quantum mechanics is indeed one of the crowning achievements of scientific discovery during the 20-th century. This shows that if Alice and Bob use the building blocks of quantum mechanics, i.e., states and measurement operators, then they can outperform any deterministic strategy in the CHSH game. A more subtle question to ask is what are the possible states and measurement operators that Alice and Bob can use to win with the highest possible probability.

The mathematical formalism used to model *quantum strategies* for non-local games is described in Chapter 2.6. In the context of the CHSH game, we know that each quantum strategy employed by Alice and Bob corresponds to a quantum state $|\psi\rangle$ in some Hilbert space $\mathcal{H}$, and order 2 unitaries A_0, A_1 for Alice and B_0, B_1 for Bob acting on $\mathcal{H}$. The condition of locality also requires that Alice's operators commute with Bob's. We consider the *bias* for this strategy, β, which is given by,

$$\beta = \langle \psi | A_0 B_0 + A_1 B_0 + A_0 B_1 - A_1 B_1 | \psi \rangle. \tag{1.1.1}$$

The probability of winning, ω, can be determined from the bias since $\beta = 8\omega - 4$.

The optimal winning value for the CHSH game can be shown to be $\frac{1}{4}(\sqrt{2} + 2)$. One way this can be seen is through the use of *sum of squares proofs*. The theory of sums of squares techniques, and how they relate to non-local games more generally, is discussed in detail in Chapter 3.4. Using these techniques we can determine an upper bound on ω of $\frac{1}{4}(\sqrt{2}+2)$ since,

$$\begin{aligned}2\sqrt{2}I-(A_0B_0+A_0B_1+A_1B_0-A_1B_1)&=\frac{\sqrt{2}}{4}\left(A_0+A_1-\sqrt{2}B_0\right)^2\\&+\frac{\sqrt{2}}{4}\left(A_0-A_1-\sqrt{2}B_1\right)^2\geq 0.\end{aligned}$$

Thus we see that $2\sqrt{2}$ is an upper bound on the bias. Interestingly, in the case of the CHSH game there is a unique state and set of measurement operators that must be used in order to win with the highest possible probability. The above sum of squares decomposition can also be used to show this fact. Indeed, if this upper-bound is saturated with the state $|\psi\rangle$ then we have,

$$B_0|\psi\rangle=\frac{1}{\sqrt{2}}(A_0+A_1)|\psi\rangle,\quad\text{and}\quad B_1|\psi\rangle=\frac{1}{\sqrt{2}}(A_0-A_1)|\psi\rangle. \tag{1.1.2}$$

Using the above identities we can show that B_0 and B_1 must anti-commute with respect to $|\psi\rangle$:

$$\begin{aligned}\sqrt{2}\left(B_0B_1+B_1B_0\right)|\psi\rangle&=\left(B_0(A_0-A_1)+B_1(A_0+A_1)\right)|\psi\rangle\\&=(A_0-A_1)B_0+(A_0+A_1)B_1)|\psi\rangle\\&=((A_0-A_1)(A_0+A_1)+(A_0+A_1)(A_0-A_1))|\psi\rangle\\&=(A_0A_1-A_1A_0+A_1A_0-A_0A_1)|\psi\rangle\\&=0.\end{aligned}$$

Thus B_0 and B_1 anti-commute, that is $-(B_0B_1)^2=I$, with respect to a semi-norm induced by $|\psi\rangle$. We can similarly show A_0 and A_1 anti-commute. These anti-commuting relations, along with the fact that B_0 and B_1 are order two unitaries, allow us to relate optimal quantum strategies to the representation theory for the group G, given by the following presentation.

$$G=\left\langle X,Y,J\mid X^2,Y^2,J^2,J(YZ)^2,JXJ^{-1}X^{-1},JYJ^{-1}Y^{-1}\right\rangle.$$

In particular if $|\psi\rangle,A_0,A_1,B_0,B_1$ is any quantum strategy that wins with a probability of $\frac{1}{4}(\sqrt{2}+2)$ then the map $(X,Y,J)\mapsto(A_0,A_1,-I)$ determines what we refer to as a $|\psi\rangle$-representation for G. For detail on $|\psi\rangle$-representations, please see Definition 5.2.2. Alternatively, a $|\psi\rangle$-representation can be viewed as a representation of G, in the usual sense. If we let $\mathcal{K}$ denote the subspace of $\mathcal{H}$ that is generated by words in A_0,A_1 applied to $|\psi\rangle$, then the map $(X,Y,J)\mapsto(A_0|_{\mathcal{K}},A_1|_{\mathcal{K}},-I)$ determines a representation of G on $\mathcal{K}$. A similar reasoning can be applied to the operators of Bob. Furthermore, there is a unique irreducible representation of G satisfying $J\mapsto -I$ given by

$$X\mapsto\sigma_X=\begin{bmatrix}0&1\\1&0\end{bmatrix},Y\mapsto\sigma_Y=\begin{bmatrix}0&-i\\i&0\end{bmatrix}.$$

An application of Theorem 5.2.3 and Lemma 5.2.4 tells us that the operators of Alice and Bob, up to an application of an isometry, act as σ_X and σ_Y on the state $|\psi\rangle$. We can also determine that the state $|\psi\rangle$, up to an application of local isometry, is of the form $|\psi\rangle'\otimes|junk\rangle$. Where $|\psi\rangle'$ is given by,

$$|\psi\rangle'=\frac{1}{\sqrt{4+2\sqrt{2}}}\left(\left(1+\frac{1-i}{\sqrt{2}}\right)|00\rangle-\left(1+\frac{1+i}{\sqrt{2}}\right)|11\rangle\right).$$

This strategy can be seen to be unitarily equivalent to the more standard one presented with $A_0=\sigma_X\otimes I, A_1=\sigma_Z\otimes I$ and $|\psi\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. This shows that the CHSH game can be used to develop a protocol that can certify the maximally entangled state on two qubits and Pauli operators σ_X and σ_Z. Such certification protocols are often referred to as *self-testing* protocols and non-local games that can be used for such protocols are called *rigid*.

The above discussion on the self-testing properties of CHSH is fairly technical and it is important to not miss the forest for the trees here. This result tells us that if Alice and Bob want to employ a strategy that wins the CHSH game with highest possible winning probability, then they are greatly constrained in their choice of strategy. Firstly, we know that they must employ a quantum strategy and take advantage of an entangled state. Furthermore, in a strong sense, there is a unique quantum state and set of measurements that they must use. Astonishingly, all of this information can be determined by the exchange of classical information in form of the questions and answers.

More realistically, such a set up is unlikely to be realised with actual players named Alice and Bob. Instead one can use these results to develop a protocol where by classical interaction with two separated black box quantum systems can certify the presence of a particular entangled state or measurement operators.

It is not hard to imagine that engineers and people in the applied sciences may one day make use of these protocols as important building blocks of technologies that exploit the nature of quantum mechanics. Indeed, these protocols can allow scientists to certify what state they have their hands on and what measurements were actually performed when working in lab.

Aside from the potential technological implications of such results, there is also an appealing aesthetic motivation here. Self-testing results, such as the one discussed above for CHSH, rely on the natural relations and symmetries of groups. In the case of CHSH, the proof requires the establishment of the anti-commuting relations. These types of results allow for protocols where one can certify the presence of group relations and symmetries in nature.

The main goal of the work contained in Chapter 5 was to explore several natural questions within the topic of self-testing. Precise formulations of these questions are detailed in Section 5.1. We also refer the reader to this chapter for a discussion of what was previously known in the literature regrading these questions.

Question 1.1.1. *What states can we self-test for using non-local games?*

Question 1.1.2. *What operators can we self-test for using non-local games?*

Question 1.1.3. *Can we use non-local games to certify the presences of certain algebraic relations amongst operators?*

Question 1.1.4. *In what ways is it possible for a non-local game to fail to provide a self-test protocol for any set of operators or state?*

Several of the above questions were suggested to the authors of [CMMN20] by Professor Henry Yuen at the outset of a summer research project in 2019. This research project would eventually become the work presented in Chapter 4. Although the work does not provide a complete answer to any of the above questions, it does provide a substantial addition to what is known to the scientific community regarding these questions. In order to obtain these results, we introduce a new family of non-local games that can be realised as generalizations of the CHSH game to $\mathbb{Z}_n$, the ring of integers modulo n. Different generalizations of the CHSH game have been studied before but proved to be less amenable to analysis [BS15]. We show that this family of games all have quantum strategies that outperform the best classical strategy. We obtain our results on self-testing by employing a collection of techniques sometimes referred to as sum of square proofs. Combining these techniques with representation theory of finite groups and a powerful theorem due to Gowers and Hatami [GH17] we are able to obtain our results on the topic of self-testing for our game in the case $n = 3$. Since Chapter 5 already contains an extensive introduction we direct readers to 5.1 for more detailed discussion of this work.

1.2 Quantum Graphs

Chapter 4 focuses on a collection of results on a topic sometimes referred to as quantum graph theory. Quantum graph theory is an operator space generalization of graph theory that was initially motivated by work both in complexity theory [SB07] and physics [DSW13]. In order to understand these motives, we first discuss the well known connections between noisy channels, graph theory, and complexity theory. We also note that quantum graph theory has appeared in the literature as non-commutative graph theory, which is the name that is used in Chapter 4.

1.2.1 Noisy channels and graphs

Suppose Alice uses a finite alphabet $A = \{a_1, a_2 \ldots a_n\}$ to send messages through a *noisy channel* to Bob, who receives them as letters from his finite alphabet $B = \{b_1, b_2, \ldots, b_m\}$. We can represent the noisy channel by a matrix $N = (P(b_i|a_j))$, where $P(b_i|a_j)$ determines the probability that Bob receives letter b_i given that Alice sent a_j. The study of the *zero-error capacity* of such noisy channels was first due to Shannon [Sha56]. Here we define the zero-error capacity of channel N as the maximum number of $a_i \in A$ that Alice can send through the channel such that Bob knows exactly what was sent. In other words, this is the size of the largest collection $a_{i_1}, \ldots a_{i_m} \in A$ such that for any $b_k \in B$ we have $p(b_k|a_{i_j})p(b_k|a_{i_k}) = 0$ for all choices of $j \neq k$.

The study of zero-error capacity and similar notions of channel capacity are important for information theory and have led to foundational results such as Shannon's noisy channel coding theorem [Sha48]. Graph theory is an important tool in this analysis. For our purposes we will only consider loop-free, undirected graphs. A graph G will be a an ordered pair $G = (V, E)$ consisting of a finite set of vertices V and $E \subset V \times V$ such that if $(e_i, e_j) \in E$ then $i \neq j$ and $(e_j, e_i) \in E$. Given a noisy channel $N = (P(b_i|a_j))$ we can construct an associated graph, G_N, known as the *confusability graph* of the channel. This graph will have vertices consisting of Alice's alphabet, $V = A$, and for $i \neq j$ we have $(a_i, a_j) \in E$ precisely when $P(b_k|a_i)P(b_k|a_j) \neq 0$ for some $b_k \in B$. It is not hard to make the observation that the *independence number*, $\alpha(G_N)$, is equal to the zero error capacity of the noise channel N.

Another important parameter of a noisy channel N is the so called *least packing number*. Suppose in addition to her noisy channel N, Alice also has a separate, expensive, yet noise free channel M that she can use to send information to Bob. The least packing number of N tells us how much extra information Alice needs to send through M such that she can use her entire alphabet A without the potential for any errors. More formally, suppose Alice has two finite alphabets A and C that she can send through noisy channel $N = (P(b_i|a_j))$ and noise free channel M, respectively. Alice sends inputs (a_i, c_j) through $N \times M$ to Bob, who receives $(N(a_i), c_j)$. The least packing number is the smallest size of alphabet C such that Bob can always identify a_i from $(N(a_i), c_j)$. One can determine this value by taking the chromatic number, $\chi(G_N)$, of the associated confusability graph G.

Aside from the connections to information theory, the parameters $\alpha(G)$ and $\chi(G)$ are also interesting from the point of view of complexity theory. The complexity class NP consists of the class of problems whose solutions can be verified by a polynomial-time deterministic verifier. A problem is called NP-hard if it is as difficult to solve as any NP problem. The study of NP-hard problems was initiated by Cook [Coo71], Levin [Lev73] and Karp [Kar72]. Calculating the graph parameters $\alpha(G)$, and $\chi(G)$ are both known to be NP-hard. Consequently, the same can be said about calculating the zero-error capacity or least packing number of a noisy channel. There is no known method to efficiently calculate either of these parameters. In [Lov79] Lovász introduces a semi-definite programming relaxation, which we call $\theta(G)$, which can be used to provide bounds on these parameters. The relationship is summarized below in what is sometimes referred to as the Lovász sandwich theorem, $\alpha(G) \leq \theta(G) \leq \chi(\overline{G})$. Here $\overline{G}$ denotes the graph complement of G, which is obtained from G by having an edge between disconnected points in G and removing any edge between connected points in G.

1.2.2 Quantum channels and quantum graphs

Informally, a *quantum channel* is a linear map between two matrix algebras that both preserves the trace of a matrix and preserves positivity of a matrix, in a strong sense. More precisely, in Chapter 4 we view quantum channels as completely positive, trace preserving maps. Early work on quantum graph theory has had several motives. In [SB07] Shor and Beigi introduce a notion of zero error capacity for a *quantum channel* and show that computing this capacity is QMA-hard. QMA is the class of problems for which there exists a short "quantum proof" or a quantum state, that can be verified with high probability by a "quantum verifier". It is considered to be the analogue of the complexity class NP for quantum computers. This result can be viewed as a quantum version of the fact that it is $NP-$hard to compute the zero error capacity of a noisy channel.

In [DSW13] authors Duan, Severini and Winter further expand on the topic of error capacity for a *quantum channel*. Instead of having motives focused on complexity theory they generalize the notion of a confusability graph to the setting of quantum channels. In particular they show that to each *quantum channel* $\mathcal{N} : M_n \to M_d$ one can associate to it a special type of linear subspace or *operator system*, $\mathcal{S}_{\mathcal{N}} \subseteq M_n$. The relationship between a quantum channel, $\mathcal{N}$, and the operator system , $\mathcal{S}_{\mathcal{N}}$, is analogous to the relationship between a noisy channel and the associated confusability graph. It is for this reason that operator systems are sometimes referred to as *quantum graphs*. Furthermore, Duan, Severini, and Winter define the notion of an independence number, $\alpha(\mathcal{S})$, and parameter, $\theta(S)$, for an operator system. They are able show that the zero error capacity of a *quantum channel*, $\mathcal{N}$, is equal to the independence number, $\alpha(\mathcal{S}_{\mathcal{N}})$, of it's associated quantum graph. They also show that these parameters generalize the first part of the Lovász sandwich theorem as they satisfy the inequality $\alpha(S) \leq \theta(S)$.

In addition to the two motivations above quantum graphs also prove to be of great mathematical interest. It possible to view any noisy channel N as a special case of a quantum channel and it is also possible to view any graph G as a special case of a quantum graph $\mathcal{S}_G$. For the latter construction refer to Definition 4.2.1 in Chapter 4. The work of Paulsen and Ortiz tell us that the inclusion of graphs as quantum graphs via $G \mapsto \mathcal{S}_G$ preserves all the graph theoretic information [OP15]. It is due to these observations that the study of quantum graphs should properly be thought of as a mathematical generalization of graph theory instead of simply an analog for it. Graph theory is an enormous topic and is central to the study of combinatorics. In light of the work of Paulsen and Ortiz one can generate questions of mathematical inquiry by exploring which graph theory results extend to the more general setting of quantum graphs.

There are several different motivations for the study of quantum graphs, including mathematical motivations as well as motivations from complexity theory and physics. As the different motives for studying quantum channels are pursued it would be naive to assume that results which successfully generalize ideas from one area will always be of significance for all. Indeed, it is surprising that in the case of the independence number of a quantum graph, all three of these goals are aligned. From a mathematical stand point we have $\alpha(G) = \alpha(S_G)$ for all graphs G. Additionally $\alpha(S)$ both extends the notion of NP-hard to QMA-hard and extends the notion of zero error capacity of a noisy channel to the zero error capacity of a quantum channel. It is not inconceivable that one could define a parameter β such that $\alpha(G) = \beta(\mathcal{S}_G)$ for all graphs but it is neither QMA-hard to compute or able determine the zero error capacity of a quantum channel.

1.2.3 A Quantum Lovász inequality

One of the primary goals of the work in Chapter 4 was to investigate in what sense one can properly generalize the inequality, $\theta(G) \leq \chi(\overline{G})$, which is the second half of the Lovász sandwich theorem.

In order to investigate this we were motivated to generalize the notion of graph complement $G \mapsto \overline{G}$ in the setting of quantum graphs. The natural map to try is to send a quantum graph $S \subseteq M_n$ to it's orthogonal complement $S^\perp$ under the Hilbert-Schmidt inner product on M_n. Since every operator system will always contain the identity matrix the map $S \mapsto S^\perp$ seemingly fails to send a quantum graph to a quantum graph. Our approach was to also consider a notion of quantum graph first introduced by Stahlke [Sta16] that is similar but distinct to quantum graphs as conceived in [DSW13]. We refer to the two notions as *submatricial traceless self-adjoint operator space* and *submatricial operator system* respectively. In Theorem 4.2.7 we establish that the relationship between the two notions is precisely that of orthogonal complementation under the Hilbert-Schmidt inner product and we use this fact to extend the notion of graph complements to quantum graphs. The second ingredient needed to generalize the inequality $\theta(G) \leq \chi(\overline{G})$ is a notion of chromatic number of a quantum graphs.

In [HPP16] the notion of the least packing number of a quantum channel is described. Furthermore, they define a quantum graph parameter $\chi(S)$ that both satisfies $\chi(G) = \chi(S_G)$ and can calculate the least packing number of a quantum channel. Due to these desirable properties this may be a suitable choice for the chromatic number of a quantum graph. Unfortunately, when it comes to the goal of generalizing the Lovász sandwich theorem this parameter falls short. Indeed in Example 3 we provide an operator system S such that $\theta(S) = n > \chi(S^\perp) = 1$. This tells us that, in this case, one can not hope to satisfy all of the competing motives for quantum graphs. In particular, if one wants to keep a connection to information theory via the least packing number, then one can not hope to also generalize the Lovász inequality.

In Definition 4.3.1 we introduce a new parameter which we call the the *strong chromatic number*. In Theorem 4.3.7 we show that this parameter can be used to successfully generalize the second half of the Lovász sandwich theorem. Of-course, as discussed in the previous paragraph we cannot have our cake and eat it too. The strong chromatic number fails to have any straight forward connection to computing the least packing number of a quantum channel or any other property relevant to information theory. It is for this reason that the work in Chapter 4 focuses entirely on quantum graphs as mathematical generalizations of graphs and does not mention noisy channels or quantum channels.

An alternative approach to generalizing Lovász sandwich theorem was first established by Stahlke in [Sta16]. Stahlke makes connections to quantum channels much more the focus of his work and defines a chromatic number for quantum graphs which we denote χ_{St}. We provide an upper and lower bound for χ_{St}.

1.2.4 Sabidussi Theorem and Hedetniemi's Conjecture

Graph theory is an area of mathematics where simple to state problems can often prove to be quite intractable. This is perhaps best illustrated by the famous Four Color Theorem, which took over 100 years from its conjecture to its eventual resolution by Appel and Haken [AH89]. Many other outstanding questions involving the colourings of graphs remain open, including the Erdős–Faber–Lovász conjecture and Hadwiger's conjecture. If a full resolution to a problem remains intractable incremental progress can be made by either attempting to prove the result in a more narrow setting or refuting a version of the conjecture in a more general setting. Quantum graphs can provide a more general setting for which one can test conjectures against. We were initially motivated to provide a more general setting for the refutation of the longstanding Hedetniemi's conjecture. At the time of our earliest pre-print this conjecture remained unsolved [KM17]. Surprisingly, this question has since been resolved in the negative by the remarkable work of Shitov [Shi19].

In order to help introduce Hedetniemi's conjecture we consider the following outlandish sci-fi scenario:

> A deadly disease is spreading world-wide and all physical access to the local math department has been halted. Virtual classrooms, where graduate students can congregate, are to be created. To foster harmonious social interaction graduate students will be grouped together provided that either they have complementary math specialties, or they pursue complementary hobbies.

In such a far-fetched scenario what is the least number of virtual classrooms that would be needed? In order to answer this question one could generate two graphs. The first graph would consist of the math specialties of all students, and would have an edge between two specialties if they are not complimentary, such as axiomatic set theory and applied fluid dynamics. The second graph would consist of graduate student hobbies and would link two hobbies provided they are not complimentary, such as crocheting and gunsmithing. If we let k be the lesser of the chromatic numbers of the two graphs then k virtual rooms will be sufficient. Hedetniemi's conjecture purports that k will always be the least number of rooms needed. More formally, if we let $G \times H$ denote the categorical product of two graphs, then the following equality always holds,

$$\chi(G \times H) = \min\{\chi(G), \chi(H)\}.$$

One direction of this inequality is fairly trivial and the conjecture speculated as to the other. This seemingly innocuous statement remained unsolved for half a century. In order to formulate a version of Hedetniemi's conjecture for quantum graphs we generalize the categorical product of two graphs to the setting of quantum graphs. Given two graphs G and H one can construct a third graph known as the *categorical product*, $G \times H$, of G and H as follows. The nodes of $G \times H$ will consist of all order pairs (v, a) where v is a node from G and a is a node from H. We say there is an edge between nodes (v, a) and (w, b) whenever there is an edge between v and w in G and an edge between a and b in H. For any graphs G and H a coloring of either graph can be used to construct a coloring for the categorical product $G \times H$. Consequently one has the following inequality $\chi(G \times H) \leq \min\{\chi(G), \chi(H)\}$. The question as to whether or not the above is actually an equality for all graphs G and H was the long standing conjecture due to Hedetniemi [Hed66]. We call the above inequality, Hedetniemi's inequality, and in Section 4.4 we obtain a generalization for this in the context of quantum graphs. We note that the reverse inequality has been shown to not hold for all graphs [Shi19].

A similar identity exists for the Cartesian product and is due to Sabidussi [Sab57]. The Cartesian product of two graphs G and H, written $G\square H$, is given as follows. The nodes of $G\square H$ will consist of all order pairs (v, a) and there will be an edge between (v, a) and (w, b) if either there is an edge between v and w and $a = b$ or $v = w$ and there is an edge between a and b. Sabidussi's theorem states that for any two graphs G and H we have $\chi(G\square H) = \max\{\chi(G), \chi(H)\}$. In Section 4.4 we generalize this identity to the setting of quantum graphs. We achieve this generalization for both the strong chromatic number and an additional parameter we introduce referred to as the *minimal chromatic number*.

1.2.5 Future directions

Exhibiting an example of a QMA-hard problem was one of the earliest motivations for thinking of quantum graphs. One opportunity for further investigation is to determine if any of the above mentioned chromatic number graph parameters for quantum graphs are also QMA-hard to compute. This would be analogous to the fact that both the independence number and chromatic number of a graph are NP-hard to compute. Although we do not investigate this, in Theorem 4.2.15 and Theorem 4.3.5 we show how to compute various parameters for quantum graphs in terms of computing their classical analog across families of graphs.

Several other works have been completed that focus on extending notions from graph theory to the setting of quantum graphs. In [Wea17] Weaver examines extremal graph theory in the setting of quantum graphs and successfully obtains a generalization of a well known theorem due to Ramsey. A version of Ramsey's theorem is obtained for quantum graphs as infinite dimensional operator systems in the work of Kennedy et al [KKS17]. The study of graphs that have infinite nodes has been a part of graph theory since it's inception featured by König's in his 1936 book Theorie der endlichen und unendlichen Graphen (The Theory of finite and infinite graphs). For an updated version featuring commentary by Tutte please see [Kö12]. The study of operator systems in infinite dimensions have provided a rich landscape of theory and structure. The work of Kennedy et al. shows that there is much potential in connecting ideas from infinite graph theory to operator systems on infinite dimensional spaces.

Another setting where ideas from graph theory heavily intersect with work in quantum information theory is in the study of non-local games. In [CNM$^+$07] the notion of a quantum chromatic number is introduced. Here two isolated players try to convince a verifier that a given graph is $k-$colourable. If the players have access to entanglement then it is possible to win this game even if the given graph is not $k-$colourable. The study of non-local games based on graphs has grown considerably and the literature also features games based on the independence number, graph homomorphism and graph isomorphism. For some select highlighted works see [PT15], [RM16], [SSTW16]. In [SBG20] a non-local game is introduced that is based in part on homomorphisms between quantum graphs. This work provides motive for further exploration of non-local games.

Contents

Chapter 2

Operator Theory Formalism of Quantum Mechanics

The early development of quantum mechanics is not attributable to any single scientist as it is the culmination of many notable contributing physicists including Max Planck, Albert Einstein, Niels Bohr, Erwin Schrödinger and Werner Heisenberg. Similarly, the mathematical formalism that was eventually able to provide a unifying framework for quantum mechanics is due to several notable contributors including David Hilbert, John von Nuemann, Francis Joseph Murray and Paul Dirac. Most introductory courses in quantum information theory take for granted this operator theory formalism without providing much insight on it's origins.

In this section we develop this formalism starting from a collection of axioms detailing the probabilistic nature of quantum states and their accompanying observables. Discussions of physical intuition or experimental motivation is not a primary motivation here. Instead, we aim to present this content in a style that resembles a graduate course in abstract mathematics. That is, as often as possible, we explicitly state definitions and clearly state important conclusions as theorem statements or exercises. The content presented here was initially completed during a graduate reading course on *The Mathematical Foundations of Quantum Mechanics* by George W. Mackey and is largely based on Chapter 2-2 [Mac04].

2.1 The Axioms of a Quantum System

We view a quantum system $S = (\mathcal{O}, \mathcal{S})$ as an ordered pair comprised of states $\mathcal{S}$ and the set of observables $\mathcal{O}$. To each pair consisting of an observable $A \in \mathcal{O}$ and state $\alpha \in \mathcal{S}$, there exists a Borel probability measure, α_A on the real line $\mathbb{R}$. Informally, this means each observation we can make about a state is fundamentally random. Furthermore, the associated probabilities of our observations are determined by both what we are trying to observe and what state we are observing. The description above is far too general as it says little more then observations of states are random. If we instead require this family of probability measures to satisfy a handful of somewhat natural axioms then a rich mathematical structure emerges. We present the defining axioms of a quantum system in Definition 2.1.1.

Before we proceed to the definition we need to recall some notation regarding probability measures. Given a probability measure p and Borel function $f : \mathbb{R} \to \mathbb{R}$ we can define the push-forward measure, denoted $f(p)$, by $f(p)(E) = p(f^{-1}(E))$. It is clear that $f(p)$ will also be a probability measure. Also if p_i is a sequence of probability measures and t_i are non-negative numbers such that $\sum_i t_i = 1$ then we can define a new probability measure $p = \sum_i t_i p_i$ by $p(E) =$

$\sum_i t_i p_i(E)$ for all $E \subseteq \mathbb{R}$. For any Borel set E we can define the indicator, or characteristic function χ_E, which evaluates to 1 on the set E and 0 elsewhere.

Definition 2.1.1. A *quantum system* S is an ordered pair, $S = (\mathcal{O}, \mathcal{S})$, consisting of a set of observables $\mathcal{O}$, and states $\mathcal{S}$, such that for each pair $\alpha \in \mathcal{S}$ and $A \in \mathcal{O}$, there exists a Borel probability measure α_A on $\mathbb{R}$, and this family of measures satisfies the following axioms:

1. If $\alpha_A = \alpha_{A'}$ for all $\alpha \in \mathcal{S}$ then $A = A'$. If $\alpha_A = \alpha'_A$ for all $A \in \mathcal{O}$ then $\alpha = \alpha'$.
2. For each $A \in \mathcal{O}$ and for each Borel function f, there exists a unique observable $f(A) \in \mathcal{O}$ such that $\alpha_{f(A)} = f(\alpha_A)$ for all states $\alpha \in \mathcal{S}$.
3. If $\{\alpha_i\}_{i \in \mathbb{N}}$ is a sequence of states and $\{t_i\}_{i \in \mathbb{N}}$ is a sequence of non-negative real numbers such that $\sum_i t_i = 1$, then there exists a unique state $\alpha \in \mathcal{S}$ such that for all $A \in \mathcal{O}$ we have
$$\alpha_A = \sum_i t_i (\alpha_i)_A.$$

In order to state the last two axioms for Definition 2.1.1 we introduce some notation regarding a particularly important set of observables called *questions*. An observable $Q \in \mathcal{O}$ is called a *question* if $\alpha_Q(\{0,1\}) = 1$. We let $\mathcal{Q} \subseteq \mathcal{O}$ denote the set of all questions and write $Q_1 \leq Q_2$ if $\alpha_{Q_1}(\{1\}) \leq \alpha_{Q_2}(\{1\})$ for all $\alpha \in \mathcal{S}$. We also say questions Q_1 and Q_2 are *disjoint* if $\alpha_{Q_1}(\{1\}) + \alpha_{Q_2}(\{1\}) \leq 1$ for all $\alpha \in \mathcal{S}$. Additionally, a map q from Borel sets $\mathbb{B}$ to $\mathcal{Q}$ is called a *question valued measure* if:

a) $E \bigcap F = \emptyset \implies q(E)$ and $q(F)$ are disjoint questions.

b) $\{E_i\}_i$ are pairwise disjoint then $q(\bigcup_i E_i) = \sum_i q(E_i)$

c) $\alpha_{q(\emptyset)} = \delta_0$ and $\alpha_{q(\mathbb{R})} = \delta_1$ for all $\alpha \in \mathcal{S}$.

Keeping the notation outlined above we now return to our axioms.

4. Let $\{Q_i\}_{i \in \mathbb{N}}$ be a sequence of pairwise disjoint questions. Then there exists a question $Q = \sum_i Q_i$ such that for all $\alpha \in \mathcal{S}$
$$\alpha_Q(\{1\}) = \sum_i \alpha_{Q_i}(\{1\}).$$
5. If q is a question valued measure then there exists an observable $A \in \mathcal{O}$ such that $q(E) = \chi_E(A)$ for all $E \in \mathbb{B}$.

The first axiom simply tells us that states and observables are exactly determined by the probability measures they can generate. Informally, the second axiom says that the set of observations we can make is closed under the application of any reasonable function and the third axiom tells us that the set of states is closed under infinite convex combinations. Non-trivial convex combinations of states are viewed as mixtures of states with state α_i occurring with probability t_i.

In the above definition of a quantum system we also smuggled in some important concepts. In particular we defined the set of observables $\mathcal{Q} \subseteq \mathcal{O}$ which we call questions. Questions can be thought of as observables that receive a "yes" or "no" response when an observation is made of any particular state. We equipped this set with a partial order where one question is greater than another if the probability of a "yes" response is greater for every state.

We also can equip the set of questions with a *orthocomplement* by letting the *complement* of a question Q to be the question $1 - Q$. Where $1 - Q$ is satisfies $\alpha_{1-Q}(\{1\}) = 1 - \alpha_Q(\{1\}$ for all states α. By Axiom 1 this is enough to uniquely define the the question $1 - Q$. More simply, the complement of a question Q is a question $1 - Q$ that receives a "yes" response with the same probability that question Q receives a "no" response. Partial motivation for the the notion of disjoint questions is given in Exercise 2.1.3 below. It should be noted that this definition of disjoint questions allows for the possibility of a question to be disjoint from itself. Indeed, as long as $\alpha_Q(\{1\} \leq \frac{1}{2}$ this will be the case.

The set of questions together with their partial order and orthocomplement will play a central role in the rest of our discussion. In fact, we will eventually see that they are sufficient to recover the entire quantum system $S = (\mathcal{O}, \mathcal{S})$. Below are a collection of exercises that provide some insight into the structure of questions and provide some mathematical motivation for the partial ordering and the orthocomplement.

Exercise 2.1.1. *An observable $A \in \mathcal{O}$ is a question if and only if $A = A^2$. (Here we use the notation A^2 to denote the image of A under the Borel function $x \mapsto x^2$.)*

Exercise 2.1.2. *For each Borel set $E \in \mathbb{B}$ and observable $A \in \mathcal{O}$ there exists a unique question $\chi_E(A) \in \mathcal{Q}$ that satisfies*

$$\alpha_{\chi_E(A)}(\{1\}) = \alpha_A(E)$$
$$\alpha_{\chi_E(A)}(\{0\}) = \alpha_A(\mathbb{R} \backslash E)$$

for all states $\alpha \in \mathcal{S}$.

The question $\chi_E(A)$ can be understood as the question that receives a "yes" response with the same probability that A makes an observation in the set E.

Exercise 2.1.3. *Let $E, F \in \mathbb{B}$ be Borel sets. Then for any observables $A \in \mathcal{O}$ the following are true:*

- *If $E \bigcap F = \emptyset$ then $\chi_E(A)$ and $\chi_F(A)$ are disjoint questions.*
- *If $E \subseteq F$ then $\chi_E(A) \leq \chi_F(A)$.*
- *$\chi_E(A)$ is the orthocomplement of $\chi_{\overline{E}}(A)$.*

Mackey also provides a way to view the question Q in Axiom 4 as the least upper-bound of $\{Q_i\}$, which the following theorem outlines.

Theorem 2.1.2. *If $\{Q_i\}_i$ is a sequence of pairwise disjoint questions and $R \geq Q_i$ for all $i \in \mathbb{N}$, then $R \geq \sum_i Q_i$.*

Proof. The proof for this result is given in [Mac04]. Alternatively, it may be considered as a exercise, although it is quite challenging. □

Thus far it may seem that in a quantum system $S = (\mathcal{O}, \mathcal{S})$, the sets of observables $\mathcal{O}$ and states $\mathcal{S}$ are not very intuitive. We conclude this section by discussing a correspondence to these sets that makes working with them more natural. First, we note that there is a one-to-one correspondence between the set of observables $\mathcal{O}$ and the set of question valued measures $q : \mathbb{B} \to \mathcal{Q}$.

Theorem 2.1.3 (Observables correspond to question valued measures)**.** *For each question valued measure q the observable A defined from Axiom 5 is unique. Moreover, without loss of generality one can assume there is a one-to-one correspondence between the set of observables $\mathcal{O}$ and the set of question valued measures.*

Proof. the first part of this proof is suitable for an exercise. For the second please consult Makey's discussion. □

In order for us to determine a useful correspondence for the set of states $\mathcal{S}$, we need to define an *abstract state* on the set of questions.

Definition 2.1.4. We say a map $m : \mathcal{Q} \to [0,1]$ is called an *abstract state* on the set of questions if it satisfies the following criteria:

a) If $\{Q_i\}$ are pairwise disjoint then $m(\sum_i Q_i) = \sum_i m(Q_i)$.

b) We will simply use 0 to denote the question satisfying $\alpha_0 = \delta_0$ for all $\alpha \in \mathcal{S}$. Similarly, we let 1 denote the question satisfying $\alpha_1 = \delta_1$ for all $\alpha \in \mathcal{S}$. Then we require the map m to satisfy $m(0) = 0$ and $m(1) = 1$.

We note that Mackey refers to these maps as "probability measures on the set of questions".

Next are a series of exercises that show given any state $\alpha \in \mathcal{S}$, we can obtain an abstract state on the set of questions. We also see that this set is strongly convex in the sense that is is closed under countable convex combinations.

Exercise 2.1.4 (States give rise to abstract states). *If α is a state, show that the map $m_\alpha : \mathcal{Q} \to [0,1]$ defined by $m_\alpha(Q) = \alpha_Q(\{1\})$ is an abstract state on the set of questions. Moreover, show that if $m_\alpha = m'_\alpha$ then $\alpha = \alpha'$.*

Exercise 2.1.5. *Let $\{\alpha_i\}_{i\in\mathbb{N}}$ be a sequence of states and $\{t_i\}_{i\in\mathbb{N}}$ a sequence of non-negative real numbers such that $\sum_i t_i = 1$. Show that $m = \sum_i t_i m_{\alpha_i}$ defines an abstract state and that $m_{\sum_i \alpha_i} = m$.*

We will eventually see that the set of abstract states and the set of states are in one-to-one correspondence. One of the directions of this correspondence was outlined in Exercise 2.1.4. We do not make the other direction automatic by the addition of an axiom as was the case for obervables via axiom 5. For the moment, we remark that if there was a one-to-one correspondence, then the set of abstract states on the set of questions would have to satisfy the two following properties:

1. If $\{m_i\}_i$ is a sequence of abstract states and $\{t_i\}_i$ are non-negative numbers that sum to 1, then there exists an abstract state m such that $m = \sum_i t_i m_i$.

2. If $m(Q_1) \leq m(Q_2)$ for all abstract states m then $Q_1 \leq Q_2$.

A collection of abstract states on the set of questions that satisfy Property 1 is called *strongly convex* and we say that the set is *full* if it satisfies Property 2.

We will return to the discussion of abstract states on the set of questions later. Our next immediate goal is to show that a quantum system can be completely determined by the partially ordered set of questions $\mathcal{Q}$. To do this, we need to introduce the notion of a *quantum logic*.

2.2 Quantum Logic

We will eventually show that one can determine the entire quantum system $S = (\mathcal{O}, \mathcal{S})$ from the set of questions $\mathcal{Q}$. In order to do this, we introduce the idea of a quantum logic, which is a partially ordered set together with special involution called an orthocomplement. We show that given any quantum logic, one can determine a set of observables $\mathcal{O}$ and states $\mathcal{S}$ that satisfy the axioms from Definition 2.1.1. Conversely, given any quantum system $S = (\mathcal{O}, \mathcal{S})$ one can determine a quantum logic by looking at the set of questions $\mathcal{Q} \subseteq \mathcal{O}$.

Definition 2.2.1. A *quantum logic* is a partially ordered set $\mathcal{L}$ equipped with an an involution $a \mapsto a'$ such that:

1. If $a_1 \leq a_2$ then $a_2' \leq a_1'$
2. If $\{a_i\}_i$ is a sequence of elements of $\mathcal{L}$ such that $a_i \leq a_j'$ for $i \neq j$, then there exists a unique least upper bound for this sequence, denoted $\bigcup_i a_i$.
3. $a \cup a' = b \cup b'$ for all $a, b \in \mathcal{L}$. We call this element 1.
4. If $a \leq b$ then $b = a \cup (b' \cup a)'$ for all $a, b \in \mathcal{L}$.

Different definitions for a quantum logic than the one above appear in mathematical literature.

The partial order and involution of a quantum logic should remind us of the set of questions in a quantum system. We say that elements a_1 and a_2 are disjoint if $a_1 \leq a_2'$ and we refer to the involution with the above properties as an orthocomplement on $\mathcal{L}$. As we did for the set of questions in a quantum system, we can define the notions of an *abstract state* and aa $\mathcal{L}-$valued measure for a quantum logic.

Definition 2.2.2. A function $m : \mathcal{L} \to [0, 1]$ is an abstract state on $\mathcal{L}$ if

a) $m(1) = 1$ and $m(1') = 0$.

b) $m(\bigcup_i a_i) = \sum_i m(a_i)$ for any sequence of disjoint elements $\{a_i\}$.

A family $\mathcal{F}$ of abstract states on $\mathcal{L}$ is called *full* if $m(a_1) \leq m(a_2)$ for all $m \in \mathcal{F}$ implies that $a_1 \leq a_2$. A family $\mathcal{F}$ is called *strongly convex* if it is closed under infinite convex combinations.

Definition 2.2.3. An *$\mathcal{L}$-valued measure* is a function $q : \mathbb{B} \to \mathcal{L}$ that satisfies

a) $E \cap F = \emptyset \implies q(E)$ and $q(F)$ are disjoint elements of $\mathcal{L}$.

b) If $\{E_i\}_i$ are pairwise disjoint then $q(\bigcup_i E_i) = \bigcup_i q(E_i)$.

c) $q(\emptyset) = 1'$ and $q(\mathbb{R}) = 1$.

In order to see how a quantum logic can give rise to a quantum system, we need a natural way of constructing probability measures. Given an $\mathcal{L}$-valued measure q and an abstract state $m : \mathcal{L} \to [0, 1]$, we define a Borel probability measure p by $p(E) = m(q(E))$. We are now ready to state the main theorem of this section.

Theorem 2.2.4. *If $S = (\mathcal{O}, \mathcal{S})$ is a quantum system then the partially ordered set of questions equipped with the involution $Q \mapsto 1 - Q$ is a quantum logic. Conversely, if $\mathcal{L}$ is a quantum logic, we can obtain a quantum system by taking the observables $\mathcal{O}$ to be the set of $\mathcal{L}$-valued measures and take the set of states $\mathcal{S}$ to be any full and strongly convex set of abstract states.*

Proof. Suppose $S = (\mathcal{O}, \mathcal{S})$ is a quantum system. We show the involution $Q \mapsto 1 - Q$ satisfies the four properties in Definition 2.2.1. If $Q_1 \leq Q_2$ then, by definition, for all states α we have $\alpha_{Q_1}(\{1\}) \leq \alpha_{Q_2}(\{1\})$. So for any state α we have $\alpha_{1-Q_1}(\{1\}) \geq \alpha_{1-Q_2}(\{1\})$, thus $1 - Q_1 \geq 1 - Q_2$. The second property follows from the Axiom 4 together with Theorem 2.1.2. Here, the sum of disjoint questions takes the role of the least upper bound. Properties 3 and 4 can be shown to hold as well.

The converse is left as an exercise to the reader. □

When viewing a quantum system as a quantum logic, we see that observables are determined by the set of $\mathcal{L}$-valued measures and states are determined by a full and strongly convex family of abstract states. We eventually want to see how we can view the set of observables as self-adjoint operators on a separable Hilbert space and states as density operators. Before moving to this discussion, we take a small detour to talk about the differences between classical and quantum systems.

2.3 Classical vs. Quantum Systems

One crucial part of obtaining a good mathematical foundation for quantum systems is being able to differentiate them from classical systems. In classical systems, there is a one-to-one correspondence between questions and Borel subsets of a symplectic manifold. In order to understand how this view fails in the generality of quantum systems, we introduce the idea of *simultaneously answerable* questions.

Definition 2.3.1. Let Q_1 and Q_2 be questions. We say Q_1 and Q_2 are *simultaneously answerable* (or *compatible*) if there exists mutually disjoint questions Q_3, R_1, R_2 such that $Q_1 = R_1 + Q_3$ and $Q_2 = R_1 + Q_3$. We also say two observables A and B are *compatible* if for all Borel sets E, F the questions $\chi_E(A)$ and $\chi_F(B)$ are compatible.

The idea of compatible questions is both intuitive and natural. Informally, when two questions are compatible then it makes sense to ask about the probabilities that both events occur and the probability that one but not the other event occurs. See Figure 2.1 to help motivate the definition of compatible questions. It is the departure from this intuitive picture that is the main divergence between classical and quantum systems.

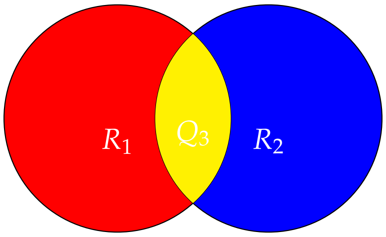

Figure 2.1: Two compatible questions Q_1 and Q_2.

Exercise 2.3.1 (Classical Comparison)**.** *If Q_1 and Q_2 are any classical questions (i.e Borel subsets of a symplectic manifold) then they are simultaneously answerable.*

Exercise 2.3.2. *Questions Q_1 and Q_2 are simultaneously answerable if and only if there is an observable A and Borel sets E_1 and E_2 such that $Q_1 = \chi_{E_1}(A)$ and $Q_2 = \chi_{E_2}(A)$.*

The axioms we have presented thus far do not imply that that every two questions are simultaneously answerable. In the situation that any two questions are compatible then the set of questions can be shown to form a Boolean algebra.

Definition 2.3.2. A partially ordered set, equipped with the usual union and intersection operations aswell as with a orthocomplement is called a *Boolean algebra* if it is a lattice (i.e any two elements have a least upper-bound and greatest lower-bound) and satisfies the distributive law (i.e $Q_1 \cap (Q_2 \cup Q_3) = Q_1 \cap Q_2 \cup Q_1 \cap Q_3$).

Exercise 2.3.3. *If any two questions are simultaneously answerable then the set of questions $\mathcal{Q}$ is a Boolean algebra. Conversely, if the set of questions is a Boolean algebra with the canonical ordering and orthocomplement then any two questions are compatible.*

The conclusion allows us to highlight the difference between classical systems, which correspond to Boolean algebras, and more general quantum systems, which correspond to what we defined as a quantum logic in subsection 2.2. We next will see how quantum systems can be realised by looking at Hilbert spaces.

2.4 Hilbert Spaces

In this subsection, we outline the connection between the definition of a quantum system as given in Definition 2.1.1 and the more common setting of a quantum system on a separable Hilbert space. The way this connection is made is to recognize that one can obtain a quantum logic from looking at the collection of closed subspaces of a Hilbert space $\mathcal{H}$. This collection is equipped with a partial order given by containment. We can also use the orthogonal complement given by the Hilbert space inner product to define an orthocomplement in the sense of Definition 2.2.1. We leave the simple details to the reader.

Theorem 2.4.1. *The partially ordered set of all closed subspaces of a separable Hilbert space $\mathcal{H}$ is a quantum logic and thus a realisation of a quantum system $S = (\mathcal{S}, \mathcal{O})$.*

Proof. Exercise. □

Mackey treats this discussion differently. First, he includes a lengthy discussion about possibly weakening the definition of Boolean algebras which we completely omit. Second, he notes that the realisation of a quantum system in terms of the partially ordered closed subspaces of a Hilbert spaces is one of many possible choices and includes this particular choice as an additional axiom. Please refer back to Mackey to see his comments on this choice. Due to the following theorem by Kakutani, we do not need to consider the more general setting of Banach spaces.

Theorem 2.4.2 (Kakutani)**.** *If the lattice of closed subspaces of a Banach space X is equipped with an orthocomplement then the norm is equivalent to a Hilbert space norm and the orthocomplement is the standard one on a Hilbert space.*

A valid alternative to the Hilbert space approach is to consider the lattice of projections in a factor von-Neumann algebra; we do not consider this possibility here. Instead, we restrict ourselves to those quantum systems $S = (\mathcal{S}, \mathcal{O})$ that can be determined by the set of closed subspaces of some separable Hilbert space $\mathcal{H}$. Using the one-to-one correspondence between closed subspaces and orthogonal projections $P \in B(\mathcal{H})$, we can view the set of questions $\mathcal{Q} \subseteq \mathcal{O}$ as being the set of projection operators on the Hilbert space $\mathcal{H}$. Of course, since $B(\mathcal{H})$ is a factor von-Neumann algebra, this can be viewed as a special case of the von-Neumann algebra approach.

Many familiar properties and definitions pertaining to operators on a Hilbert space can be extended to a quantum system in a meaningful way. Before we move towards our final goal of characterizing observables and states as particular operators, we look at some of these definitions. For the next few definitions, we fix a quantum system $S = (\mathcal{S}, \mathcal{O})$ in the sense of Definition 2.1.1.

Definition 2.4.3. Let $A \in \mathcal{O}$ be an observable and $E \subseteq \mathbb{B}$ be a Borel set. We say E is of *measure zero* with respect to A if for all states $\alpha \in \mathcal{S}$ we have $\alpha_A(E) = 0$. We also let $\rho(A)$, called the *resolvent of* A, denote the union of all open intervals I that are of measure zero with respect to A and let $\sigma(A)$, called the *spectrum of* A, denote the complement of $\rho(A)$.

Exercise 2.4.1. *E is of measure zero with respect to A if and only if $\chi_E(A) = 0$.*

Definition 2.4.4. The set of points $x \in \mathcal{H}$ such that $\chi_{\{x\}}(A) \neq 0$ is called the *point spectrum of A*. If the spectrum of A is a bounded set then we say A is bounded. The *norm of A* is defined as $\|a\| = \sup_{\lambda \in \sigma(A)} |\lambda|$.

Definition 2.4.5. If A is bounded then for each $\alpha \in \mathcal{S}$, the measure α_A is concentrated in a finite interval and hence we can evaluate the integral

$$\int_{-\infty}^{\infty} x\alpha_A.$$

We denote this value $m_\alpha(A)$ and call this the *expected value*.

Exercise 2.4.2. *If the observable A is a question then A is bounded and m_α in the definition above agrees with definition from Exercise 2.1.4.*

Exercise 2.4.3. *Show the following are equivalent for projections P and Q:*

1. *P and Q are disjoint as elements of a quantum logic.*

2. *The range of P and Q are orthogonal subspaces.*

3. *$PQ = QP = 0$.*

Additionally, show that if P and Q are disjoint, then their least upper bound as elements in a quantum logic $P \cup Q$ is given by their sum as projections $P + Q$.

2.5 States and Observables as Operators

In Section 2.4, we established the view that any quantum system $S = (\mathcal{S}, \mathcal{O})$ can be determined by taking the set of questions to be a set of projections for some corresponding separable Hilbert space $\mathcal{H}$. In order to better understand this realisation of a quantum system, we explore both the set of observables $\mathcal{O}$ and the set of states $\mathcal{S}$.

We first begin with a discussion of observables. Recall from Theorem 2.2.4 that we can identify the set of observables with the set of question valued measures. Working with our assumption that the underlying set of questions corresponds to projections on some Hilbert space $\mathcal{H}$, we will show that you can identify the set of observables $\mathcal{O}$ with the set of valued measures. We take some time to recall operator valued measures from operator theory.

Definition 2.5.1. A map $Q : \mathbb{B} \to B(\mathcal{H})$ from the set of Borel sets $\mathbb{B}$ to the set of bounded operators on $\mathcal{H}$ is called an *operator valued measure* if for any $x, y \in \mathcal{H}$ and any countable disjoint collection $\{B_i\}$ of Borel sets we have

$$\left\langle Q\left(\bigcup B_i\right) x, y\right\rangle = \sum_i \langle Q(B_i)x, y\rangle.$$

Exercise 2.5.1. *If Q is an operator valued measure then for each pair $x, y \in \mathcal{H}$, the map $E \mapsto \langle Q(E)x, y\rangle$ is a complex valued Borel measure.*

When an operator valued measure has a range consisting of projection operators then it is called a *projection valued measure*. The next exercise helps us square this terminology with question valued measures introduced in Section 2.1.

Exercise 2.5.2. *Let $S = (\mathcal{O}, \mathcal{S})$ be a quantum system. Assume we can identify the set of questions $\mathcal{Q} \subseteq \mathcal{O}$ with the set of projections on a Hilbert space $\mathcal{H}$. Show that any question valued measure in the sense of Definition 2.1.1 is an operator valued measure in the sense of Definition 2.5.1. Conversely, show that if $Q : \mathbb{B} \to B(\mathcal{H})$ is an operator valued measure such that $Q(E)$ is a projection for all Borel sets E, then Q is a question valued measure.*

The above exercises tell us that we can view the set of observables as the set of projection valued measures. In order to go one step further, we need invoke a version of the spectral theorem stated below.

Theorem 2.5.2 (Spectral theorem for self-adjoint operators)**.** *Let $\mathcal{H}$ be a separable Hilbert space. There is a one-to-one correspondence between self-adjoint operators A on $\mathcal{H}$ and projection valued measures $Q : \mathbb{B} \to B(\mathcal{H})$.*

It should be noted that this correspondence is not restricted to bounded operators. That is, it is possible that some observables will give rise to unbounded self-adjoint operators. In order to better understand the correspondence between observables and the corresponding operator, a solid understanding of the Borel functional calculus is needed. Since these technicalities are beyond the scope of this Thesis, we refer the reader Chapters 7 and 8 of [Hal13]. A careful reading of these chapters should allow one to tackle the following exercise.

Exercise 2.5.3. *Let $Q : \mathbb{B} \to B(\mathcal{H})$ be a question valued measure (and hence a projection valued measure) and let A be the corresponding self-adjoint operator given by Theorem 2.5.2. Show that Q is bounded in the sense of Definition 2.4.3 if and only if A is a bounded operator. Show that the operator norm of A agrees with the norm of Q. Finally, show that the definitions of spectrum and resolvent agree, i.e show that $\sigma(Q) = \sigma(A)$ and $\rho(Q) = \rho(A)$.*

We conclude our discussion of observables as operators at this point and proceed to our view of states as density operators. In Theorem 2.2.4, we identify the set of states $\mathcal{S}$ with a full and strongly convex set of abstract states. Clearly, the set of all abstract states will be full and strongly convex. Below we discuss how we can always considered this to be the canonical choice. To begin, consider abstract states that are constructed from unit vectors of the underlying Hilbert space. See the exercise below for the details.

Exercise 2.5.4. *Let $\mathcal{H}$ be a separable Hilbert space and $\phi \in \mathcal{H}$ be a unit vector. Then the map $P \mapsto \langle P\phi, \phi \rangle$ defines an abstract state on the set of questions (i.e projections) in the sense of Definition 2.1.4.*

Given a unit vector $\phi \in \mathcal{H}$, we use m_ϕ to denote the corresponding abstract state, called a *pure state*, on the set of questions. Note the map $\phi \mapsto m_\phi$ defines a map from unit vectors in $\mathcal{H}$ to abstract states. This map will not be injective, in particular $m_\phi = m_\psi$ if $\phi = c\psi$ for $|c| = 1$. More generally, if we have a sequence of unit vectors $\{\phi_i\} \subset \mathcal{H}$, we can define an abstract state m on the set of questions by taking an infinite convex combination

$$m(P) = \sum_i t_i m_{\phi_i}(P).$$

It can be shown that the set of all abstract states on the set of questions is a convex set and the pure states are extreme points of this convex set. Moreover, any abstract state can be written as a (possibly infinite) convex combination of pure states. Using this fact, we can give a sufficient condition for the state space $\mathcal{S}$ in an quantum system to be taken to be the set of all abstract states.

Theorem 2.5.3. *Suppose for each non-zero question $Q \in \mathcal{Q}$, there exists a state $\alpha \in \mathcal{S}$ such that $m_\alpha(Q) = 1$. Then the set of states $\mathcal{S}$ is in one-to-one correspondence with the set of abstract states.*

Remark 2.5.4. Mackey proves this theorem after introducing an additional axiom. We instead included it in the hypothesis.

Recall in Definition 2.4.5 we introduced the expected value m_α corresponding to a state α. In the next exercise, we show how this expected value corresponds to the more common definition in quantum information theory courses. (Again, a good understanding of the Borel functional calculus and the spectral theorem is required for the following exercise.)

Exercise 2.5.5. *For any state $\alpha \in \mathcal{S}$ that corresponds to a pure state m_ϕ and for any observable A with corresponding self-adjoint operator A', we have*

$$m_\alpha(A) = \langle A'\phi, \phi \rangle = m_\phi(A').$$

Now that we have established when it is reasonable to identify the set of states $\mathcal{S}$ with the set of all abstract states, we proceed to identify states as density operators. In order to do this, we first recall the set of *trace-class* and *density* operators from operator theory.

Definition 2.5.5. Let $\mathcal{H}$ be a separable Hilbert space. An operator $A \in B(\mathcal{H})$ is called *trace-class* if for some (equivalently all) orthonormal basis $\{e_n\}$,

$$\sum_n \langle (A^*A)^{1/2} e_n, e_n \rangle < \infty.$$

If A is a trace-class operator we define the trace $Tr(A)$ by

$$Tr(A) = \sum_n \langle A e_n, e_n \rangle.$$

Definition 2.5.6. A trace-class operator A that is positive semi-definite with $Tr(A) = 1$ is called a *density operator*.

For the next three exercises, a decent background in basic functional analysis and operator theory is required. For example, any course that covers content similar to the first 4 Chapters of [Ped89] should suffice.

Exercise 2.5.6. *The set of trace-class operators is a two sided ideal in $B(\mathcal{H})$.*

Exercise 2.5.7. *If A is a trace-class operator such that $A \geq 0$ (i.e positive semi-definite and $Tr(A) = 1$) then we can define an abstract state on the set of projections by the map $p \mapsto Tr(AP)$.*

Thus every density operator corresponds to an abstract state; this correspondence is actually one-to-one. Indeed, if m_ϕ is a pure state, one can define the projection onto the one dimensional P_ϕ. Then P_ϕ is a density operator. Furthermore, for any projection P we have $Tr(P_\phi P) = \langle P\phi, \phi \rangle = m_\phi$. We can do the same for mixed states, i.e. for states that are not pure.

Exercise 2.5.8. *Let $m = \sum_i t_i \phi_i$ be a mixed abstract state on the set of projections. Then $A = \sum_i t_i P_{\phi_i}$ is a density operator with $Tr(A) = 1$. Furthermore, for all projections P we have the equality*

$$m(P) = Tr(AP).$$

These exercises combined with the correspondence established between self-adjoint operators and observables allows us to conclude the following theorem.

Theorem 2.5.7 (Observables and States as operators). *Let $S = (\mathcal{S}, \mathcal{O})$ be a quantum system whose set of questions $\mathcal{Q} \subseteq \mathcal{O}$ is taken to be the set of projections on a Hilbert space $\mathcal{H}$. Then the set of observables $\mathcal{O}$ is in one-to-one correspondence with the set of self-adjoint operators on $\mathcal{H}$ and, if we assume the hypothesis of Theorem 2.5.3, there is a one-to-one correspondence between the set of states $\mathcal{S}$ and the set of density operators.*

We include one final exercise that requires the reader to have a good understanding of the correspondence above.

Exercise 2.5.9. *Let $B \in \mathcal{O}$ be an observable with corresponding self-adjoint operator $B' \in B(\mathcal{H})$ and let $\alpha \in \mathcal{S}$ be a state with corresponding density operator A. If m_α is the expected value outlined in Definition 2.4.5 we have the equality*

$$m_\alpha(B) = Tr(AB').$$

2.6 Quantum Strategies for non-local games

We now return to the topic of non-local games. Recall, in this setting two players, Alice and Bob, collaborate to win a game played against a referee. The players are allowed to discuss and coordinate an agreed upon strategy before the start of the game. Once the game starts they are forbidden to communicate with one another and each given a single question and each provide a single response. The players win or lose this single round game based on the questions and answers provided. Crucially, since the players do not communicate once the game commences they are not aware of the question the player received.

Formally, a non-local game is described by a tuple $(V, I_A, I_B, O_A, O_B, \pi)$ consisting of finite input and outputs sets for Alice and Bob and a rule function $V : I_A \times I_B \times O_A \times O_B \to \{0, 1\}$ as well as a distribution π on $I_A \times I_B$. Alice and Bob are given inputs x and y respectively with probability $\pi(x, y)$ and produce respective outputs a and b. The players win when $V(x, y, a, b) = 1$. A strategy for this game consists of a conditional probability function, or correlation, $P = P(a, b|x, y)$, that determines the probability Alice and Bob respond with answers a and b when given questions x and y. In order to model the fact that the players are separated we restrict the players to use only so called *non-signalling* strategies. That is, we require the conditional probabilities for Alice and Bob $P_A(a|x), P_B(b|y)$ to be well defined. The following sets of correlations outlined below are all examples of non-signaling strategies.

Deterministic strategies are the natural way to model the strategies Alice and Bob can make if they are restricted by the physical rules of classical mechanics. In this scenario Alice and Bob plan to pick a predetermined output for each possible input they receive.

Definition 2.6.1 (Deterministic Strategies). A strategy, P, for a non-local game $(V, I_A, I_B, O_A, O_B, \pi)$ is called *deterministic* if there exist functions $f : I_A \to O_A$ and $g : I_B \to O_B$ such that

$$P(a, b|x, y) = \delta_a(f(x))\delta_b(g(y)).$$

Classical strategies are not restricted to only include deterministic strategies. More generally, Alice and Bob can employ randomness when determining their responses.

Definition 2.6.2 (Classical Strategies). A strategy, P, for a non-local game $(V, I_A, I_B, O_A, O_B, \pi)$ is called *classical* if there exists a probability space (Ω, μ) such that for each $x \in I_A$ and $y \in I_B$ there exist $f_x : \Omega \to O_A$ and $g_y : \Omega \to O_B$ with $P(a, b|x, y) = \mu(f_x^{-1}(a) \bigcap g_y^{-1}(b))$.

An alternative set of strategies can be determined if Alice and Bob are allowed to take advantage of the axioms described in Section 2.1. Here we imagine that Alice and Bob will prepare a pure state α and for each input $x \in I_A$, that Alice receives she has a set of questions, $\{P_x^a : a \in O_A\}$. Similarly, for each input $y \in I_B$, Bob has a set of questions $\{Q_y^b : b \in O_B\}$. Given input x Alice will return output a only if the answer to question P_x^a is yes. Likewise, Bob, will return output b exactly when the answer to question Q_y^b is yes.

We make two additional requirements on what are the possible questions Alice and Bob can use. Firstly, in order for Alice to always make a reply we require that for any state α Alice always receives a yes response to one of her questions. The same requirement is made for the questions Bob receives. In the language our axioms this corresponds to the requirement that for every x, y we have $\sum_a P_x^a = \sum_y Q_y^b = 1$. Secondly, the non-signalling condition requires that conditional probabilities, $P_A(a|x)$ and $P_B(b|y)$, are well-defined. This corresponds to the requirements that each pair of questions P_x^a and Q_y^b are simultaneously answerable, in the sense of Definition 2.3.1. Using the correspondence outlined in Theorem 2.5.7 we know that the questions of Alice and Bob can be identified with projections on some Hilbert space H and their shared pure state α can be identified with a unit vector. Furthermore, the non-locality condition can be shown to be equivalent to a requirement that Alice's projections commute with Bob's. We then obtain the following definition for commuting operator strategies.

Definition 2.6.3 (Commuting Operator Strategies). P is a commuting operator strategy for a non-local game $(V, I_A, I_B, O_A, O_B, \pi)$ if there exists a tuple $(H, \phi \in H, \{P_x^a\}, \{Q_y^b\})$, where H is a Hilbert space, $\phi \in H$ is a unit vector, and $\{P_x^a\}$ and $\{Q_y^b\}$ are families of projections that satisfy,

1. $\sum_a P_x^a = I$ for all $x \in I_A$
2. $\sum_b Q_y^b = I$ for all $y \in I_B$
3. $P_x^a Q_y^b = Q_y^b P_x^a$ for all x, y, a, b
4. $P(a, b|x, y) = \langle P_x^a Q_y^b \phi, \phi \rangle$.

One may consider the requirement that the questions of Alice and Bob are simultaneously answerable too strong. Indeed, since Alice and Bob only ask questions with respect to a predetermined state, α, it makes sense to consider strategies that Alice and Bob can employ when they can consider questions that are only simultaneously answerable with respect to this chosen state α. In the operator theory formalism this would correspond to a requirement $P_x^a Q_y^b \phi = Q_y^b P_x^a \phi$. We refer to these strategies as *state-commuting operator strategies*.

Alternatively, we can consider some sets of strategies that are formulated by placing stronger requirements. The so called *tensor product strategies* are determined by requiring the Hilbert space H to have a decomposition in terms of tensor products as $H = H_A \otimes H_B$. The projections for Alice and Bob are required to only act non-trivially on H_A and H_B, respectively. It was originally conjectured by Tsirelson that the closure of the set of tensor product strategies was equal to the set of commuting operator strategies. This was recently shown to be incorrect [JNV$^+$20].

In the case that the underlying Hilbert space H is restricted to be finite dimensional, the set of corresponding strategies is simply referred to as *quantum strategies*.

Chapter 3

Sums of Squares

Various natural notions of positivity appear throughout mathematics. In some cases, such as the Choi-Effros characterization of abstract operator systems, positivity really explains much of the underlying structure [CE77]. One of the most intuitive notions of positivity is given by the square of a number. In the case of the complex numbers $\mathbb{C}$, it is straightforward to determine if a number α is positive, namely α is positive if we can express it as a hermitian square $\alpha = \beta\overline{\beta}$. Informally we can view the decomposition $\beta\overline{\beta}$ here as a witness of the positivity of α.

Finding such a witness in various different contexts is the essence of sum of squares (SOS) techniques. The high level idea underlying this approach is that if an object satisfies some natural notion of positivity then there should be an obvious explanation, or SOS proof, of this fact. It is not always the case that an SOS certificate is necessary for positivity.

The 17-th problem in Hilbert's famous list of unsolved problems aimed to characterize when a real polynomial in several variables takes only non-negative values. In 1888, Hilbert [Hil88] proved that not all such polynomials are sums of squares: the first explicit counter example was due to Motzkin [Mot67], with later counter examples due to Robinson [Rob69], Choi [CL76], and Lam [CL77]. It should be noted that for each of these counterexamples, the sum of the coefficients is zero. A proper characterization was famously given by Emil Artin in 1927, who confirms that such polynomials must be a sum of squares of rational functions [Art27] in any number of variables.

In this Chapter we are concerned with generalizations of these ideas to the setting of non-commutative algebras. In Section 3.4 we connect these concept to the topic of non-local games.

3.1 Non-commutative Sums of Squares

In 2002, a highly celebrated paper due to Helton [Hel02], similar considerations were made for so called non-commutative polynomials. Informally, non-commutative polynomials are polynomials in several variables, $X_1, \ldots X_n$, in which $X_i X_j$ is not identified with $X_j X_i$. Instead of evaluating such polynomials at tuples of points they are evaluated at tuples of real matrices. Helton shows that if a non-commutative polynomial returns a positive semi-definite matrix under all evaluations then it must be expressible as a sum of squares. A simplified argument due to McCollough and Putinar extends Helton's result to the complex numbers [MP05].

A more formal description of these results can be stated in terms of $*$-algebras. Indeed, non-commutative polynomials can be viewed as elements in the the complex algebra A, that is freely generated by variables $X_1, \ldots X_n$. We can equip A with a formal involution by extending the map $X_i \mapsto X_i^*$ in the natural way. Note, we do not require any relations to hold between X_i and X_i^*. We call A, equipped with this involution, the free $*$-algebra in n variables. In this setting, evaluating non-commutative polynomials at a tuple of matrices corresponds to a finite dimensional $*$-representation of A. Using this formalism we can state the results of Putinar and McCollough as follows.

Theorem 3.1.1. *Let A be the free $*$-algebra in n variables. If a hermitian element $f \in A$ is positive under all finite dimensional $*$-representations then there exists $g_1, \dots g_m \in A$ such that $f = \sum_i g_i g_i^*$.*

In Section 3.4 we explain the connections between non-commutative sums of squares and strategies for non-local games. Theorem 3.1.1 is often invoked in the context of sums of squares proofs for non-local games. As we will see in Section 3.4 the $*$-algebra A is not exactly the right object to work with in the context of non-local games. This is because the operators that Alice and Bob use to make a quantum strategy for a non-local game satisfy some relations. For example, in a quantum strategy for the CHSH game, Alice and Bob both use observables of order 2 that commute with one another. The correct language to describe these relations is found by extending the idea sums of squares to group rings.

3.2 Sums of Squares for Group Rings

Let $\mathbb{C}[G]$ be the $*$-algebra of a discrete group G. As in the case of non-commutative polynomials, we use $*$-representations to play the role of evaluation of our "polynomials". In this setting $*$-representation correspond to unitary representations of the group. In order to obtain an analgue of Theorem 3.1.1 for groups rings we need to understand the answer to the following question.

Question 3.2.1. *If $b \in \mathbb{C}[G]$ is hermitian and $\pi(g)$ is positive semidefinite for all unitary representations π, then is b necessarily expressible as a sum of hermitian squares?*

Answers to this question have been provided in the positive for $G = \mathbb{F}_n$, the free group on n generators, and $G = \mathbb{Z}^2$. The free group case has been credited to Schmüdgen, although it originally appears in the following paper by Netzer and Thom [NT13]. Netzer and Thom credit the work of Scheiderer in [Sch06], [Sch99] to resolve this question in the positive for $\mathbb{Z}^2$ and in the negative for $\mathbb{Z}^3$ respectively.

A slightly stronger result for $\mathbb{F}_n$ is due to Ozawa [Oza13]. Ozawa shows that if $b \in \mathbb{C}[\mathbb{F}_n]$ is hermitian with $supp(b) \subseteq EE^{-1}$ and b is positive semidefinite under all unitary representations then b is expressible as $b = \sum a_i a_i^*$ where $supp(a_i) \subseteq E$. Here $supp(b)$ denotes the support of b. In [Rud63] Rudin shows that there exists an element $f \in \mathbb{C}[\mathbb{Z}^2]$ with support that is contained in the set $\{(i, j) : |i| \leq 2N, |j| \leq 2N\}$ for some integer $N \geq 3$, satisfying $\chi(f) \geq 0$ for all $\chi \in \mathbf{T}^2$ but f can not be expressed as a sum $b = \sum a_i a_i^*$ where for each i the support of a_i is contained in the set $\{(i, j) : 0 \leq i \leq N, 0 \leq j \leq N\}$. As a consequence we know $\mathbb{Z}^2$ does not satisfy this stronger version of the sum of squares property.

In [Oza13] it is shown that, for any discrete group G, if b is a hermitian element in $\mathbb{C}[G]$ that is positive under all unitary representations then b must be in the so called archimedean closure of the cone sums of hermitian squares. That is, for all $\varepsilon > 0$ we have $b + \varepsilon 1$ is expressible as a sum of hermitian squares.

In this section we obtain a new sum of squares result for the group ring of $\mathbb{Z}^k$. We consider hermitian elements whose coefficient sum is non-zero. We show that if b is such an element then b is positive under all unitary representations if and only if it is expressible as a sum of hermitian squares. In order to obtain this result we borrow heavily from the results of Netzer and Thom who introduce *generalized representations* of a group in their proof that $\mathbb{F}_n$ satisfies the *sum of squares property* [NT13]. We use amenability of $\mathbb{Z}^k$ which provides an important approximation property for the left regular representation of $\mathbb{Z}^k$. This allows us to apply the techniques of Netzer and Thom to elements $b \in \mathbb{C}[\mathbb{Z}^n]$ that are not in the augmentation ideal.

3.2.1 Notation

Let G be a discrete group and let $\mathbb{C}[G]$ denote the usual group algebra of G. Elements of $\mathbb{C}[G]$ are formal finite linear combinations of elements from G. A typical element is of the form $b = \sum_g \alpha_g g$ with all but finitely many α_g equal to 0. The group algebra also comes equipped with the following involution, $(\sum_g \alpha_g g)^* := \sum_g \overline{\alpha_g} g^{-1}$. Let $\mathbb{C}[\mathbb{G}]_h$ denote the set of elements b in group algebra that satisfy $b^* = b$. We let $\sum^2 \mathbb{C}[G]$ denote the set of all elements $b \in \mathbb{C}[G]$ that are expressible as a sum of hermitian squares. That is, there exists elements $f_1, \ldots f_m$ such that $b = \sum_i f_i^* f_i$.

We define the augmentation homomorphism $\varepsilon : \mathbb{C}[G] \to \mathbb{C}$ by,

$$\varepsilon(\sum_g \alpha_g g) = \sum_g \alpha_g.$$

The kernel of ε is known as the augmentation ideal of $\mathbb{C}[G]$,

$$\omega(G) := \mathrm{Ker}(\varepsilon) = \left\{ a = \sum_g \alpha_g g \in \mathbb{C}[G] : \sum_g \alpha_g = 0 \right\}.$$

We will also make use of ultrafilters and ultraproducts. Given an ultrafilter ω, let $\mathbb{R}^\omega$ denote the ultrapower of the reals. We let $\mathbf{C}$ denote the algebraically closed field $\mathbb{R}^\omega[i]$. Note that the ultrapower $\mathbb{R}^\omega$ can be equiped with a topology in a natural way, see [Ban77]. Thus it makes sense to consider limits of sequences of numbers in $\mathbf{C}$.

We also recall the definition of doubly commuting operators.

Definition 3.2.2. Let A and B be linear operators on a Hilbert space. We say that A and B doubly commute if $[A, B] = [A, B^*] = [A^*, B] = 0$.

3.2.2 Generalized Representations

In [NT13] Theorem 3.11 the following powerful seperation theorem is given.

Theorem 3.2.3 (Netzer and Thom)**.** *Let G be a discrete group and let b be an element in the group ring that is not expressible as a sum of hermitian squares. Then there exists, an ultrafilter ω and a $\mathbb{C}$-linear functional $\phi : \mathbb{C}[G] \to \mathbf{C} = \mathbb{R}^\omega[i]$, with $\phi(a^*) = \overline{\phi(a)}$ such that,*

$$\phi(b) < 0 \textit{ and } \phi(a^* a) > 0 \textit{ for all } a \in \mathbb{C}[G] \backslash \{0\}.$$

One can apply the famed GNS construction on ϕ to obtain a $\mathbf{C}$-vector space equipped with a positive definite sesquilinear form that takes values in $\mathbf{C}$. The details of this construction are contained in the proof of Theorem 3.3.1. For a good review of this construction see [Dav96]. More generally if $\mathbf{C} = \mathbb{R}^\omega$ for some ultrafilter ω we have the following generalized notion of a Hilbert space.

Definition 3.2.4. A vector space H over $\mathbf{C}$ is called a generalized Hilbert space if it comes equipped with a $\mathbf{C}$-valued positive definite sesquilinear form $\langle \cdot, \cdot \rangle$.

This sesquilinear form gives rise to a **C**-valued norm on H. Note in our definition that we do not require H to be complete with respect to this norm.

We will use $L(H)$ to denote the set of linear operators on this space. Since $\mathbb{R}^{\omega}$ may fail to satisfy the least upper bound property it is not possible to define an operator norm here. Nevertheless we can still use this sesquilinear form to determine the adjoint of a linear operator as well as a unitary linear map, $U \in B(H)$ such that $U^*U = UU^* = I$. Using this adjoint we can view $L(H)$ as a $*$ algebra.

3.2.3 Approximation Properties of the Ring of Integers

Amenability of a discrete group is a well studied subject. For good introduction to the topic in a context relevant to this paper see [Oza13]. In the case of $\mathbb{Z}^n$, amenability of this group allows us to conclude some strong approximation properties about the left regular representation $\lambda : \mathbb{Z}^n \to L(\mathbb{C}[\mathbb{Z}^n])$. In particular we will make use of the following well known construction.

Proposition 3.2.5. *There exists a sequence of unit vectors $v_i \in \mathbb{C}(G)$ such that $|\langle \lambda(s)v_i, v_i\rangle_{\mathbb{C}(G)} - 1| \to 0$ for all $s \in \mathbb{Z}^n$.*

Proof. Let F_i be a Følner sequence for $\mathbb{Z}^n$. We then define

$$v_i = \frac{1}{|F_i|^{\frac{1}{2}}}\chi_{F_i}.$$

We then confirm the following calculations

$$\begin{aligned}\|\lambda(s)v_i - v_i\|_{\mathbb{C}(G)} &= \|\frac{1}{|F_i|^{\frac{1}{2}}}\chi_{sF_i} - \frac{1}{|F_i|^{\frac{1}{2}}}\chi_{F_i}\|_{\mathbb{C}(G)} \\ &= \frac{|sF_i \triangle F_i|}{|F_i|} \to 0.\end{aligned}$$

Note this also tells us that $\langle \lambda(s)v_i, v_i\rangle_{\mathbb{C}(G)} \to 1$.

$$\begin{aligned}|\langle \lambda(s)v_i, v_i\rangle_{\mathbb{C}(G)} - 1| &= |\langle \lambda(s)v_i, v_i\rangle_{\mathbb{C}(G)} - \langle v_i, v_i\rangle_{\mathbb{C}(G)}| \\ &= |\langle \lambda(s)v_i - v_i, v_i\rangle_{\mathbb{C}(G)}| \\ &\leq \|\lambda(s)v_i - v_i\|_{\mathbb{C}(G)} \to 0\end{aligned}$$

where the last inequality is obtained by applying Cauchy Schwarz inequality. □

3.3 A Weak Sum Of Squares Property

Given a generalized Hilbert space H, an operator $X \in L(H)$, and integer $m \in \mathbb{Z}$ we introduce the following notation,

$$X(m) = \begin{cases} X^m, & m \geq 0 \\ X^{*^{-m}}, & m \leq 0 \end{cases}.$$

Using this notation we are now ready to state the following result.

Theorem 3.3.1. *let $b = \sum_{(n_1,\dots n_d)} \alpha_{n_1,\dots n_d}(n_1,\dots,n_d) \in \mathbb{C}[\mathbb{Z}^d]_h$ with b not in the augmentation ideal, $\omega(\mathbb{Z}^d)$, and $b \notin \sum^2 \mathbb{C}[\mathbb{Z}^d]$. Then there exists a d-tuple, $X = (X_1,\dots,X_d)$, of doubly commuting contractions on a finite dimensional Hilbert space $\mathcal{K}$, and a vector $x \in \mathcal{K}$ such that,*

$$\left\langle \sum_{(n_1,\dots n_d)} \alpha_{(n_1,\dots,n_d)} X_1(n_1)\dots X_k(n_d)x, x \right\rangle < 0.$$

Proof. In order to keep the notation concise the following proof is given for the case $\mathbb{Z}^2$. The more general case can be seen to follow from the same argument.

Let $b = \sum \alpha_{(m,n)}(m,n)$ be a hermitian element of the group ring that is not expressible as a sum of hermitian squares. Then by [NT13, Thm. 3.11], there exists an ultrapower $\mathbf{R} = \mathbb{R}^{\omega}$, and a completely positive linear functional $\phi : \mathbb{C}[\mathbb{Z}^2] \to \mathbf{C} := \mathbf{R}[i]$ with,

$$\phi(a^*) = \overline{\phi(a)}, \text{ and } \phi(b) < 0.$$

Let $A = \mathbf{C} \otimes_{\mathbb{C}} \mathbb{C}[\mathbb{Z}^2]$. Then A is a $*$-algebra over $\mathbf{C}$ and we can extend ϕ to a complete positive map on A in a canonical way. We next apply the GNS construction on ϕ. Define the the following ideal in A,

$$N := \{a \in A : \phi(a^*a) = 0\}.$$

Let H represent the quotient A/N. H comes equipped with the $\mathbf{C}$-valued form,

$$\langle a + N, c + N \rangle = \phi(c^*a).$$

We define a generalized representation $\pi : \mathbb{C}[\mathbb{Z}^2] \to L(H)$ by $\pi(f)h = f \cdot h$. and let $\xi := 1 + N \in H$. Note $\langle b\xi, \xi \rangle = \phi(b) < 0$.

We can now construct the generalized representation $\lambda \otimes \pi : \mathbb{Z}^2 \to L(\mathbb{C}(\mathbb{Z}^2) \otimes_{\mathbb{C}} H)$ defined by,

$$\lambda \otimes \pi(g)(a \otimes h) = \lambda(g)a \otimes \pi(g)h.$$

Here we are viewing $\mathbb{C}(\mathbb{Z}^2) \otimes_{\mathbb{C}} H$ as a $\mathbf{C}-$vector space, equipped with the sesquilinear form

$$\langle a_1 \otimes h_1, b_1 \otimes h_2 \rangle = \langle a_1, a_2 \rangle_{\mathbb{C}[\mathbb{Z}^2]} \cdot \langle h_1, h_2 \rangle_H.$$

We also need to introduce the following generalized representation $\lambda \otimes I : \mathbb{Z}^2 \to L(\mathbb{C}(\mathbb{Z}^2) \otimes_{\mathbb{C}[\mathbb{Z}^2]} H)$ defined by,

$$\lambda \otimes I(g)(a \otimes h) = \lambda(g)a \otimes h.$$

By proposition 3.2.5 there exists a sequence of vectors $v_i \in \mathbb{C}[\mathbb{Z}^2]$ satisfying $\langle \lambda(s)v_i, v_i \rangle \to 1$ for all $s \in \mathbb{Z}^2$. We then see that $\langle \lambda(b)v_i, v_i \rangle = \sum \alpha_{m,n} \langle \lambda((m,n))v_i, v_i \rangle \to \sum \alpha_{m,n} = 1$. (We may assume that $\sum \alpha_{m,n} = 1$. If this was not the case then we can simply normalize since $b \notin \omega(\mathbb{Z}^2)$.) We thus get,

$$\begin{aligned}
\langle \lambda \otimes \pi(b))(v_i \otimes \xi), v_i \otimes \xi \rangle &= \langle \pi(b)\xi, \xi \rangle_H \cdot \langle \lambda(b)v_i, v_i \rangle \\
&= \langle \pi(b)\xi, \xi \rangle_H \cdot \left(\sum \alpha_{m,n} \langle \lambda((m,n))v_i, v_i \rangle \right) \\
&\to \langle \pi(b)\xi, \xi \rangle_H < 0.
\end{aligned}$$

Thus we can fix large enough i such that $x = v_i \otimes \xi$ satisfies,

$$\langle \lambda \otimes \pi(b)x, x \rangle < 0.$$

Recall in Proposition 3.2.5, v_i was defined using a finite set $F_i \subseteq \mathbb{Z}^2$. That is we can write x as,

$$x = \frac{1}{|F_i|^{\frac{1}{2}}} \sum_{(m,n)\in F_i} \delta_{(m,n)} \otimes \xi.$$

Define a new vector $x' \in \mathbb{C}[\mathbb{Z}^2] \otimes H$ as

$$\frac{1}{|F_i|^{\frac{1}{2}}} \sum_{(m,n)\in F_i} \delta_{(m,n)} \otimes \pi(m,n)\xi.$$

Using Fell's absorption principle we can confirm that,

$$\langle \lambda \otimes I(b)x', x'\rangle = \langle \lambda \otimes \pi(b)x, x\rangle < 0.$$

From here we wish to define a finite dimensional subspace of $K \subseteq \mathbb{C}[\mathbb{Z}^2] \otimes H$ with the goal of eventually applying the transfer principle. Let us define integers D_1 and D_2 by $D_1 := \max\{|x|, |y| : (x,y) \text{ is in the support of } b\}$ and $D_2 := \max\{|m|, |n| : (m,n) \in F_i\}$. Then consider the following subspace,

$$K := \operatorname{span}\{\delta_{(a,b)} \otimes \pi(m,n)\xi : |a|, |b| \leq D_1 + D_2, \text{ and } |m|, |n| \leq D_2\}.$$

It is clear from the definition of K that we have both x' and $\lambda \otimes I(b)x' \in K$. We next let $A := \lambda \otimes I(1,0)$ and $B := \lambda \otimes I(0,1)$. We now wish to show PAP and PBP doubly commute, where P is the orthogonal projection onto K. The fact that such an orthogonal projection exists follows from applying the Gram-Schmidt process to find an orthonormal basis of K. We explore the different cases. Suppose $k = \delta_{(a,b)\otimes\pi((m,n)\xi} \in K$ and we have $|a+1|$ and $|b+1| \leq D_1 + D_2$. Then we have $Ak, Bk, ABk, BAk \in K$ and hence,

$$PAPPBPk = PAPBk = PABk = PBAk = PBPPAPk.$$

We now turn our attention to the other cases. Consider $k = \delta_{(a,b)} \otimes \pi(m,n)\xi \in K$ with $|a+1| > D_1 + D_2$. Note that we will have $Ak, ABk = BAk, \in K^{\perp}$. Indeed if $k' = \delta_{(a',b')} \otimes \pi(m',n')\xi \in K$ then $a+1 \neq a'$ so $\delta_{(a,b)} \perp \delta_{(a',b')}$ and $\delta_{(a,b+1)} \perp \delta_{(a',b')}$ in $\mathbb{C}[\mathbb{Z}^2]$ and so,

$$\langle Ak, k'\rangle = \langle \delta_{(a+1,b)}, \delta_{(a',b')}\rangle \cdot \langle \pi(m,n)\xi, \pi(m'n')\xi\rangle = 0$$
$$\langle ABK, k'\rangle = \langle \delta_{(a+1,b+1)}, \delta_{(a',b')}\rangle \cdot \langle \pi(m,n)\xi, \pi(m'n')\xi\rangle = 0.$$

Hence,

$$PAPPBPk = PBPPAPk = 0.$$

The case for $k = \delta_{(a,b)} \otimes \pi(m,n)\xi \in K$ with $|b+1| > D_1 + D_2$ is symmetric so we also get,

$$PAPPBPk = PBPPAPk = 0.$$

Let $X = PAP$ and $Y = PBP$. Above we have shown that X commutes with Y and a similar argument will show that X commutes with Y^* and Y commutes with X^*.

We also have the following identity,

$$\left\langle \sum_{(m,n)\in \operatorname{supp}(b)} \alpha_{(m,n)} X(m)Y(n)x', x' \right\rangle = \langle \lambda \otimes I(b)x', x'\rangle < 0. \tag{3.3.1}$$

Recall that, for $m, n \in \mathbb{Z}$ we have,

$$X(m) = \begin{cases} X^m, & m \geq 0 \\ X^{*^{-m}}, & m \leq 0 \end{cases} \text{ and } Y(n) = \begin{cases} Y^n, & n \geq 0 \\ Y^{*^{-n}}, & n \leq 0 \end{cases}$$

To conclude proof we need to apply a version of the Lefschetz transfer principle. Let d denote the dimension of finite dimensional vector space K over $\mathbf{C}$. We can view X as a $d \times d$ matrix $X = (x_{i,j})$ with entries from $\mathbf{C}$ and we can view $k \in K$ as the tuple $k = (k_1, k_2, \ldots k_d) \in \mathbf{C}^d$. Since $X = PAP$ we have for all $k \in K$ we have $\|Xk\| \leq \|k\|$. A similar consideration can be made for Y. We then can conclude the following statements about $\mathbf{C}$,

$$\exists\ X = x_{i,j} \in \mathbf{C}^{d \times d} \text{ such that } \forall (k_1, \ldots, k_d) \in \mathbf{C}^d, \text{ we have } \sum_j \left| \sum_i k_j x_{i,j} \right|^2 \leq \sum_j |k_j|^2.$$

$$\exists\ Y = y_{i,j} \in \mathbf{C}^{d \times d} \text{ such that } \forall (k_1, \ldots, k_d) \in \mathbf{C}^d, \text{ we have } \sum_j \left| \sum_i k_j y_{i,j} \right|^2 \leq \sum_j |k_j|^2.$$

$$\exists x' \in \mathbf{C}^d \text{ such that } \langle \sum \alpha_{m,n} X(m) Y(n) x', x' \rangle < 0.$$

$$[X, Y] = [X, Y^*] = [X^*, Y].$$

We can apply the transfer principle to these first order statements to conclude the following:

There exists a finite dimensional Hilbert space $\mathcal{K}$ along with vector $x \in \mathcal{K}$ and doubly commuting contractive operators X and Y on $\mathcal{K}$ such that the identity in (1) holds. □

We will spend the rest of this section showing how one can use Theorem 3.3.1 to show $\mathbb{Z}^k$ satisfies a weak sum of squares property. We state the well known dilation results due to Sz-Nagy and Foias for convenience.

Theorem 3.3.2 (Sz-Nagy-Foias). *Let $\{T_i\}_{i=1}^n$ be a family of doubly commuting contractions on a Hilbert space $\mathcal{K}$. Then there exists a Hilbert space $\mathcal{H}$ containing $\mathcal{K}$ as a subspace, and a family of doubly commuting unitaries $\{U_i\}_{i=1}^n$ on $\mathcal{H}$, such that*

$$T_1(k_1) \ldots T_n(k_n) = P_{\mathcal{K}} U_1^{k_1} \ldots U_n^{k_n}|_{\mathcal{K}}.$$

Applying this dilation theorem to our previous result we get the following.

Corollary 3.3.3. *Let $k \in \mathbb{N}$ and $b \in \mathbb{C}[\mathbb{Z}^k]_h$ with $b \notin \omega(\mathbb{Z}^d)$. If $\pi(b) \geq 0$ for all unitary representations then $b \in \Sigma^2\mathbb{C}[\mathbb{Z}^d]$.*

Proof. Given such an element, if $b \notin \sum^2 \mathbb{C}[\mathbb{Z}^d]$ then by Theorem 3.3.1 there exists a d-tuple, $X = (X_1, \ldots, X_d)$, of doubly commuting contractions on a finite dimensional Hilbert space $\mathcal{K}$,and a vector $x \in \mathcal{K}$ such that,

$$\left\langle \sum_{(n_1, \ldots n_d)} \alpha_{(n_1, \ldots, n_d)} X_1(n_1) \ldots X_d(n_d) x, x \right\rangle < 0.$$

Applying Theorem 3.3.2 there exist doubly commuting unitary operators $U_1, \dots U_d$ on a Hilbert space $\mathcal{H} \supseteq \mathcal{K}$ such that,

$$\left\langle \sum_{(n_1,\dots n_d)} \alpha_{(n_1,\dots,n_d)} U_1(n_1) \dots U_d(n_d)x, x \right\rangle < 0.$$

Since this tuple of unitaries doubly commute then they can induce a unitary representation $\pi : \mathbb{Z}^d \to B(\mathcal{H})$ defined by

$$\underbrace{\pi((0,0,\dots,1\dots,0))}_{i} = U_i.$$

Finally since $\langle \pi(b)x, x \rangle < 0$ we obtain a contradiction. □

3.4 Non-local games and Sums of Squares

3.4.1 Groups and Commuting Operator Strategy Correspondence

In [PHMS19] the authors describe a correspondence between unitary representations of a particular family of groups and the operators of Alice and Bob in a commuting operator strategy. Below we outline some of the details of this correspondence. Once this correspondence is established we can describe the connection between the sum of squares property for these groups and the quantum value of a non-local game.

In Chapter 2 we saw the formal definition of commuting operator strategies for non-local games. For convenience we restate the definition here.

Definition 3.4.1. [Commuting Operator Strategies] P is a commuting operator strategy for a non-local game $(V, I_A, I_B, O_A, O_B, \pi)$ if there exists a tuple $(H, \phi \in H, \{P_x^a\}, \{Q_y^b\})$, where H is a Hilbert space, $\phi \in H$ is a unit vector, and $\{P_x^a\}$ and $\{Q_y^b\}$ are families of projections that satisfy,

1. $\sum_a P_x^a = I$ for all $x \in I_A$
2. $\sum_b Q_y^b = I$ for all $y \in I_B$
3. $P_x^a Q_y^b = Q_y^b P_x^a$ for all x, y, a, b
4. $P(a, b|x, y) = \langle P_x^a Q_y^b \phi, \phi \rangle$.

For each input the measurement systems of Alice and Bob can be used to construct a unitary operator in a canonical way. Let $n = |I_A|$ and $m = |O_A|$. For convenience we label the input and output set for Alice as $I_A = \{0, \dots, n-1\}$ and $O_A = \{0, 1, \dots, m-1\}$. If we let $\omega = e^{\frac{2\pi i}{m}}$ then for each $x \in I_A$ we can define the following order m unitary operator,

$$U_x := \sum_{a=0}^{m-1} \omega^a P_x^a.$$

Given any collection of n such unitaries $\{U_x\}_{x \in I_A}$ the universal property of free-products allows us to define a representation for the group $\mathbb{F}(n, m) := \mathbb{Z}_m * \mathbb{Z}_m * \cdots * \mathbb{Z}_m$.

Similarly, if we take $r = |I_B|$ and $s = |O_B|$ and we let $\mu = e^{\frac{2\pi i}{s}}$ then one can obtain a collection of order r unitaries via the formula

$$V_y := \sum_{b=0}^{s-1} \mu^b Q_y^b.$$

The collection $\{U_x, V_y\}$ determines a unitary representation for the group $\mathbb{F}(n,m) \times \mathbb{F}(r,s)$.

In [PHMS19] a converse to the above construction also holds. That is, given any unitary representation of the group $\mathbb{F}(n,m) \times \mathbb{F}(s,r)$ one can construct a collection of commuting projections for Alice and Bob that satisfy 1.,2. and 3. for Definition 3.4.1. To see this we let $\{U_x, V_y\}$ denote the canonical generators of the group and define the following elements in the group ring $\mathbb{C}[\mathbb{F}(n,m) \times \mathbb{F}(s,r)]$,

$$P_x^a := \frac{1}{m}\sum_{k=0}^{m-1}(\omega^{-a}U_x)^k. \tag{3.4.1}$$

$$Q_y^b := \frac{1}{s}\sum_{k=0}^{s-1}(\mu^{-b}V_y)^k. \tag{3.4.2}$$

If $\pi : \mathbb{C}[\mathbb{F}(n,m) \times \mathbb{F}(s,r)] \to B(H)$ is a unitary representation then $\pi(P_x^a), \pi(Q_y^b)$ will be such a set of projections for Alice and Bob.

3.4.2 Sum of Squares Certificates for Games

Given a non-local game $\mathcal{G} = (V, I_A, I_B, O_A, O_B, \pi)$ and strategy $P = P(a,b|x,y)$ we can calculate the probability of winning, w_P, as

$$w_P = \sum_{x,y,a,b} V(x,y,a,b)\pi(x,y)P(a,b|x,y).$$

The *commuting operator value* of the game G is then taken to be the supremum of w_P over all commuting operator strategies P. To each such game we can define a particular element of the group algebra $\mathbb{C}[\mathbb{F}(n,m) \times \mathbb{F}(s,r)]$ called the *game polynomial* $f_{\mathcal{G}}$ defined by,

$$f_{\mathcal{G}} := \sum_{x,y,a,b} V(x,y,a,b)\pi(x,y)P_x^a Q_y^b.$$

Using the correspondence between commuting operator strategies and unitary representations of the associated groups we obtain the following result.

Theorem 3.4.2. *Given a non-local game $(V, I_A, I_B, O_A, O_B, \pi)$, λ is an upper bound for the commuting operator value of this game if and only if for all unitary representations, π of $\mathbb{C}[\mathbb{F}(n,m) \times \mathbb{F}(s,r)]$, we have $\pi(\lambda 1 - f_{\mathcal{G}})$ is a positive semi-definite operator.*

We know from [Oza13] that if a hermitian element in the group ring $\mathbb{C}[\mathbb{F}(n,m) \times \mathbb{F}(s,r)]$ is positive under all representations then it must be in the so called archimedian closure of the elements expressible as sums of hermitian squares. Consequently we have the following result.

Theorem 3.4.3. *Given a non-local game $\mathcal{G} = (V, I_A, I_B, O_A, O_B, \pi)$, λ is a strict upper bound for the commuting operator value of this game if and only if $\lambda 1 - f_{\mathcal{G}}$ is expressible as a sum of hermitian squares.*

In [NPA08] a useful semi-definite program is given to determine if λ is a strict upper bound on the commuting operator value of a given non-local game. In [PNA10] the authors provide a semi-definite program to obtain a sum of squares certificate for strict upper bounds on the commuting operating value. The answer to Question 3.2.1 is still not known for the group $\mathbb{F}(n,m) \times \mathbb{F}(s,r)$ and hence it is not known if the commuting operator value of a game will always have a corresponding sum of squares certificate.

Conjecture 3.4.4. *If λ is the commuting operator value for for a non-local game, $\mathcal{G}$, then $\lambda 1 - f_{\mathcal{G}}$ is expressible as a sum of hermitian squares.*

In [Oza13], a stronger sum of squares property is shown to hold for the free group. More specifically, the answer to the following question is yes for the case G is the free group with k generators.

Question 3.4.5. *Suppose $b \in \mathbb{C}[G]$ is hermitian with the support of b contained in $E^{-1}E$. If $\pi(b)$ is positive semidefinite for all unitary representations π, then is b necessarily expressible as a sum of hermitian squares, $b = \sum_i f_i^* f_i$, with each f_i having support in E?*

By Tarski–Seidenberg theorem it is a decidable problem to determine if an element $b \in \mathbb{C}[G]$ is is expressible as $b = \sum_i f_i^* f_i$ with each f_i having support in E. In [Slo19] Slofstra shows that determining whether or not a non-local game has commuting operator value strictly less then 1 is an undecidable problem. As a consequence of this fact we get the following result. This argument was shared with me in a private email exchange with William Slofstra.

Theorem 3.4.6. *The answer to Question 3.4.5 is no for the case $G = \mathbb{F}(n,m) \times \mathbb{F}(s,r)$.*

A non-local game $\mathcal{G} = (V, I_A, I_B, O_A, O_B, \pi)$ is called *synchronous* when $I_A = I_B$ and $O_A = O_B$ and $v(x,x,a,b) = 0$ whenever $a \neq b$. In the case of synchronous games the representation theory theory of the group $\mathbb{F}(n,m)$ determines the possible commuting operator strategies for Alice and Bob. It is still not known if the answer to either Question 3.2.1 or Question 3.4.5 is yes. The following conjecture is then worth investigation.

Conjecture 3.4.7. *If λ is the commuting operator value for for a synchronous non-local game then $\lambda 1 - f_{\mathcal{G}} = \sum_i f_i^* f_i$, with each f_i having support in E, where E is a set that is computable using the support of $\lambda 1 - f_{\mathcal{G}}$.*

Chapter 4

Quantum Graphs

4.1 Introduction

Given a graph on n vertices one can associate two different subspaces of the $n \times n$ matrices that encode all of the information of the graph. This has motivated the generalization of several well known graph theoretic concepts to a larger class of objects.

In [DSW13], Duan, Severini, and Winter describe a version of non-commutative graph theory whose underlying objects consist of *submatricial operator systems*. The aforementioned authors generalize the independence number and Lovász theta number to submatricial operator systems.

In [Sta16], Stahlke works with a similar but distinct definition of a non-commutative graph. Instead of working with submatricial operator systems, Stahlke associates a subspace of matrices whose elements all have zero trace to a graph. Stahlke generalizes several classical graph theory concepts to these traceless subspaces including the chromatic number, clique number and notion of graph homomorphism.

Thus, there are two quite different subspaces of matrices to associate to graphs that lead to two different ways to create a non-commutative graph theory. In this paper we discuss both the *submatricial operator system* and *submatricial traceless self-adjoint operator space* definitions of a non-commutative graph.

There is currently no notion of the complement of a non-commutative graph that generalizes the graph complement. By working with both of the above definitions we are able to generalize the complement of a graph using the orthogonal complement with respect to the Hilbert-Schmidt inner product. We conclude this section by reviewing the definition of several non-commutative graph parameters and show that some of these parameters can be approximated by evaluating classical graph parameters.

In [Lov79] Lovász introduced his well known theta number of a graph, $\theta(G)$. Lovász shows that this number determines the following bounds on the independence number, $\alpha(G)$, and the chromatic number of the graph complement $\chi(\overline{G})$.

$$\alpha(G) \leq \theta(G) \leq \chi(\overline{G}).$$

These two inequalities are often referred to as the Lovász sandwich theorem. In [DSW13], it is shown that that the independence number of a submatricial operator system is bounded above by its Lovász number. This provides the first inequality for a generalized Lovász sandwich theorem. In [Sta16] Stahlke introduces a version of the chromactic number denoted χ_{St}, that generalizes the second inequality.

In section 4.3 we introduce new generilzations of the chromatic number, χ_0 and $\widehat{\chi}$, that provide lower and upper bounds on χ_{St}. Using $\widehat{\chi}$ we provide a simplified proof of a weaker sandwich inequality. The advantage is that we can answer a question posed by Stahlke by generalizing the equation $\chi(G)\omega(\overline{G}) \geq n$ to non-commutative graphs.

Given two graphs G and H the Cartesian product is the graph $G\Box H$ with vertex set $V(G) \times V(H)$ and edge relation given by $(v, a) \sim (w, b)$ if one of $v \sim_G w$ and $a = b$ or $v = w$ and $a \sim_H b$ holds. A Theorem of Sabidussi tell us $\chi(G\Box H) = \max\{\chi(G), \chi(H)\}$ for any G and H. We introduce a Cartesian product and establish a generalization of this result for *submatricial traceless self-adjoint operator spaces* in Section 4.4 . In section 4.4 we also establish a categorical product for submatricial traceless self-adjoint operator space and extend a Theorem of Hedetniemi to submatricial traceless self-adjoint operator spaces.

4.1.1 Notation

Let M_n denote the vector space of $n \times n$ matrices over $\mathbb{C}$. This vector space can also be viewed as a Hilbert space using the inner product $\langle A, B\rangle := \text{tr}(B^*A)$. By a submatricial operator system, we mean a linear subspace S of M_n for which the identity matrix I belongs to S and for which S is closed under the adjoint map *. A submatricial traceless self-adjoint operator space is a linear subspace $\mathcal{J} \subset M_n$ for which $\mathcal{J}$ is closed under the adjoint operation * and for which given any $A \in \mathcal{J}$, the trace of A is zero.

If S and T are two submatricial operator systems, then a linear map ϕ from S into T is called completely positive (cp) if for each positive integer n, and for each positive semi-definite matrix $X = [x_{i,j}]_{i,j}$ in $M_n(S)$, the matrix

$$\phi^{(n)}(X) := \left[\phi(x_{ij})\right]_{i,j}$$

in $M_n(T)$ is positive semi-definite. We say that the cp map ϕ is unital and completely positive (ucp) if ϕ maps the identity I to the identity I. We say that ϕ is completely positive and trace preserving (cptp) if $\text{tr}(\phi(X)) = \text{tr}(X)$ for all $X \in S$. For more on cp maps see [Pau03].

We will also be using the following graph theory terminology. A graph $G = (V, E)$ is an ordered pair consisting of a vertex set V and edge set $E \subset V \times V$. Since we are working with undirected graphs we require that if $(i_1, i_2) \in E$ then $(i_2, i_1) \in E$. We say vertices i_1 and i_2 are *adjacent*, or connected by an edge, and write $i_1 \sim i_2$, whenever $(i_1, i_2) \in E$. An *independent set* of a graph G is a subset $v \subset V$ such that for any two distinct elements $i_1, i_2 \in v$ we have $i_1 \not\sim i_2$. For a graph with n vertices it will be standard to consider the vertex set to be $V = \{1, \ldots, n\}$, which we will denote by $[n]$.

4.2 Non-commutative graphs

A non-commutative graph is sometimes viewed as any submatricial operator system S. Non-commutative graphs have also been described as any submatricial traceless self-adjoint operator space $\mathcal{J}$. In this section we review how one can view a classical graph as either of these objects without losing information about the graph itself. We also discuss several parameters for non-commutative graphs.

4.2.1 Non-commutative graphs as operator systems

Definition 4.2.1. Let $G = (V, E)$ be a graph with vertex set $[n]$. Define $S_G \subset M_n$ by

$$S_G := \operatorname{span}\{E_{i,j} : (i,j) \in E \text{ or } i = j\}.$$

Observe that for any graph G, S_G will be a submatricial operator system. In [OP15], it is shown that graphs G and H are isomorphic if and only if S_G and S_H are isomorphic in the category of operator systems. We discuss this in more details in 4.2.2.

Given a graph G, if vertices i, j are not adjacent, then $e_i e_j^* = E_{i,j}$ is orthogonal to the submatricial operator system S_G. Similarly if $\{i_1, \dots, i_k\}$ is an independent set of vertices in G then for any $j \neq k$ we have $e_{i_j} e_{i_k}^*$ is orthogonal to S_G. If $v = (v_1, \dots, v_k)$ is an orthonormal collection of vectors in $\mathbb{C}^n$ then v called an *independent set* for a submatricial operator system $S \subset M_n$ if for any $i \neq j$, $v_i v_j^*$ is orthogonal to S.

Definition 4.2.2. Let S be a submatricial operator system. We define the *independence number*, $\alpha(S)$, to be the largest $k \in \mathbb{N}$ such that there exists an independent set for S of size k.

A graph $G = (V, E)$ has a k-colouring if and only if there exists a partition of V into k independent sets. In [HPP16] Paulsen defines a natural generalization of the chromatic number to non-commutative graphs. We say a submatricial operator system $S \subset M_n$ has *k-colouring* if there exists an orthonormal basis for $\mathbb{C}^n$, $v = (v_1, \dots, v_n)$, such that v can be partitioned into k independent sets for S.

Definition 4.2.3. Let $S \subset M_n$ be a submatricial operator system. The *chromatic number*, $\chi(S)$, is the least $k \in \mathbb{N}$ such that S has a k-colouring.

For any submatricial operator system $S \subset M_n$ we have $\chi(S) \leq n$ since you can partition any basis of $\mathbb{C}^n$ into n independent sets. In Theorem 4.2.12 we show that both of the above parameters provide a generalization of the classical graph theory parameters, that is we show $\alpha(S_G) = \alpha(G)$ and $\chi(S_G) = \chi(G)$. This first equality is originally found in [DSW13] and the second can be found in [HPP16].

Example 4.2.4. Consider the submatricial operator system $S := \operatorname{span}\{I, E_{i,j} : i \neq j\} \subset M_n$. Let u_1, u_2 be two orthonormal vectors and let i be an element of the support of u_1. Since $u_1^* u_2 = 0$ there must be an element $j \neq i$ of the support of u_2. Then $\langle u_1 u_2^*, E_{i,j} \rangle = u_1(i)\overline{u_2(j)} \neq 0$. Thus we see that $\alpha(S) = 1$. This also tell us that $\chi(S) = n$.

As in [DSW13], given a graph G one can compute the Lovász theta number $\theta(G)$ as,

$$\theta(G) = \max\{\|I + T\| : I + T \geq 0,\ T_{i,j} = 0 \text{ for } i \sim j\}.$$

Here the supremum is taken over all $n \times n$ matrices and $I + T \geq 0$ indicates that $I + T$ is positive semidefinite.

The following inequality is due to Lovász. For a good self-contained review please see [Knu94].

Theorem 4.2.5. *Let G be a graph and $\overline{G}$ be the graph complement of G. Then,*

$$\alpha(G) \leq \theta(G) \leq \chi(\overline{G}).$$

In order to obtain an generalization of 4.2.5 we need to identify the the appropriate generalization of a graph complement. Given a submatricial operator system $S \subset M_n$ we use the orthogonal complement $S^\perp$ to generalize the graph complement. Note that the orthogonal complement of a submatricial operator system is no longer a submatricial operator system since it will fail to contain the identity operator. In fact since $I \in S$ we will have $\text{tr}(A) = \langle A, I \rangle = 0$ for every A element of $S^{\perp}$. In [Sta16], Stahlke works with precisely these objects. We show that it is useful to consider both submatricial operator systems and submatricial traceless self-adjoint operator spaces to generalize the graph complement.

4.2.2 The complement of a non-commutative graph

In this section, we introduce the analogue of the notion of a graph complement for non-commutative graphs. Using this, we define a notion of clique number independence number and chromatic number.

Definition 4.2.6. Let G be a finite graph with vertex set $[n]$. The *traceless self-adjoint operator space associated to G* is the linear space

$$\mathcal{J}_G := \text{span}\{E_{i,j} : i \sim j\} \subset M_n \ .$$

A *traceless non-commutative graph* is any submatricial traceless self-adjoint operator space.

Remark 1. *The traceless self-adjoint operator space $\mathcal{J}_G$ is the traceless non-commutative graph S_G given in [Sta16]. Given a finite graph G with vertex set $[n]$, we have the identity $\mathcal{J}_G^{\perp} = S_{\overline{G}}$. This identity in particular suggests that the graph complement of a non-commutative graph should be its orthogonal complement. In [Sta16], Stalhke suggests that the graph complement of $\mathcal{J}_G$ should be $(\mathcal{J}_G + \mathbb{C}I)^{\perp}$. However, this notion of complement would mean that $\mathcal{J}_{\overline{G}} \neq (\mathcal{J}_G + \mathbb{C}I)^{\perp}$ for any graph with at least two vertices. We shall see that, so long as one is willing to pay the price of working with two different notions of a non-commutative graph, the orthogonal complement is the correct analogue of the graph complement.*

Proposition 4.2.7. *The traceless self-adjoint operator subspaces of M_n are exactly the orthogonal complements of submatricial operator systems. That is, S is a submatricial operator system if and only if $S^{\perp}$ is a traceless self-adjoint operator space.*

Proof. If S is an operator subsystem of M_n then for any $X \in S^{\perp}$, $tr(X) = \langle X, I \rangle = 0$. As well, if $X \in S^{\perp}$, for any $Y \in S$, $\text{tr}(XY) = \overline{\text{tr}(Y^*X^*)} = 0$. This proves that $S^{\perp}$ is a traceless self-adjoint operator space. Conversely, if S is a traceless self-adjoint operator space, then $S^{\perp}$ contains I since for all $X \in S$, $\langle X, I \rangle = \text{tr}(X^*I) = 0$. If $X \in S^{\perp}$ then $\langle X^*, Y \rangle = \text{tr}(XY) = \overline{\text{tr}(Y^*X^*)} = 0$. Therefore, $X^* \in S^{\perp}$. This proves that $S^{\perp}$ is an operator system. □

Proposition 4.2.8. *If G is a graph with vertex set $[n]$ then $S_G^{\perp} = \mathcal{J}_{\overline{G}}$.*

Proof. Observe that for $i, j, k, l \in [n]$, $E_{ij} \in S_G^{\perp}$ if and only if for all $k \simeq_G l$, $\text{tr}(E_{ij}E_{kl}) = 0$. This is only possible if $i \sim_{\overline{G}} j$. □

It is a result of Paulsen and Ortiz [OP15, Proposition 3.1] that two graphs G and H of the same vertex set $[n]$ are isomorphic if and only if there is a $n \times n$ unitary matrix U for which $US_GU^* = S_H$.

Corollary 4.2.9. *Suppose that G and H are graphs with vertex set $[n]$. The graphs G and H are isomorphic if and only if there is an $n \times n$ unitary matrix U such that $U\mathcal{J}_GU^* = \mathcal{J}_H$.*

Proof. For any $n \times n$ unitary matrix U, $(US_GU^*)^{\perp} = U\mathcal{J}_{\overline{G}}U^*$. Since G and H are isomorphic if and only if their graph complement is, the result follows. □

Remark 2. *In [Wea17] a* qunatum graph *is defined as a reflexive, symmetric quantum relation on a $*$-subalgebra $\mathcal{M} \subseteq M_n$. In this framework a submatricial operator system S is indeed quantum graph when taking $\mathcal{M} = M_n$. This approach fails to provide a complement for a quantum graph since $S^\perp$ will fail to be a reflexive quantum relation on any $\mathcal{M} \subseteq M_n$ and hence will not be a quantum graph.*

The notion of an independent set for an submatricial operator system was described solely in terms of an orthogonality relation. We can similarly say that an orthonormal collection of vectors $v = (v_1, \ldots, v_n)$ in $\mathbb{C}^n$ is an *independent set* for a submatricial traceless self-adjoint operator space $\mathcal{J} \subset M_n$ if for any $i \neq j$, $v_i v_j^*$ is orthogonal to $\mathcal{J}$. We say $\mathcal{J}$ has a k-coloring if there exists an orthonormal basis $v = (v_1, \ldots, v_n)$ of $\mathbb{C}^n$, that can be partitioned into k independent sets for $\mathcal{J}$.

Definition 4.2.10. Let $\mathcal{J} \subset M_n$ be a submatricial traceless self-adjoint operator space.

1. The independence number, $\alpha(\mathcal{J})$, is the largest $k \in \mathbb{N}$ such that there exists an independent set of size k for $\mathcal{J}$.

2. The chromatic number $\chi(\mathcal{J})$ is the least integer k such that $\mathcal{J}$ has k-colouring.

It is not hard to show that χ is monotonic and α is reverse monotonic under inclusion. This holds when considering these as parameters on submatricial operator systems as well as submatricial traceless self-adjoint operator spaces.

Next we show that if G is a graph, S_G and $\mathcal{J}_G$ have the same independence number and chromatic number. We start with a lemma. The following proof is in [**?**, Lemma 7.28]:

Lemma 4.2.11. *Let $v_1, \ldots, v_n$ be a basis for $\mathbb{C}^n$. There exists a permutation σ on $[n]$ so that for each i, the $\sigma(i)$th component of v_i is non-zero.*

Proof. Let $A = [a_{i,j}]$ denote the matrix with column i equal to v_i. Since we have a basis, $\det(A) \neq 0$. But

$$\det(A) = \sum_{\sigma \in Sym([n])} sgn(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} .$$

There must therefore be some σ for which the product $a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}$ is non-zero. This permutation works. □

It has been shown that $\alpha(G) = \alpha(S_G)$ and $\chi(G) = \chi(S_G)$ in [DSW13] and [HPP16] respectively. We are able to obtain the analogous results for submatricial self-adjoint operator spaces.

Theorem 4.2.12. *Let G be a graph on n vertices, we have $\alpha(G) = \alpha(S_G) = \alpha(\mathcal{J}_G)$ and $\chi(G) = \chi(S_G) = \chi(\mathcal{J}_G)$.*

Proof. The inclusion $\alpha(S_G) \leq \alpha(\mathcal{J}_G)$ follow from reverse monotonicity. If $i_1, \ldots, i_k$ are an independent set of vertices in the graph G then we have that the standard vectors $e_{i_1}, \ldots, e_{i_k}$ is an independent set for S_G so we get

$$\alpha(G) \leq \alpha(S_G) \leq \alpha(\mathcal{J}_G) .$$

Next suppose that $v_1, \ldots, v_k$ are an independent set for $\mathcal{J}_G$. Then since $v_1, \ldots, v_k$ is an linearly independent set of vectors we can find a permutaiton σ on $[n]$ so that $\left\langle v_i, e_{\sigma(i)} \right\rangle$ is non-zero for all i.

We note that if vertices $\sigma(j)$ and $\sigma(k)$ are adjacent in G then we have $E_{\sigma(j),\sigma(k)} \in \mathcal{J}_G$. But then $\langle v_j v_k^*, E_{\sigma(j),\sigma(k)} \rangle = \langle v_j, e_\sigma(j) \rangle \left\langle e_{\sigma(k)}, v_k \right\rangle \neq 0$ a contradiction. Thus $\sigma(1), \ldots, \sigma(k)$ are an independent set for the graph G so $\alpha(\mathcal{J}_G) \leq \alpha(G)$. The proof for χ follows the same argument. □

Recall for a classical graph G the clique number, $\omega(G)$, satisfies that $\omega(G) = \alpha(\overline{G})$.

Definition 4.2.13. Let S be a submatricial operator system and let $\mathcal{J}$ be a submatricial traceless self-adjoint operator space.

1. Define the clique number, $\omega(S)$, to be the independence number of the submatricial traceless self-adjoint operator space $S^{\perp}$.

2. Define the clique number, $\omega(\mathcal{J})$, to be the independence number of the submatricial operator system $\mathcal{J}^{\perp}$.

It should be noted that the above definition $\omega(\mathcal{J})$ of a traceless submatricial operator space is first mentioned in [Sta16]. We can use Theorem 4.2.12 to conclude that for any graph G we have $\omega(G) = \omega(S_G) = \omega(\mathcal{J}_G)$.

The next proposition shows that α, ω, and χ may be computed purely from the associated parameters for graphs. We can achieve this by associating a family of graphs to each submatricial traceless self-adjoint operator space or submatricial operator system.

Definition 4.2.14. Given a submatricial operator system $S \subseteq M_n$ and an orthonormal basis $v = (v_1, \ldots, v_n)$ we can construct two different graphs.

1. *The confusability graph* of v, with respect to S, denoted $H_v(S)$, is the graph on n vertices with $i \sim j$ if and only if $v_i v_j^* \in S$.

2. *The distinguishability graph* of v, with respect to S, denoted $G_v(S)$ is the graph on n vertices with $i \sim j$ if and only if $v_i v_j^* \perp S$.

We can also define the confusability and distinguishability graphs of an orthonormal basis $v = (v_1, \ldots, v_n)$ with respect to submatricial traceless self-adjoint operator spaces $\mathcal{J} \subseteq M_n$ in the same way. We would then have for $S = \mathcal{J}^{\perp}$, $G_v(S) = H_v(\mathcal{J})$ and $H_v(S) = G_v(\mathcal{J})$. When it is clear what the underlying system or submatricial traceless self-adjoint operator space is we simply write G_v and H_v.

Theorem 4.2.15. *Let $\mathcal{J}$ be a submatricial traceless self-adjoint operator space in M_n and let $\mathcal{B}$ denote the set of ordered orthonormal bases for $\mathbb{C}^n$. We have the identities*

$$\begin{aligned}\alpha(\mathcal{J}) &= \sup_{v \in \mathcal{B}} \alpha(\overline{G_v}) \ , \\ \chi(\mathcal{J}) &= \inf_{v \in \mathcal{B}} \chi(\overline{G_v}) \ , \text{ and} \\ \omega(\mathcal{J}) &= \sup_{v \in \mathcal{B}} \omega(H_v) \ .\end{aligned}$$

The same identity holds if we replace $\mathcal{J}$ with a submatricial operator system in M_n.

Proof. Suppose $v_1, \ldots, v_c$ is a maximal independent set for $\mathcal{J}$, that is for $i \neq j$ we have $v_i v_j^* \perp \mathcal{J}$. We can extend this collection to an orthonormal basis $v = (v_1, \ldots, v_c, v_{c+1}, \ldots v_n)$. Note that the vertices $1, \ldots, c$ in the graph $\overline{G_v}$ are an independence set since for distinct $i, j \in [c]$ we have $v_i v_j^* \perp \mathcal{J}$. This gives $i \sim j$ in G_v. Thus there is no edge between i and j in $\overline{G_v}$. Therefore $\alpha(\overline{G_v}) \geq c$ so we have $\alpha(\mathcal{J}) \leq \sup_{v \in \mathcal{B}} \alpha(\overline{G_v})$. Conversely, for each $v \in \mathcal{B}$ if $i_1, \ldots, i_c$ are an independent set for $\overline{G_v}$ then $i_j \sim i_k$ in G_V. We then have $v_{i_1}, \ldots, v_{i_c}$ is an independent set for $\mathcal{J}$. This gives $\alpha(\mathcal{J}) \geq \alpha(\overline{G_v})$.

The proof of the second identity is similar. If $\chi(\mathcal{J}) = c$ then there exists orthonormal basis $v = (v_1, \dots, v_n)$ and a partition $P_1, \dots P_c$ of $[n]$ such that $v_i v_j^* \perp \mathcal{J}$ for distinct i and j in the same partition. Define a colouring f of $\overline{G_v}$ by having $f(i) = l$ if and only if $i \in P_l$. We see that for $i \neq j$ if we have $f(i) = f(j)$ then $v_i v_j^* \perp \mathcal{J}$ giving that $i \sim j$ in G_v so f is indeed a c colouring of $\overline{G_v}$. This gives $\chi(\mathcal{J}) \geq \inf_{v \in \mathcal{B}} \chi(\overline{G_v})$. Conversely, if f is any c colouring of $\overline{G_v}$ for some $v \in \mathcal{B}$ then we can obtain a c colouring of $\mathcal{J}$ by partitioning $[n]$ into sets $P_1, \dots P_c$ where $i \in P_l$ if and only if $f(i) = l$. Then if distinct $i, j \in P_l$ we have $i \sim j$ in G_v so $v_i v_j^* \perp \mathcal{J}$.

Lastly, suppose $(v_1, \dots, v_k)$ is a collection of orthonormal vectors such that for distinc i, j we have $v_i v_j^* \in \mathcal{J}$. We can extend this set to a orthonormal basis $v = (v_1, \dots v_n)$ and we immediately get that the vertices $\{1, \dots, k\}$ form a clique in H_v. For the other direction note for any basis $v = (v_1, \dots v_n)$ H_v has a clique $i_1, \dots, i_k$ then $v_1, \dots v_k$ will satisfy $v_i v_j^* \in \mathcal{J}$ for distinct i and j. □

We next extend the definition of Lovász' theta function, [Lov79], to non-commutative graphs. This was first extended to submatricial operator spaces in [DSW13]. We introduce a natural extension to submatricial operator systems as well.

Definition 4.2.16. Let S be a submatricial operator system and $\mathcal{J}$ be a submatricial traceless self-adjoint operator space. Define the theta number of a submatricial operator system, $\theta(S)$ and the complementary theta number of a submatricial traceless self-adjoint operator space, $\overline{\theta}$ as follows.

1. $\theta(S) = \sup\{\|I + T\| : T \in M_n,\ I + T \geq 0,\ T \perp S\}$.
2. $\overline{\theta}(\mathcal{J}) = \sup\{\|I + T\| : T \in M_n,\ I + T \geq 0, T \in \mathcal{J}\}$.

Observe that $\theta(S_G) = \theta(G)$ and $\overline{\theta}(\mathcal{J}_G) = \theta(\overline{G})$ for all graphs G.

Example 3. *Recall the previously mentioned submatricial operator system $S := \operatorname{span}\{I, E_{i,j} : i \neq j\} \subset M_n$. We see that $\theta(S) = n$ since we can take T to be the diagonal matrix with $n-1$ for the $1,1$ entry and -1 for all other diagonal entries. We also see that if $v = (e_1, \dots, e_n)$ is the standard basis for C^n then v is a clqiue for S and thus we have $\chi(S^\perp) = 1$. This shows that using the definition of the chromatic number from [HPP16] we can not hope to generalize the Lovász sandwich theorem.*

4.3 Non-commutative Lovász inequality

We see by the previous example that one needs a different generalization of the chromatic number in order to obtain a Lovász sandwich Theorem for non-commutative graphs. Here we introduce the strong and minimal chromatic number of a submatricial operator system and provide a generalization on Lovász theorem.

4.3.1 The Strong chromatic number

Let $\mathcal{J} \subset M_n$ be a submatricial traceless self-adjoint operator space. A collection of orthonormal vectors $v = (v_1, \dots, v_k)$ in $\mathbb{C}^n$ is called a *strong independent set for* $\mathcal{J}$ if for any i, j,we have $v_i v_j^*$ is orthogonal to $\mathcal{J}$. We say that $\mathcal{J}$ has a *strong k-colouring* if there exist an orthonormal basis $v = (v_1, \dots, v_n)$ of $\mathbb{C}^n$ that can be partitioned into k strong independent sets for $\mathcal{J}$. We will show in Corollary 4.3.6, $\widehat{\chi}(\mathcal{J}_G)$ agrees with the chromatic number of G, for any graph G.

Definition 4.3.1. Let $\mathcal{J} \subset M_n$ be a submatricial traceless self-adjoint operator space. The *strong chromatic number*, $\widehat{\chi}(\mathcal{J})$, is the least $k \in \mathbb{N}$ such that $\mathcal{J}$ has a strong k-colouring. If $\mathcal{J}$ has no strong-k colouring then we say $\widehat{\chi}(\mathcal{J}) = \infty$.

As with χ we have $\widehat{\chi}$ is monotonic with respect to inclusion.

Example 4. *Suppose that $S = \mathbb{C}1 + \operatorname{span}\{E_{i,j} : i \neq j\} \subset M_n$ and ζ is a nth root of unity. Define $v_k = (1, \zeta^k, \zeta^{2k}, \dots, \zeta^{(n-1)k})$. Observe that the v_i are orthogonal and that $v_k v_k^*$ belongs to S for all k. Thus $S^\perp$ does have a strong-n colouring and we get $\widehat{\chi}(S^\perp) \leq n$.*

Example 5. *Consider the submatricial traceless self-adjoint operator space $\mathcal{J} = \mathbb{C}\Delta \subset M_n$ where $\Delta = \operatorname{diag}(n-1, -1, -1, \dots, -1)$. Observe that $\mathcal{J} \subset S^\perp$. By monotonicity, $\widehat{\chi}(\mathcal{J}) \leq \widehat{\chi}(S^\perp) \leq n$. It is known that $\overline{\theta}(\mathcal{J}) = n$ (see [OP15, Remark 4.3]). We show in Theorem 4.3.7 that $\widehat{\chi}$ is bounded below by $\overline{\theta}$ Thus we have $\widehat{\chi}(\mathcal{J}) = \widehat{\chi}(S^\perp) = n$.*

In [Sta16] Stahlke introduces a different chromatic number for submatricial traceless self-adjoint operator spaces.

Definition 4.3.2. Let $\mathcal{J}$ and $\mathcal{K}$ be submatricial traceless self-adjoint operator spaces in M_n and M_m respectively. We say that there is a *graph homomorphism from $\mathcal{J}$ to $\mathcal{K}$*, denoted $\mathcal{J} \to \mathcal{K}$, if there is a cptp (completely positive and trace preserving) map $\mathcal{E} : M_n \to M_m$ with associated Kraus operators $E_1, \dots, E_r$ for which $E_i \mathcal{J} E_j^* \subset \mathcal{K}$ for any i and j.

Stalhke's chromatic number of a submatricial traceless self-adjoint operator space $\mathcal{J}$, denoted $\chi_{St}(\mathcal{J})$, is the least integer c for which there is a graph homomorphism $\mathcal{J} \to \mathcal{J}_{K_c}$ if one exists. We set $\chi_{St}(\mathcal{J}) = \infty$ otherwise.

Observe that χ_{St} is monotonic under graph homomorphism by construction.

Theorem 4.3.3. *For any submatricial traceless self-adjoint operator space $\mathcal{J} \subset M_n$ we have $\widehat{\chi}(\mathcal{J}) \geq \chi_{St}(\mathcal{J})$.*

Proof. Suppose $\widehat{\chi}(\mathcal{J}) = r$. There exists a orthonormal basis $v_1, \dots, v_n$ that can be partitioned into strong independent sets $P_1, \dots, P_r$. By reordering the vectors, we may assume that whenever $v_i \in P_\ell$ and $v_j \in P_{\ell+1}$, that $i < j$. By conjugating by the unitary $U : v_i \mapsto e_i$, we get the inclusion $\bigoplus_{i=1}^r M_{|P_i|} \subset U\mathcal{J}^\perp U^* = (U\mathcal{J}U^*)^\perp$.

This then gives us $(\bigoplus_{i=1}^r M_{|P_i|})^\perp \supset (U\mathcal{J}U^*)$. We have that $\mathcal{J} \to U\mathcal{J}U^*$ by conjugating by the unitary U. Similarly we have $U\mathcal{J}U^* \to (\oplus_{i=1}^r M_{|P_i|})^\perp$ by inclusion. Since χ_{St} is monotonic with respect to homomorphisms we get $\chi_{St}(\mathcal{J}) \leq \chi_{St}((\oplus_{i=1}^r M_{|P_i|})^\perp) = \chi(\overline{G}) = r$ where G is the disjoint union of r complete graphs. □

Corollary 4.3.4. *If $\mathcal{J} \subset M_n$ is a submatricial traceless self-adjoint operator space for which for some basis $v = (v_1, \dots, v_n)$, the diagonals $v_i v_i^*$ are orthogonal to $\mathcal{J}$, then $\chi_{St}(\mathcal{J}) \leq n$.*

In [LPT17] it was shown that $\alpha(S) = \alpha(M_d(S))$ for all submatricial operator systems S. The proof they give will also work to show $\alpha(\mathcal{J}) = \alpha(M_d(\mathcal{J}))$ and $\widehat{\chi}(\mathcal{J}) = \widehat{\chi}(M_d(\mathcal{J}))$ for submatricial traceless self-adjoint operator spaces $\mathcal{J}$ and $d \in \mathbb{N}$.

Recall that for $d, n \geq 1$, the partial trace map is

$$M_d \otimes M_n \to M_n : X \otimes Y \mapsto \operatorname{tr}(X)Y .$$

As is the case with χ we can approximate $\widehat{\chi}$ using the chromatic number for classical graphs.

Theorem 4.3.5. *Let $\mathcal{J} \subset M_n$ be a submatricial traceless self-adjoint operator space. Suppose that $\mathcal{B}_{\mathcal{J}}$ denotes the set of ordered orthonormal bases $v = (v_1, \dots, v_n)$ of $\mathbb{C}^n$ for which $v_i v_i^* \in \mathcal{J}$ for all i. For each*

$v = (v_1, \dots, v_n)$ in $\mathcal{B}_{\mathcal{J}}$, define the graph G_v with vertices $[n]$ and edge relation given by $i \sim j$ if $v_i v_j^*$ is orthogonal to $\mathcal{J}$. Then,

$$\widehat{\chi}(\mathcal{J}) = \inf_{v \in \mathcal{B}} \chi(\overline{G_v}) ,$$

whenever $\widehat{\chi}(\mathcal{J})$ is finite.

Proof. The proof is exactly as in Theorem 4.2.15. □

Corollary 4.3.6. *For any finite graph G, $\widehat{\chi}(\mathcal{J}_G) = \chi(G)$.*

Proof. By Theorem 4.3.5, $\widehat{\chi}(\mathcal{J}_G) \leq \chi(\overline{G_v})$ where $v = (e_1, \dots, e_n)$. The complement of the graph G_v is the graph G. This gets us the bound $\widehat{\chi}(\mathcal{J}_G) \leq \chi(G)$. As well, by Theorem 4.3.3, $\chi(G) = \chi_{St}(\mathcal{J}_G) \leq \widehat{\chi}(\mathcal{J}_G)$. □

Using the strong chromatic number we are easily able to generalize other graph inequalities that for now remain unanswered for χ_{St}. In [Sta16] Stahlke asks if for all submatricial traceless self-adjoint operator spaces $\mathcal{J} \subset M_n$, one can show $\chi_{St}(\mathcal{J})\omega(\mathcal{J}^c) \geq n$, where $\mathcal{J}^c$ is the proposed complement $\mathcal{J}^c = (\mathcal{J} + \mathbb{C}I)^{\perp}$. The question is motivated by the simple graph inequality $\chi(G)\omega(\overline{G}) \geq n$. Indeed for $\mathcal{J} \subset M_n$ a submatricial traceless self-adjoint operator space if we suppose $\widehat{\chi}(\mathcal{J}) = k$ then we can find an orthonormal basis $v = (v_1, \dots, v_n)$ and a partition of v into independent sets $P_1, \dots, P_k$. By definition of $\omega(\mathcal{J}^{\perp})$ we know that $|P_i| \leq \omega(\mathcal{J}^{\perp})$ for $i = 1, \dots, k$. Thus we have $n = \sum_i |P_i| \leq \sum_i \omega(\mathcal{J}^{\perp}) = \widehat{\chi}(\mathcal{J})\omega(\mathcal{J}^{\perp})$.

Using [Sta16], one can establish that $\overline{\theta}(\mathcal{J}) \leq \chi_{St}(\mathcal{J})$ for any submatricial traceless self-adjoint operator space $\mathcal{J} \subset M_n$: if $c = \chi_{St}(\mathcal{J})$, then there is a graph homomorphism $\mathcal{J} \to \mathcal{J}_{K_c}$. In [Sta16, Theorem 19], it is shown that $\overline{\theta}_n$ is monotonic under graph homomorphisms. We therefore get the inequality

$$\overline{\theta}_n(\mathcal{J}) \leq \overline{\theta}_n(\mathcal{J}_{K_c}) = \theta(\overline{K_c}) \leq \chi(K_c) = c .$$

We can now establish a Lovász sandwich Theorem for $\widehat{\chi}$.

Theorem 4.3.7. *Let S be a submatricial operator system. For any $d \geq 1$, we have the inequalities*

$$\alpha(S) \leq \theta(S) \leq \widehat{\chi}(S^{\perp}) .$$

Proof. The inequality $\alpha(S) \leq \theta(S)$ is a result in [DSW13, Lemma 7] so we will only prove the other inequality. Let $v = (v_1, \dots, v_n)$ be an orthonormal basis that can be partitioned into k strong independent sets for $S^{\perp}$. Then consider the graph $G_v(S^{\perp})$ as defined in Theorem 4.2.15. We have $\widehat{\chi}(S^{\perp}) = \chi(\overline{G_v})$. There exists a unitary $U \in M_n$ such that we get the the inclusion $S \supset US_{G_v}U^*$. Since θ is reverse monotonic under inclusion and invariant under conjugation by a unitary, we establish the inequalities

$$\theta(S) \leq \theta(S_{G_v}) = \theta(G_v) \leq \chi(\overline{G_v}) = \widehat{\chi}(S^{\perp}).$$

□

Similarly we get the follow inequality for any submatricial traceless self-adjoint operator space $\mathcal{J}$.

$$\alpha(\mathcal{J}^{\perp}) \leq \overline{\theta}(\mathcal{J}) \leq \widehat{\chi}(\mathcal{J}).$$

It should be pointed out that using $\chi_{St}(\mathcal{J}) \leq \widehat{\chi}(\mathcal{J})$, as shown in Theorem 4.3.3 , and the fact that $\omega(\mathcal{J}) = \alpha(\mathcal{J}^{\perp})$, one can obtain the the above inequality as a corollary of Corollary 20 in [Sta16] . In this sense the above can be considered as a simplified proof of a weaker result.

4.3.2 The minimal chromatic number

In this section, we wish to construct a concrete definition of a homomorphism monotone chromatic number.

Definition 4.3.8. Let $\mathcal{J} \subset M_n$ be a submatricial traceless self-adjoint operator space. Define the minimal chromatic number of $\mathcal{J}$, denoted $\chi_0(\mathcal{J})$, to be the least integer c for which there exists a basis $v_1, \ldots, v_n$ of $\mathbb{C}^n$ and a partition $P_1, \ldots, P_c$ of $[n]$ for which whenever $i, j \in P_s$, we have the relation $v_i v_j^* \perp \mathcal{J}$.

We note thatχ_0 differs from $\widehat{\chi}$ since we no longer require that we are working with an orthonormal basis. This parameter agrees with the chromatic number for graphs. We define the competely bounded version of this parameter by $\chi_{0,cb}(\mathcal{J}) = \inf_d \chi_0(M_d(\mathcal{J}))$.

Proposition 4.3.9. *Let G be a finite graph. We have the relation $\chi(G) = \chi_0(\mathcal{J}_G)$.*

Proof. Since $\chi_0(\mathcal{J}_G) \leq \chi(G)$, it suffices to show that $\chi(G) \leq \chi_0(\mathcal{J}_G)$. For this proof, let c be minimal and let $v_1, \ldots, v_n$ be a basis in $\mathbb{C}^n$ for which there is a partition $P_1, \ldots, P_c$ of $[n]$ such that whenever i, j in P_s, $v_i v_j^* \perp \mathcal{J}_G$. We then have a permutation σ of $[n]$ for which $\left\langle v_i, e_{\sigma(i)} \right\rangle$ is non-zero. By conjugating $\mathcal{J}_G$ by the permutation matrix defined by σ, assume that $\sigma(i) = i$ for all i. Define the c-colouring $f : V(G) \to [c]$ By $f(i) = s$ for s such that $i \in P_s$. To see that this is a colouring, suppose not. There are then $i \sim j$ for which $i, j \in P_s$ for some s. By definition then we have, $E_{i,j}$ belongs to $\mathcal{J}_G$. We observe then,

$$\left\langle v_i v_j^*, E_{i,j} \right\rangle = \operatorname{tr}(v_j v_i^* e_i e_j^*) = \langle v_i, e_i \rangle \left\langle v_j, e_j \right\rangle \neq 0 \; .$$

This is contradicts the fact that $v_i v_j^* \in \mathcal{J}^\perp$. □

We recall the following result, which arises as a consequence of the Stinespring dilation Theorem (see [Sta16, Definition 7]).

Lemma 4.3.10. *Let $\mathcal{J} \subset M_n$ and $\mathcal{K} \subset M_m$ be submatricial traceless self-adjoint operator spaces. There is a graph homomorphism $\mathcal{J} \to \mathcal{K}$ if and only if there is a $d \geq 1$ and an isometry $E : \mathbb{C}^n \to \mathbb{C}^m \otimes \mathbb{C}^d$ for which $E\mathcal{J}E^* \subset M_d(\mathcal{K})$.*

We use this equivalent characterization to show that $\chi_{0,cb}$ is monotonic under graph homomorphisms.

Theorem 4.3.11. *Let $\mathcal{J} \subset M_n$ and $\mathcal{K} \subset M_m$ be submatricial traceless self-adjoint operator spaces. If there is a graph homomorphism $\phi : \mathcal{J} \to \mathcal{K}$ with d associated Kraus operators, then we have the inequality*

$$\chi_0(\mathcal{J}) \leq \chi_0(M_d \otimes \mathcal{K}) \; .$$

In particular, $\chi_{0,cb}(\mathcal{J}) \leq \chi_{0,cb}(\mathcal{K})$.

Proof. Suppose that $P_1, \ldots, P_c$ is a partition of the set $[d] \times [m]$ and $(w_i : i \in [d] \times [m])$ is a basis for which whenever i, j are in the same P_s, then $w_i w_j^* \perp M_d \otimes \mathcal{K}$. By lemma 4.3.10, there is an isometry E for which the map $\phi : M_n \to M_d \otimes M_m : X \mapsto EXE^*$ sends $\mathcal{J}$ to $M_d \otimes \mathcal{K}$. Consider the set $\{E^* w_i : i \in [d \times m]\}$. This set spans $\mathbb{C}^n$. To see this, for any $v \in \mathbb{C}^n$, since $Ev \in \mathbb{C}^d \otimes \mathbb{C}^m$, there are some λ_i for which $Ev = \sum_i \lambda_i w_i$. Multiplying on the left by E^* tell us that v is spanned by the $E^* w_i$. If i, j belong to the same P_s, then for any $X \in \mathcal{J}$,

$$\left\langle E^* w_i (E^* w_j)^*, X \right\rangle = \left\langle w_i w_j^*, EXE^* \right\rangle = 0 \; .$$

For each $i \in [c]$, let $C_i = \{E^* w_j : j \in P_i\}$. We will define a sequence of linear subspaces $V_1, \ldots, V_c$ for which $\sum_{i=1}^{c} V_i = \mathbb{C}^n$ inductively. For the base case, set $V_1 = \operatorname{span} C_1$. For $i > 1$, let

$$V_i = \operatorname{span}\left\{ v \in \operatorname{span} C_i : v \notin \sum_{k<i} V_k \right\} .$$

By construction, for distinct i and j, the vectors the V_i are linearly independent in relation to the vectors of V_j and $\sum_i V_i = \mathbb{C}^n$. For each s, let $Q_s = \{v_{s,1}, \ldots, v_{s,d_s}\}$ be a basis in V_s, where $d_s = dim(V_s)$. Since each vector in Q_s is a linear combination of the vectors in C_s, we get that whenever, $i, j \in [d_s]$, given any $X \in \mathcal{J}$,

$$\left\langle v_{s,i} v_{s,j}^*, X \right\rangle = 0 .$$

The vectors $\{v_{s,i} : s \in [c], i \in [d_s]\}$ then form a basis for $\mathbb{C}^n$ and are partitioned by the sets $\{Q_s : s \in [c]\}$. This proves that $\chi_0(\mathcal{J}) \leq \chi_0(M_d \otimes \mathcal{K})$. If $r \geq 1$ and E is an isometry for which the map $\phi : M_n \to M_d \otimes M_m : X \mapsto EXE^*$ sends $\mathcal{J}$ to $M_d(\mathcal{K})$, then the map

$$1 \otimes \phi : M_r \otimes M_n \to M_{r+d} \otimes M_m : X \otimes Y \mapsto X \otimes \phi(Y)$$

is a map implemented by conjugation by the isometry $1 \otimes E$. By lemma 4.3.10, $1 \otimes E$ is a graph homomorphism $M_r(\mathcal{J}) \to M_r(\mathcal{K})$. By the above proof, we get the bound $\chi_0(M_r(\mathcal{J})) \leq \chi_0(M_{r+d}(\mathcal{K})) \leq \chi_{0,cb}(\mathcal{K})$ for every $r \geq 1$. This establishes the inequality

$$\chi_{0,cb}(\mathcal{J}) \leq \chi_{0,cb}(\mathcal{K}) .$$

□

Corollary 4.3.12. *Let $\mathcal{J}$ be a submatricial traceless self-adjoint operator space. We have the inequality*

$$\chi_{0,cb}(\mathcal{J}) \leq \chi_{St}(\mathcal{J}) .$$

Proof. We first show that $\chi_{0,d}(\mathcal{J}_G) = \chi(\mathcal{J}_G)$ for any $d \geq 1$ and any graph G. Let $G^{[d]}$ denote the graph on vertices $V(G) \times [d]$ for which $(v, i) \sim (w, j)$ if $v \sim w$ in G. The projection $G^{[d]} \to G : (v, i) \mapsto v$ and the inclusion $G \to G^{[d]} : v \mapsto (v, 1)$ are graph homomorphisms. We therefore get by monotonicity of χ that $\chi(G) = \chi(G^{[d]})$. On the other hand, we know that $\chi_0(\mathcal{J}_G) = \chi(G) = \chi(G^{[d]}) = \chi_0(M_d(\mathcal{J}_G)) = \chi_{0,d}(\mathcal{J}_G)$. In particular, for any $c \geq 1$, $\chi_{0,cb}(\mathcal{J}_{K_c}) = \chi(K_c) = c$. □

Remark 6. *We were unable to determine if $\chi_{0,cb} = \chi_0$. Never the less the obtain value by working with $\chi_{0,cb}$ since we know it is a homomorphism monotone parameter.*

4.4 Sabidussi's Theorem and Hedetniemi's conjecture

As an application of our new graph parameters, in this section, we generalize two results for chromatic numbers on graph products. For convenience we will let $\overline{\chi}(X) = \widehat{\chi}(X^{\perp})$ for X a submatricial traceless self-adjoint operator space or a submatricial operator system.

Definition 4.4.1. Let G and H be finite graphs.

1. Define the categorical product of G and H to be the graph $G \times H$ with vertex set $V(G) \times V(H)$ and edge relation given by $(v, a) \sim (w, b)$ if $v \sim_G w$ and $a \sim_H b$.
2. Define the Cartesian product of G and H to be the graph $G \square H$ with vertex set $V(G) \times V(H)$ and edge relation given by $(v, a) \sim (w, b)$ if one of the following holds
   (a) $v \sim_G w$ and $a = b$ or
   (b) $v = w$ and $a \sim_H b$.

4.4.1 Sabidussi's theorem

We generalize the Theorem of Sabidussi [Sab57].

Theorem 4.4.2 (Sabidussi). *Let G and H be finite graphs. We have the identity*

$$\chi(G\square H) = \max\{\chi(G), \chi(H)\} .$$

The first step in generalizing this Theorem is to generalize the cartesian product.

Definition 4.4.3. Let $\mathcal{J} \subset M_n$ and let $\mathcal{K} \subset M_m$ be submatricial traceless self-adjoint operator spaces. Let $v \subset \mathbb{C}^n$ and $w \subset \mathbb{C}^m$ be bases. Define the cartesian produt of $\mathcal{J}$ and $\mathcal{K}$ relative to (v, w) as the submatricial traceless self-adjoint operator space

$$(\mathcal{J}\square\mathcal{K})_{v,w} = \mathcal{J} \otimes \mathcal{D}_w + \mathcal{D}_v \otimes \mathcal{K}$$

where for a basis $x = (x_1, \dots, x_n)$, $\mathcal{D}_x = \operatorname{span}\{x_i x_i^* : i \in [n]\}$.

In the case when $e = (e_1, \dots, e_n)$ and $f = (e_1, \dots, e_m)$, we define the cartesian product $\mathcal{J}\square\mathcal{K}$ to be $(\mathcal{J}\square\mathcal{K})_{e,f}$.

Lemma 4.4.4. *Let G and H be finite graphs with $[n] = V(G)$ and $[m] = V(H)$. We have the identity $\mathcal{J}_G\square\mathcal{J}_H = \mathcal{J}_{G\square H}$.*

Proof. Observe that $\mathcal{J}_G \otimes \mathcal{D}_m = \operatorname{span}\{E_{v,w} \otimes E_{i,i} : v \sim_G w, i \in [m]\}$ and that $\mathcal{D}_n \otimes \mathcal{J}_H = \operatorname{span}\{E_{i,i} \otimes E_{v,w} : i \in [n], v \sim_H w\}$. Combining these, we get that $E_{i,j} \otimes E_{k,l} \in \mathcal{J}_G\square\mathcal{J}_H$ if and only if $i \sim_G j$ and $k = l$ or $i = j$ and $k \sim_H l$. This is exactly what it means to be a member of $\mathcal{J}_{G\square H}$. □

Lemma 4.4.5. *Suppose that $\mathcal{J} \subset M_n$ and $\mathcal{K} \subset M_m$ are submatricial traceless self-adjoint operator spaces. Suppose $v \subset \mathbb{C}^n$ and $w \subset \mathbb{C}^m$ are bases. There exist graph homomorphisms $\mathcal{J} \to \mathcal{J} \otimes \mathcal{D}_w$ and $\mathcal{K} \to \mathcal{D}_v \otimes \mathcal{K}$. In particular, there exist graph homomorphisms $\mathcal{J} \to (\mathcal{J}\square\mathcal{K})_{v,w}$ and $\mathcal{K} \to (\mathcal{J}\square\mathcal{K})_{v,w}$.*

Proof. Define $\phi : M_n \to M_n \otimes M_m : X \mapsto \frac{1}{\|w_1\|^2} X \otimes w_1 w_1^*$. This map has Kraus operator $E : \mathbb{C}^n \to \mathbb{C}^n \otimes \mathbb{C}^m : v \mapsto v \otimes w_1/\|w_1\|$. Since this Kraus operator is an isometry, we know that ϕ is cptp. As well, $\phi(\mathcal{J}) = \mathcal{J} \otimes w_1 w_1^* \subset \mathcal{J} \otimes \mathcal{D}_w$. Similarly, $\mathcal{K} \to \mathcal{D}_v \otimes \mathcal{K}$. Since $\mathcal{J} \otimes \mathcal{D}_w \subset (\mathcal{J}\square\mathcal{K})_{v,w}$ and $\mathcal{D}_v \otimes \mathcal{K} \subset (\mathcal{J}\square\mathcal{K})_{v,w}$, we conclude that $\mathcal{J} \to (\mathcal{J}\square\mathcal{K})_{v,w}$ and $\mathcal{K} \to (\mathcal{J}\square\mathcal{K})_{v,w}$. □

Theorem 4.4.6. *Let $\mathcal{J} \subset M_n$ and $\mathcal{K} \subset M_m$ be submatricial traceless self-adjoint operator spaces. Let $v \subset \mathbb{C}^n$ and $w \subset \mathbb{C}^m$ be bases. We have the inequality*

$$\max\{\chi_{0,cb}(\mathcal{J}), \chi_{0,cb}(\mathcal{K})\} \leq \chi_{0,cb}((\mathcal{J}\square\mathcal{K})_{v,w}) .$$

Proof. By lemma 4.4.5 and by Theorem 4.3.11, we get the inequalities $\chi_{0,cb}(\mathcal{J}) \leq \chi_{0,cb}((\mathcal{J}\square\mathcal{K})_{v,w})$ and $\chi_{0,cb}(\mathcal{K}) \leq \chi_{0,cb}((\mathcal{J}\square\mathcal{K})_{v,w})$. □

The reverse inequality seems to require the existence of orthogonal bases which colour our submatricial traceless self-adjoint operator spaces. The proof mimicks the proof of Sabidussi's Theorem in [GR16].

Theorem 4.4.7. *Let $\mathcal{J} \subset M_n$ and $\mathcal{K} \subset M_m$ be submatricial traceless self-adjoint operator spaces. Let $c = \max\{\chi_0(\mathcal{J}), \chi_0(\mathcal{K})\}$. Suppose that orthonormal bases $v \subset \mathbb{C}^n$ and $w \subset \mathbb{C}^m$ exist for which we have maps $f : [n] \to [c]$ and $g : [m] \to [c]$ for which whenever $f(i) = f(j)$, $v_{f(i)} v_{f(j)}^* \perp \mathcal{J}$ and whenever $g(l) = g(k)$, we have $w_{g(l)} w_{g(k)}^* \perp \mathcal{K}$. We have the inequality*

$$\chi_0((\mathcal{J}\square\mathcal{K})_{v,w}) \leq \max\{\chi_0(\mathcal{J}), \chi_0(\mathcal{K})\} .$$

Proof. Let $c = \max\{\chi_0(\mathcal{J}), \chi_0(\mathcal{K})\}$. Suppose that v, w, f, and g are as above. Define $h : [n] \times [m] \to [c] : (i,j) \mapsto f(i) + g(j) \mod c$. I claim that whenever $h(i,j) = h(k,l)$, that $(v_i \otimes w_j)(v_k \otimes w_l)^*$ is orthogonal to $(\mathcal{J}\square\mathcal{K})_{v,w}$. The identity $h(i,j) = h(k,l)$ tell us $f(i) - f(k) \equiv g(j) - g(l) \mod c$. If $f(i) - f(k) \equiv 0 \mod c$ then we have nothing to check since this means that $f(i) = f(k)$ and $g(j) = g(l)$. Otherwise, $v_i v_k^* \perp v_s v_s^*$ for all s and $w_j w_l^* \perp w_s w_s^*$ for all s. This guarantees that $v_i v_k^* \otimes w_j w_l^*$ is orthogonal to $(\mathcal{J}\square\mathcal{K})_{v,w}$. □

Remark 7. *The same proof as above will show us that for some orthonormal bases v and w,*

$$\chi((\mathcal{J}\square\mathcal{K})_{v,w}) \leq \max\{\chi(\mathcal{J}), \chi(\mathcal{K})\} \text{ and}$$
$$\overline{\chi}((\mathcal{J}\square\mathcal{K})_{v,w}^{\perp}) \leq \max\{\overline{\chi}(\mathcal{J}^{\perp}), \overline{\chi}(\mathcal{K}^{\perp})\} .$$

We are now ready to state a generalized version of Sabidussi's theorem. In the following statement please recall that $\overline{\chi}(X) = \widehat{\chi}(X^{\perp})$.

Corollary 4.4.8 (Sabidussi's Theorem for submatricial traceless self-adjoint operator spaces)**.** *Suppose that $\mathcal{J} \subset M_n$ and $\mathcal{K} \subset M_m$ are submatricial traceless self-adjoint operator spaces. There exist orthonormal bases $v \subset \mathbb{C}^n$ and $w \subset \mathbb{C}^m$ for which we have the inequalities*

$$\max\{\chi_{0,cb}(\mathcal{J}), \chi_{0,cb}(\mathcal{K})\} \leq \chi_{0,cb}((\mathcal{J}\square\mathcal{K})_{v,w}) \leq \overline{\chi}((\mathcal{J}\square\mathcal{K})_{v,w}^{\perp}) \leq \max\{\overline{\chi}(\mathcal{J}^{\perp}), \overline{\chi}(\mathcal{K}^{\perp})\} .$$

Proof. By Remark 7, we get the inequality

$$\overline{\chi}((\mathcal{J}\square\mathcal{K})_{v,w}^{\perp}) \leq \max\{\overline{\chi}(\mathcal{J}^{\perp}), \overline{\chi}(\mathcal{K}^{\perp})\} .$$

By Theorem 4.3.3 and Corollary 4.3.12, we get the inequality

$$\chi_{0,cb}((\mathcal{J}\square\mathcal{K})_{v,w}) \leq \chi_{st}((\mathcal{J}\square\mathcal{K})_{v,w}) \leq \overline{\chi}((\mathcal{J}\square\mathcal{K})_{v,w}^{\perp}) .$$

Finally, by Theorem 4.4.6 we get the final inequality. □

4.4.2 Hedetniemi's inequality

The inequality we wish to generalize in this section is a Theorem of Hedetniemi.

Theorem 4.4.9 (Hedetniemi's inequality)**.** *Suppose that G and H are finite graphs. We have the inequality*

$$\chi(G \times H) \leq \min\{\chi(G), \chi(H)\}$$

This Theorem follows as a special case of the analogous result for $\chi_{0,cb}$, first we generalize the categorical product.

Proposition 4.4.10. *Let G and H be finite graphs. We have the identity*

$$\mathcal{J}_G \otimes \mathcal{J}_H = \mathcal{J}_{G\times H} .$$

Proof. Observe that

$$\begin{aligned}\mathcal{J}_G \otimes \mathcal{J}_H &= \operatorname{span}\{E_{i,j} \otimes E_{k,l} : i \sim_G j, k \sim_H l\} \\ &= \mathcal{J}_{G\times H} .\end{aligned}$$

□

We now get a generalization of Hedetniemi's inequality to $\chi_{0,cb}$.

Proposition 4.4.11. *Suppose that $\mathcal{J} \subset M_n$ and $\mathcal{K} \subset M_m$ are submatricial traceless self-adjoint operator spaces. We have the inequality*

$$\chi_{0,cb}(\mathcal{J} \otimes \mathcal{K}) \leq \min\{\chi_{0,cb}(\mathcal{J}), \chi_{0,cb}(\mathcal{K})\} .$$

Proof. The partial trace maps produce graph homomorphisms $\mathcal{J} \otimes \mathcal{K} \to \mathcal{K}$ and $\mathcal{J} \otimes \mathcal{K} \to \mathcal{J}$. By Theorem 4.3.11, we get the inequality. □

Remark 8. *The long standing conjecture of Hedetneimi asked whether we get the identity*

$$\chi(G \times H) = \min\{\chi(G), \chi(H)\}$$

for any finite graphs G and H. This was recently resolved in the negative by the remarkable work of Yaroslov Shitov [Shi19].

Chapter 5

Non-local Games

5.1 Introduction

In 1964, Bell showed that local hidden-variable theories, which are classical in nature, cannot explain all quantum mechanical phenomena [Bel64]. 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 [MY04]. Self-testing has wide reaching applications in areas of theoretical computer science including complexity theory [NV18, FJVY19, NW19], certifiable randomness [VV12], device independent quantum cryptography [ABG$^+$07, VV14], and delegated quantum computation [CGJV19a]. See [SB19] 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 [CHSH69] 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 [CHTW04].

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 [SW87, Tsi93] 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. The simple formulation of non-local games make them more straightforward to implement experimentally and to use in complexity theoretic applications. For example, multiprover interactive proofs and their associated complexity classes, e.g., MIP, MIP* are built on top of non-local games.

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 $\mathbb{Z}_2$ [CM12]. 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 5.1.1. *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 [Mer90] 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 [CN16].

The sum of squares (SOS) decomposition technique in [BP15] 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 [CGS17]. 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 [CM12].

Question 5.1.2. *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 [MYS12].

Self-tests for measurements in higher dimensions have been primarily focused on self-testing n-fold tensor-products of σ_X and σ_Z [NV17, Col16, Mck16]. 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 [CGJV19b]. Our games provides another example that is neither Pauli nor Clifford. Since our games are LCS this resolves the question, first posed by [CS18], in the affirmative.

Question 5.1.3. *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 [CLS17] 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 [CS18] 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 [GH17, Vid18] from approximate representation theory.

Question 5.1.4. *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 [Slo19], 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 5.1.5. *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. To the best of our knowledge, this *glued magic square* provides the first example of a game that is not a self-test [Mer90].

5.1.1 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 5.4, we give a lower-bound on the *quantum value* of this family of games. Specifically in Theorem 5.4.9, 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 [NPA08]. 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 5.6, 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 5.1.4.

In section 5.7, 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 5.1.1. This game also answers Question 5.1.2 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 **??**, we introduce the sum of squares framework, using an important lemma proven in Section 5.2.4, that gives a streamlined method for proving self-testing. We then use this framework to prove self-testing for our games. Furthermore, in Section 5.8, we show that when restricted to pseudo-telepathic games, the SOS framework reduces to the solution group formalism of Cleve, Liu, and Slofstra [CLS17].

In section 5.9, we construct an LCS game that is obtained from "gluing" two copies of the magic square game together. This game is summarized in Figure 5.1.1. We exhibit two inequivalent perfect strategies and thus provide an answer to Question 5.1.5.

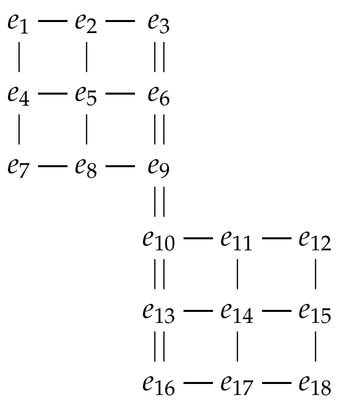

Figure 5.1: This describes an LCS game with 18 variables $e_1, e_2, \ldots, e_{18}$. Each single-line indicates that the variables along the line multiply to 1, and the double-line indicates that the variables along the line multiply to -1.

5.1.2 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 5.2.4 that encapsulates the use of GH in proving self-testing. In Section 5.2.4, we define approximate representations, irreducible strategies, the Gowers-Hatami theorem and present the proof of the following lemma.

Lemma (informal)**.** *Let G_A, G_B be groups. Suppose every optimal strategy of the game $\mathcal{G}$ induces a pair of approximate representations of G_A and G_B. Further suppose that there is a unique optimal irreducible strategy $(\rho, \sigma, |\psi\rangle)$ where ρ, σ are irreps of G_A, G_B, respectively. Then $\mathcal{G}$ is a self-test.*

Applying this lemma requires us to ascertain two properties of the game:

1. Every optimal strategy induces approximate representations of some groups G_A and G_B.
2. There is a unique irreducible strategy $(\rho, \sigma, |\psi\rangle)$ for the game $\mathcal{G}$.

The first step is to obtain the bias expression for the game $\mathcal{G}$ that allows for a simple calculation of the wining probability of any startegy $\mathcal{S} = (\{A_i\}, \{B_j\}, |\psi\rangle)$ (here A_i and B_j are Alice and Bob's measurement observables, respectively, and $|\psi\rangle$ is the shared state). The bias expression for $\mathcal{G}_n$ is given by

$$\mathcal{B}_n(A_0, A_1, B_0, B_1) = \sum_{i=1}^{n-1} A_0^i B_0^{-i} + A_0^i B_1^i + A_1^i B_0^{-i} + \omega^{-i} A_1^i B_1^i.$$

Then the winning probability of $\mathcal{S}$ is given by $\nu(\mathcal{G}, \mathcal{S}) = \langle \psi | (\frac{1}{4n} \mathcal{B}_n(A_0, A_1, B_0, B_1) + \frac{1}{n}) | \psi \rangle$. For any real λ for which there exist some polynomials T_k giving a sum of squares decomposition such as

$$\lambda I - \mathcal{B}_n(A_0, A_1, B_0, B_1) = \sum_k T_k^*(A_0, A_1, B_0, B_1) T_k(A_0, A_1, B_0, B_1),$$

provides an upper bound of $\frac{\lambda}{4n} + \frac{1}{n}$ on the optimal value of the game (which we denote by $\nu^*(\mathcal{G}_n)$). This follows since expressing $\lambda I - \mathcal{B}_n$ as an SOS proves that it is a positive semidefinite operator and consequently $\langle \psi | \mathcal{B}_n | \psi \rangle \leq \lambda$ for all states $|\psi\rangle$.

Now if we have an SOS for $\lambda = 4nv^*(\mathcal{G}) - 4$, 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.

5.1.3 Relation to prior generalizations of CHSH

Much work has been done to generalize CHSH to games over $\mathbb{Z}_n$. Initial generalizations were done by Bavarian and Shor [BS15] and later extended in Kaniewski et al. [KvT$^+$18]. The game we present in section 5.3 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.

5.1.4 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 5.6, 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

$$G_3 \cong \mathbb{Z}_3 \times A_4, G_4 \cong (\mathbb{Z}_2^3 \rtimes \mathbb{Z}_4) \rtimes \mathbb{Z}_4, G_5 \cong (\mathbb{Z}_2^4 \rtimes \mathbb{Z}_5) \times \mathbb{Z}_5,$$

$$G_6 \cong \mathbb{Z}_3 \times \left((((\mathbb{Z}_4 \times \mathbb{Z}_2^3) \rtimes \mathbb{Z}_2) \rtimes \mathbb{Z}_2) \rtimes \mathbb{Z}_3\right).$$

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 5.1.4.

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

   $$x_0 x_1 = g_1$$
   $$x_0 x_1 = g_2.$$

   Understanding the map that sends (G, g_1, g_2) to the self-tested group helps us develop a richer landscape of group self-testing.

5. How far can the SOS framework be pushed to prove self-testing? The first step in answering this question is perhaps a characterization of games (G, g_1, g_2) (and their variants, e.g., system of equations with more variables and equations) using this framework.

6. Glued magic square, as presented in Section 5.9, 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 be the first

example of a non-local game that only self-tests the state and not the measurement operators. This positively resolves a question asked in [SB19] in the context of non-local games.

Most self-testing results rely on first attaining self-testing for measurement operators. So innovative techniques are needed to prove a state self-testing result for the glued magic square game.

5.1.5 Organization of paper

In section 5.2, 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 5.3, 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 5.4, 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 5.6, we give a presentation for the groups generated by Alice and Bob's observables. In Section **??**, we present the SOS framework and give a basic example of its application in proving self-testing. In section 5.7, 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 5.8, we show that the SOS framework reduces to the solution group formalism in the case of pseudo-telepathic LCS games. Finally, in Section 5.9 we provide an example of a non-rigid game.

Acknowledgements

We would like to thank Henry Yuen for having asked many of the motivating questions for this project, as well as many insightful discussions and helpful notes on writing this paper. We also thank the reviewers from QIP for their suggestions and for suggesting the name glued magic square.

5.2 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 [Wat18, CN10, HPP16].

5.2.1 Notation

We use G to refer to a group, while $\mathcal{G}$ is reserved for a non-local game. Let $[n, m]$ denote the set $\{n, n+1, \ldots, m\}$ for integers $n \leq m$, and the shorthand $[n] = [0, n-1]$. This should not be confused with $[X, Y]$, which is used to denote the commutator $XY - YX$. We let I_n denote the $n \times n$ identity matrix and e_i, for $i \in [n]$, be the ith standard basis vector. The pauli observables are denoted σ_x, σ_y, and σ_z. The Kronecker delta is denoted by $\delta_{i,j}$.

We will let $\mathcal{H}$ denote a finite dimensional Hilbert space and use the notation $|\psi\rangle \in \mathcal{H}$ to refer to vectors in $\mathcal{H}$. We use $\mathrm{L}(\mathcal{H})$ to denote the set of linear operators in the Hilbert space $\mathcal{H}$. We use $\mathrm{U}_n(\mathbb{C})$ to denote the set of unitary operators acting on the Hilbert space $\mathbb{C}^n$. The set of projection operators acting on $\mathcal{H}$ are denoted by $\mathrm{Proj}(\mathcal{H})$. Given a linear operator $A \in \mathrm{L}(\mathcal{H})$, we let $A^* \in \mathrm{L}(\mathcal{H})$ denote the adjoint operator. For $X, Y \in \mathrm{L}(\mathcal{H})$, the Hilber-Schmidt inner product is given by $\langle X, Y\rangle = \mathrm{Tr}(X^* Y)$. We also use the following shorthands $\mathrm{Tr}_\rho(X) = \mathrm{Tr}(X\rho)$ and $\langle X, Y\rangle_\rho = \mathrm{Tr}_\rho(X^* Y)$

where $X, Y \in \mathrm{L}(\mathcal{H})$ and ρ is a density operator acting on $\mathcal{H}$ (i.e., positive semidefinite with trace 1). The von Neumann entropy of a density matrix ρ is given by $S(\rho) = -\operatorname{Tr}(\rho \log \rho)$.

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 $|\psi\rangle = U_A \otimes U_B |\Phi_n\rangle$.

5.2.2 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 5.2.1. 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 $\{E_{i,a}\}_{a \in \mathcal{O}_A} \subset \operatorname{Proj}(\mathcal{H}_A)$ and $\{F_{j,b}\}_{b \in \mathcal{O}_B} \subset \operatorname{Proj}(\mathcal{H}_B)$ 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 $\{E_{i,a}\}_{a\in\mathcal{O}_A}$ and $\{F_{j,b}\}_{b\in\mathcal{O}_B}$. 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 [CHSH69] is the tuple $(\mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B, \pi, V)$ where $\mathcal{I}_A = \mathcal{I}_B = \mathcal{O}_A = \mathcal{O}_B = \{0, 1\}$, 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 $\frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.85$ [CHSH69].

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 $\delta : \mathbb{R}^+ \to \mathbb{R}^+$ 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 **??**, we give as an example the proof of exact rigidity of the CHSH game.

5.2.3 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* [CM12].

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 [CLS17, CS18]. 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 5.7. When restriced to psuedo-telepathic LCS games, our SOS approach is identical to the solution group formalism. We present this in section 5.8 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. $\prod_{j\in V_i} g_j^{A_{ij}} = J^{b_i}$.

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

In order to precisely state our results about self-testing in Section 5.7, we recall the Gowers-Hatami theorem and $(\varepsilon, |\psi\rangle)$-representation [GH17, CS18, Vid18].

Definition 5.2.2. Let G be a finite group, n an integer, Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ of dimension n, and $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ a state with the reduced density matrix $\sigma \in \mathrm{L}(\mathcal{H}_A)$. An $(\varepsilon, |\psi\rangle)$-representation of G, for $\varepsilon \geq 0$, is a function $f : G \to U_n(\mathbb{C})$ such that

$$\mathbb{E}_{x,y}\Re\left(\langle f(x)^* f(y), f(x^{-1}y)\rangle_\sigma\right) \geq 1 - \varepsilon. \tag{5.2.1}$$

In the case of $\varepsilon = 0$, we abbreviate and call such a map a $|\psi\rangle$-representation, in which case the condition 5.2.1 simplifies to

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

or equivalently

$$f(y)^* f(x) f(x^{-1}y)|\psi\rangle = |\psi\rangle, \tag{5.2.2}$$

for all $x, y \in G$. In Condition (5.2.2), 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 (5.2.2) 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

$$f(x)f(y)|\psi\rangle = f(xy)|\psi\rangle \text{ for all } x, y \in G. \tag{5.2.3}$$

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 (5.2.3), 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 [Vid18]. 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 5.2.3 (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 [Vid18], 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 5.2.4 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 5.2.2. 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 5.2.4. *Suppose that there is only one pair of irreps $\widehat{\rho}, \widehat{\sigma}$ for which $\nu(\mathcal{G}, \widehat{\rho}, \widehat{\sigma}) = \nu^*(\mathcal{G})$. Additionally assume that $|\psi\rangle$ is the unique state (up to global phase) for which $\mathcal{S}_{\widehat{\rho},\widehat{\sigma},|\psi\rangle}$ 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 $|\widetilde{\psi}\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$, $f_A^{\widetilde{\mathcal{S}}}$ and $f_B^{\widetilde{\mathcal{S}}}$ 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*

$$V_A \otimes V_B|\widetilde{\psi}\rangle = |junk\rangle|\psi\rangle,$$
$$V_A \widetilde{A}_i \otimes V_B|\widetilde{\psi}\rangle = |junk\rangle \widehat{\rho}(P_i) \otimes I_{d_{\widehat{\sigma}}}|\psi\rangle,$$
$$V_A \otimes V_B \widetilde{B}_j|\widetilde{\psi}\rangle = |junk\rangle I_{d_{\widehat{\rho}}} \otimes \widehat{\sigma}(Q_j)|\psi\rangle,$$

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 $|\mathcal{O}_A| = |\mathcal{O}_B| = 2$. 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 $\mathcal{S} = (\{A_i\}, \{B_j\}, |\psi\rangle)$

$$\nu(\mathcal{G}, \mathcal{S}) = \langle\psi| \left(\sum_{i \in I_A, j \in I_B} \lambda_{ij} A_i \otimes B_j + \sum_{i \in I_A} \lambda_i A_i \otimes I + \sum_{j \in I_B} \lambda_j I \otimes B_j + \lambda I \otimes I \right) |\psi\rangle. \tag{5.2.4}$$

As argued earlier, by GH, we have

$$f_A^{\widetilde{\mathcal{S}}}(x) \otimes I|\widetilde{\psi}\rangle = V_A^* g_A(x) V_A \otimes I|\widetilde{\psi}\rangle, \tag{5.2.5}$$
$$I \otimes f_B^{\widetilde{\mathcal{S}}}(x)|\widetilde{\psi}\rangle = I \otimes V_B^* g_B(x) V_B|\widetilde{\psi}\rangle, \tag{5.2.6}$$

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 5.2.3, $V_{A,\rho}$ 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 (5.2.4), 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 $(\rho, \sigma) = (\widehat{\rho}, \widehat{\sigma})$. Now since $\widetilde{\mathcal{S}}$ is an optimal strategy, we have

$$p_{\rho,\sigma} = \begin{cases} 1 & (\rho, \sigma) = (\widehat{\rho}, \widehat{\sigma}), \\ 0 & \text{otherwise.} \end{cases}$$

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 $\mathcal{S}_{I\otimes\widehat{\rho}, I\otimes\widehat{\sigma}, |\widetilde{\psi}_{\widehat{\rho},\widehat{\sigma}}\rangle}$ is an optimal strategy. From the assumption of the lemma ,$|\psi\rangle$ is the unique state optimizing the strategy induced by $(\widehat{\rho}, \widehat{\sigma})$. Therefore $|\widetilde{\psi}_{\widehat{\rho},\widehat{\sigma}}\rangle = |\text{junk}'\rangle|\psi\rangle$ 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

$$|\widetilde{\psi}_{\rho,\sigma}\rangle = \begin{cases} |\text{junk}'\rangle|\psi\rangle & (\rho, \sigma) = (\widehat{\rho}, \widehat{\sigma}), \\ 0 & \text{otherwise.} \end{cases} \tag{5.2.7}$$

Now using (5.2.5), 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

$$\begin{aligned} V_A \widetilde{A}_i \otimes V_B |\widetilde{\psi}\rangle &= g_A(P_i) V_A \otimes V_B |\widetilde{\psi}\rangle \\ &= \bigoplus_{\rho,\sigma} (I_{d_A d_\rho} \otimes \rho(P_i)) \otimes I_{d_B d_\sigma^2} |\widetilde{\psi}_{\rho,\sigma}\rangle \\ &= \left(|\mathrm{junk}'\rangle \widehat{\rho}(P_i) \otimes I_{d_{\widehat{\sigma}}} |\psi\rangle\right) \oplus_{(\rho,\sigma)\neq(\widehat{\rho},\widehat{\sigma})} 0_{d_A d_\rho^2 d_B d_\sigma^2} \\ &= |\mathrm{junk}\rangle \widehat{\rho}(P_i) \otimes I_{d_{\widehat{\sigma}}} |\psi\rangle, \end{aligned}$$

where the third equality follows from (5.2.7), and in the fourth equality $|\mathrm{junk}\rangle = |\mathrm{junk}'\rangle \oplus 0$ where $0 \in \mathbb{C}^{d_A d_B (\frac{|G_A||G_B|}{d_{\widehat{\rho}} d_{\widehat{\sigma}}} - d_{\widehat{\rho}} d_{\widehat{\sigma}})}$. Note that $d_A d_B (\frac{|G_A||G_B|}{d_{\widehat{\rho}} d_{\widehat{\sigma}}} - d_{\widehat{\rho}} d_{\widehat{\sigma}})$ is a positive integer because the degree of an irreducible representation divides the order of the group. □

Corollary 5.2.5. *If in addition to the assumptions of Lemma 5.2.4, 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 $\mathcal{S}_{\widehat{\rho},\widehat{\sigma},|\psi\rangle}$.*

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 5.2.5 as seen in Sections **??** and 5.7.

5.3 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

$$\begin{aligned} x_0 x_1 &= 1, \\ x_0 x_1 &= -1. \end{aligned}$$

The CHSH viewed as an LCS is first considered in [CM12]. We generalize this to a game $\mathcal{G}_n$ over $\mathbb{Z}_n$ for each $n \geq 2$

$$\begin{aligned} x_0 x_1 &= 1, \\ x_0 x_1 &= \omega_n. \end{aligned}$$

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 5.4, 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 5.6, we present the group G_n generated by the operators in $\mathcal{S}_n$. In Section 5.7, we show that $\mathcal{G}_3$ is a self-test, and conjecture that this is true for all $n \geq 2$.

As defined in the preliminaries, conventionally, in an LCS game, Alice has to respond with an assignment to all variables in her equation. It is in Alice's best interest to always respond with a satisfying assignment. Therefore, the referee could always determine Alice's assignment to x_1 from her assignment to x_0. Hence, without loss of generality, in our games, Alice only responds with an assignment to x_0.

Formally $\mathcal{G}_n = ([2], [2], \mathbb{Z}_n, \mathbb{Z}_n, \pi, V)$ where $\mathbb{Z}_n = \{1, \omega_n, \ldots, \omega_n^{n-1}\}$, π is the uniform distribution on $[2] \times [2]$, and

$$\begin{aligned} V(0,0,a,b) = 1 &\iff a = b, \\ V(0,1,a,b) = 1 &\iff ab = 1, \\ V(1,0,a,b) = 1 &\iff a = b, \\ V(1,1,a,b) = 1 &\iff ab = \omega_n. \end{aligned}$$

Consider the quantum strategy $\mathcal{S}$ given by the state $|\psi\rangle$, and projective measurements $\{E_{0,a}\}_{a\in[n]}$ and $\{E_{1,a}\}_{a\in[n]}$ for Alice, and $\{F_{0,b}\}_{b\in[n]}$ and $\{F_{1,b}\}_{b\in[n]}$ for Bob. Note that in our measurement systems, we identify outcome $a \in [n]$ with answer $\omega_n^a \in \mathbb{Z}_n$. As done in the preliminaries, define the generalized observables $A_0 = \sum_{i=0}^{n-1} \omega_n^i E_{0,i}$, $A_1 = \sum_{i=0}^{n-1} \omega_n^i E_{1,i}$, $B_0 = \sum_{i=0}^{n-1} \omega_n^i F_{0,i}$, $B_1 = \sum_{i=0}^{n-1} \omega_n^i F_{1,i}$. We derive an expression for the winning probability of this strategy in terms of the these generalized observables. We do so by introducing the bias operator

$$\mathcal{B}_n = \mathcal{B}_n(A_0, A_1, B_0, B_1) = \sum_{i=1}^{n-1} A_0^i B_0^{-i} + A_0^i B_1^i + A_1^i B_0^{-i} + \omega_n^{-i} A_1^i B_1^i,$$

in which we dropped the tensor product symbol between Alice and Bob's operators.

Proposition 5.3.1. *Given the strategy $\mathcal{S}$ above, it holds that $\nu\left(\mathcal{G}_n, \mathcal{S}\right) = \frac{1}{4n}\langle\psi|\mathcal{B}_n|\psi\rangle + \frac{1}{n}$.*

Proof.

$$\begin{aligned} \mathcal{B}_n + 4I &= \sum_{i=0}^{n-1} A_0^i B_0^{-i} + A_0^i B_1^i + A_1^i B_0^{-i} + \omega_n^{-i} A_1^i B_1^i \\ &= \sum_{i=0}^{n-1} \sum_{a,b=0}^{n-1} \omega_n^{i(a-b)} E_{0,a} F_{0,b} + \omega_n^{i(a+b)} E_{0,a} F_{1,b} + \omega_n^{i(a-b)} E_{1,a} F_{0,b} + \omega_n^{i(a+b-1)} E_{1,a} F_{1,b} \\ &= \sum_{a,b=0}^{n-1} \sum_{i=0}^{n-1} \omega_n^{i(a-b)} E_{0,a} F_{0,b} + \omega_n^{i(a+b)} E_{0,a} F_{1,b} + \omega_n^{i(a-b)} E_{1,a} F_{0,b} + \omega_n^{i(a+b-1)} E_{1,a} F_{1,b} \\ &= n \sum_{a=0}^{n-1} E_{0,a} F_{0,a} + E_{0,a} F_{1,-a} + E_{1,a} F_{0,a} + E_{1,a} F_{1,1-a} \end{aligned}$$

in which in the last equality we used the identity $1 + \omega_n + \ldots + \omega_n^{n-1} = 0$. Also note that in $F_{1,-a}$ and $F_{1,1-a}$ second indices should be read mod n. Finally notice that

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

□

5.4 Strategies for $\mathcal{G}_n$

In this section, we present quantum strategies $\mathcal{S}_n$ for $\mathcal{G}_n$ games. In Section 5.4.2, 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 5.7, 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.

5.4.1 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., $X_n e_i = e_{\sigma_n(i)}$. For convenience, we shall often drop the n subscript when the dimension is clear from context, and so just refer to $z_n, D_{n,j}, D_{n,S}, X_n$ as z, D_j, D_S, X, respectively.

Let $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^n$. Then Alice and Bob's shared state in $\mathcal{S}_n$ is defined to be

$$|\psi_n\rangle = \frac{1}{\gamma_n} \sum_{i=0}^{n-1} (1 - z^{n+2i+1}) |\sigma^i(0), \sigma^{-i}(0)\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B,$$

where $\gamma_n = \sqrt{2n + \frac{2}{\sin\left(\frac{\pi}{2n}\right)}}$ is the normalization factor. The generalized observables in $\mathcal{S}_n$ are

$$\begin{aligned} A_0 &= X \\ A_1 &= z^2 D_0 X \\ B_0 &= X \\ B_1 &= z^2 D_0 X^*. \end{aligned}$$

Example 5.4.1. 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 5.4.2. 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

$$|\psi_3\rangle = \frac{1}{\sqrt{10}}\Big((1-z^4)|00\rangle + 2|12\rangle + (1+z^2)|21\rangle\Big).$$

One can compute that $\langle\psi|\mathcal{B}_3|\psi\rangle = 6$. Hence, by Proposition 5.3.1, we have $\nu^*(\mathcal{G}_3) \geq \frac{5}{6}$.

5.4.2 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 5.4.3. *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 5.4.4. *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 5.4.5. *$X^i D_j = D_{\sigma^i(j)} X^i$, for all $i, j \in [n]$.*

Proof. It suffices to prove $XD_j = D_{\sigma(j)}X$. We show this by verifying $XD_je_k = D_{\sigma(j)}Xe_k$ for all $k \in [n]$.

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

□

Now we prove the strategy defined in section 5.4.1 is a valid quantum strategy.

Proposition 5.4.6. *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

$$A_1^n = (z^2D_0X)^n = z^{2n}D_{\{0,\sigma^1(0),\dots,\sigma^{n-1}(0)\}}X^n = (-1)(-I)I = I.$$

Similarly,

$$B_1^n = (z^2D_0X^*)^n = z^{2n}(X^*)^nD_{\{0,\sigma^1(0),\dots,\sigma^{n-1}(0)\}} = (-1)I(-I) = I.$$

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 5.4.4 in the third equality.

□

Lemma 5.4.7. *The entangled state $|\psi\rangle$ is an eigenvector for the bias $\mathcal{B} = \sum_{j=1}^{n-1} A_0^jB_0^{-j} + A_0^jB_1^j + A_1^jB_0^{-j} + z^{-4j}A_1^jB_1^j$ 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

$$\begin{aligned}\mathcal{B}|\varphi\rangle &= \left(\sum_{j=1}^{n-1} A_0^j \otimes B_0^{-j} + A_0^j \otimes B_1^j + A_1^j \otimes B_0^{-j} + z^{-4j}A_1^j \otimes B_1^j\right)|\varphi\rangle \\ &= \left(\sum_{j=1}^{n-1} (X \otimes X^*)^j + z^{2j}\,(X \otimes D_0X^*)^j + z^{2j}(D_0X \otimes X^*)^j + (D_0X \otimes D_0X^*)^j\right)|\varphi\rangle.\end{aligned}$$

Lemma 5.4.8. $(X \otimes D_0 X^*)^j |\varphi\rangle = (D_0 X \otimes X^*)^j |\varphi\rangle$ *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

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

Note that $I \otimes D_0 |\sigma^{i+1}(0), \sigma^{-i-1}(0)\rangle = D_0 \otimes I |\sigma^{i+1}(0), \sigma^{-i-1}(0)\rangle$ since $-i-1 = 0 \bmod n$ iff $i+1 = 0 \bmod n$. Therefore

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

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 5.4.5, and in the third equality we just expanded $|\varphi\rangle$. Note that

$$(D_{[j]} \otimes I) |\sigma^{i+j}(0), \sigma^{-(i+j)}(0)\rangle = \begin{cases} -|\sigma^{i+j}(0), \sigma^{-(i+j)}(0)\rangle & i \in [n-j, n-1], \\ |\sigma^{i+j}(0), \sigma^{-(i+j)}(0)\rangle & i \in [0, n-j-1], \end{cases}$$

and we use this to split the sum

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

and make a change of variable $r = i + j$ to get

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

We have $z^{2(r-i)} = z^{2(r-n+n-i)} = z^{2n}z^{2(r-n-i)} = -z^{2(r-n-i)}$ and $\sigma^{r}(0) = \sigma^{r+n}(0)$, so by another change of variable in the second sum where we are summing over $r = [n, n+i-1]$ we obtain

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

We also have

$$\begin{aligned}\sum_{i=0}^{n-1}\left(1-z^{2i+n+1}\right)\left(1+z^{2(r-i)}\right) &= \sum_{i=0}^{n-1} 1 - z^{2r+n+1} + z^{2(r-i)} - z^{2i+n+1}\\ &= \sum_{i=0}^{n-1} 1 - z^{2r+n+1} + z^{2(r-i)} - z^{-(2i+n+1)}\\ &= (1-z^{2r+n+1})\sum_{i=0}^{n-1} 1 - z^{-(2i+n+1)}\\ &= \left(n + \frac{1}{\sin(\frac{\pi}{2n})}\right)(1-z^{2r+n+1}),\end{aligned}$$

where in the second and last equality we used Propositions 5.4.3 and 5.4.4, respectively. Putting these together, we obtain

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

□

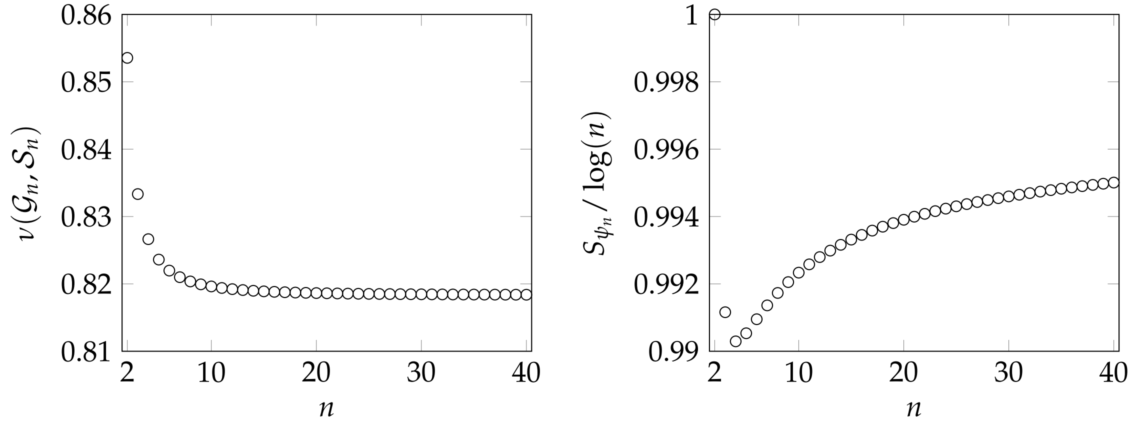

Figure 5.2: The figure on the left illustrates the fast convergence rate of the winning probabilities as they approach the limit $1/2 + 1/\pi$. The figure on the right illustrates the ratio of the entanglement entropy to the maximum entanglement entropy of the states for $n \leq 40$.

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 5.2.

Theorem 5.4.9. $\nu(\mathcal{G}_n, \mathcal{S}_n) = \frac{1}{2} + \frac{1}{2n\sin\left(\frac{\pi}{2n}\right)}$.

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 5.4.10. *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 5.4.11. *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 $n \to \infty$. In particular, up to local isometries, these states approach the maximally entangled state.*

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 $|i_A\rangle = \frac{1-z^{2i+n+1}}{\|1-z^{2i+n+1}\|}|\sigma^i(0)\rangle$ 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 $\lim_{n\to\infty}\frac{S_{\psi_n}}{\log(n)} = 1$. □

5.5 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 $(A_1A_0^*)^2 = z_n^4 I$, we could equivalently define $H_n = \langle A_0, A_1, z_n^4 I\rangle$. Also let

$$G_n = \left\langle P_0, P_1, J \mid P_0^n, P_1^n, J^n, [J, P_0], [J, P_1], J^i\left(P_0^iP_1^{-i}\right)^2 \text{ for } i = 1, 2, \ldots, \lfloor n/2\rfloor\right\rangle.$$

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 5.7, we prove this for $n = 3$.

Remark 5.5.1. 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 5.5.2. *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 5.5.3. *For every $g \in G_n$ there exist $i, j \in [n]$ and $q_k \in \{0, 1\}$ for $k = 1, 2, \ldots, n-1$ such that*

$$g = J^i P_0^j \left(P_0 P_1^{-1}\right)^{q_1}\left(P_0^2 P_1^{-2}\right)^{q_2} \cdots \left(P_0^{n-1} P_1^{-(n-1)}\right)^{q_{n-1}}.$$

Proof. First note that J is central, therefore we can write g in G_n as

$$g = J^i P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_k},$$

for some $k \in \mathbb{N}$, $i \in [n]$, $j_l \in [n]$ where $l = 1, 2, \ldots, k$. Without loss of generality, let k be even. We perform the following sequence of manipulations

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

where $s_l = -\sum_{t=l}^{k} j_t$ and $s = -\sum_{t=1}^{(k-2)/2} s_{2t+1}$. Then we use the commutation relationship from lemma 5.6.2 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 5.5.4. $|G_n| \leq n^2 2^{n-1}$ *for all* $n \in \mathbb{N}$.

Proof. Follows from lemma 5.6.3. □

Lemma 5.5.5. $|H_n| \geq n^2 2^{n-1}$ *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 5.4.5. 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 5.5.6. *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 5.5.7. *$H_n \cong G_n$ for all $n \in \mathbb{N}$.*

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

Remark 5.5.8. 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 5.6.7 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.

5.6 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 5.7, we prove this for $n = 3$.

Remark 5.6.1. 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 5.6.2. *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 5.6.3. *For every $g \in G_n$ there exist $i, j \in [n]$ and $q_k \in \{0, 1\}$ for $k = 1, 2, \ldots, n-1$ such that*

$$g = J^i P_0^j \left(P_0 P_1^{-1}\right)^{q_1} \left(P_0^2 P_1^{-2}\right)^{q_2} \cdots \left(P_0^{n-1} P_1^{-(n-1)}\right)^{q_{n-1}}.$$

Proof. First note that J is central, therefore we can write g in G_n as

$$g = J^i P_0^{j_1} P_1^{j_2} P_0^{j_3} \cdots P_1^{j_k},$$

for some $k \in \mathbb{N}$, $i \in [n]$, $j_l \in [n]$ where $l = 1, 2, \ldots, k$. Without loss of generality, let k be even. We perform the following sequence of manipulations

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

where $s_l = -\sum_{t=l}^{k} j_t$ and $s = -\sum_{t=1}^{(k-2)/2} s_{2t+1}$. Then we use the commutation relationship from lemma 5.6.2 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 5.6.4. *$|G_n| \leq n^2 2^{n-1}$ for all $n \in \mathbb{N}$.*

Proof. Follows from lemma 5.6.3. □

Lemma 5.6.5. *$|H_n| \geq n^2 2^{n-1}$ 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 5.4.5. 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 $\frac{n}{2}n2^{n-1} + \frac{n}{2}n2^{n-1} = n^2 2^{n-1}$ elements. □

Lemma 5.6.6. *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 5.6.7. *$H_n \cong G_n$ 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 5.6.8. 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 5.6.7 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.

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

In this section, we show that $\mathcal{S}_3$ is optimal, and therefore $\nu^*(\mathcal{G}_3) = 5/6$. We also show that $\mathcal{G}_3$ is a self-test for the strategy $\mathcal{S}_3$. We obtain these results by obtaining algebraic relations between operators in any optimal strategy using an SOS decomposition for $\mathcal{B}_3$.

5.7.1 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:

$$\begin{aligned}
&6I - A_0 B_0^* - A_0^* B_0 - A_0 B_1 - A_0^* B_1^* - A_1 B_0^* - A_1^* B_0 - \omega^* A_1 B_1 - \omega A_1^* B_1^* \\
&\quad = \lambda_1(S_1^* S_1 + S_2^* S_2) + \lambda_2(T_1^* T_1 + T_2^* T_2) + \lambda_3(T_3^* T_3 + T_4^* T_4) + \lambda_4(T_5^* T_5 + T_6^* T_6), \qquad (5.7.1)
\end{aligned}$$

where

$$\begin{aligned}
S_1 &= A_0 + \omega A_1 + \omega^* B_0 + \omega B_1^*, \\
S_2 &= A_0^* + \omega^* A_1^* + \omega B_0^* + \omega^* B_1, \\
T_1 &= A_0 B_0^* + aiA_0^* B_0 - aA_0 B_1 + iA_0^* B_1^* + aA_1 B_0^* - iA_1^* B_0 - \omega^* A_1 B_1 - ai\omega A_1^* B_1^*, \\
T_2 &= A_0 B_0^* + aiA_0^* B_0 + aA_0 B_1 - iA_0^* B_1^* - aA_1 B_0^* + iA_1^* B_0 - \omega^* A_1 B_1 - ai\omega A_1^* B_1^*, \\
T_3 &= A_0 B_0^* - aiA_0^* B_0 - aA_0 B_1 - iA_0^* B_1^* + aA_1 B_0^* + iA_1^* B_0 - \omega^* A_1 B_1 + ai\omega A_1^* B_1^*, \\
T_4 &= A_0 B_0^* - aiA_0^* B_0 + aA_0 B_1 + iA_0^* B_1^* - aA_1 B_0^* - iA_1^* B_0 - \omega^* A_1 B_1 + ai\omega A_1^* B_1^*, \\
T_5 &= A_0 B_0^* + bA_0^* B_0 - bA_0 B_1 - A_0^* B_1^* - bA_1 B_0^* - A_1^* B_0 + \omega^* A_1 B_1 + b\omega A_1^* B_1^*, \\
T_6 &= 6I - A_0 B_0^* - A_0^* B_0 - A_0 B_1 - A_0^* B_1^* - A_1 B_0^* - A_1^* B_0 - \omega^* A_1 B_1 - \omega A_1^* B_1^*,
\end{aligned}$$

and

$$\lambda_1 = \frac{5}{86},\ \lambda_2 = \frac{14+\sqrt{21}}{4 \cdot 86},\ \lambda_3 = \frac{14-\sqrt{21}}{4 \cdot 86},\ \lambda_4 = \frac{7}{86},$$
$$a = \frac{2\omega + 3\omega^*}{\sqrt{7}},\ b = \frac{3\omega + 8\omega^*}{7}, \omega = \omega_3.$$

This SOS decomposition tells us that $\mathcal{B}_3 \preceq 6I$ in positive semidefinite order. So from Theorem 5.3.1, it holds that $\nu^*(\mathcal{G}_3) \leq 5/6$. Combined with Theorem 5.4.9, 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.

5.7.2 Algebraic relations

As in Section **??**, we derive group and ring relations for optimal strategies of $\mathcal{G}_3$ from the SOS (5.7.1). For the rest of this section, let $(A_0, A_1, B_0, B_1, |\psi\rangle)$ be an optimal strategy. Then $\langle\psi|(6I - \mathcal{B}_3)|\psi\rangle = 0$. So it also holds that $S_i|\psi\rangle = 0$ and $T_j|\psi\rangle = 0$ for all $i \in [2]$ and $j \in [6]$. Therefore

$$(T_1 + T_2 + T_3 + T_4)|\psi\rangle = 0, \quad (T_1 + T_2 - T_3 - T_4)|\psi\rangle = 0,$$
$$(T_1 - T_2 + T_3 - T_4)|\psi\rangle = 0, \quad (T_1 - T_2 - T_3 + T_4)|\psi\rangle = 0.$$

From which by simplification we obtain the four relations

$$\begin{aligned}
A_0 B_0^*|\psi\rangle &= \omega^* A_1 B_1|\psi\rangle, \quad A_0^* B_0|\psi\rangle = \omega A_1^* B_1^*|\psi\rangle, \\
A_0 B_1|\psi\rangle &= A_1 B_0^*|\psi\rangle, \qquad A_0^* B_1^*|\psi\rangle = A_1^* B_0|\psi\rangle.
\end{aligned} \tag{5.7.2}$$

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

$$\omega^* A_0^* A_1|\psi\rangle = B_1^* B_0^*|\psi\rangle \tag{5.7.3}$$
$$\omega A_0 A_1^*|\psi\rangle = B_1 B_0|\psi\rangle \tag{5.7.4}$$
$$A_0^* A_1|\psi\rangle = B_0 B_1|\psi\rangle \tag{5.7.5}$$
$$A_0 A_1^*|\psi\rangle = B_0^* B_1^*|\psi\rangle \tag{5.7.6}$$
$$A_1^* A_0|\psi\rangle = \omega^* B_0 B_1|\psi\rangle \tag{5.7.7}$$
$$A_1 A_0^*|\psi\rangle = \omega B_0^* B_1^*|\psi\rangle \tag{5.7.8}$$
$$A_1^* A_0|\psi\rangle = B_1^* B_0^*|\psi\rangle \tag{5.7.9}$$
$$A_1 A_0^*|\psi\rangle = B_1 B_0|\psi\rangle. \tag{5.7.10}$$

From the pair of relations (5.7.3) and (5.7.9) as well as the pair of relations (5.7.4) and (5.7.10), we obtain the following relations between Alice's observables acting on the state $|\psi\rangle$:

$$\begin{aligned} A_0^* A_1 |\psi\rangle &= \omega A_1^* A_0 |\psi\rangle, && (5.7.11) \\ A_1 A_0^* |\psi\rangle &= \omega A_0 A_1^* |\psi\rangle. && (5.7.12) \end{aligned}$$

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 (**??**).

Proposition 5.7.1. $(H + H^*)|\psi\rangle = -2|\psi\rangle$

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

$$(B_0 B_1^* + B_1^* B_0)|\psi\rangle = (2A_0^* + 2\omega^* A_1^* + \omega A_0 A_1 + \omega A_1 A_0)|\psi\rangle. \qquad (5.7.13)$$

Similarly we have

$$(B_1 B_0^* + B_0^* B_1)|\psi\rangle = (2A_0 + 2\omega A_1 + \omega^* A_0^* A_1^* + \omega^* A_1^* A_0^*)|\psi\rangle. \qquad (5.7.14)$$

We proceed by simplifying $T_6|\psi\rangle = 0$ using relations (5.7.2) to obtain

$$(3I - A_0 B_0^* - A_0^* B_0 - A_0 B_1 - A_0^* B_1^*)|\psi\rangle = 0.$$

Let $P = A_0 B_0^* + A_0^* B_0 + A_0 B_1 + A_0^* B_1^*$, and write

$$\begin{aligned} 0 &= \big(3I - A_0 B_0^* - A_0^* B_0 - A_0 B_1 - A_0^* B_1^*\big)^* \big(3I - A_0 B_0^* - A_0^* B_0 - A_0 B_1 - A_0^* B_1^*\big)|\psi\rangle \\ &= \big(13I - 5P + A_0^*(B_1 B_0^* + B_0^* B_1) + A_0(B_0 B_1^* + B_1^* B_0) + B_0^* B_1^* + B_0 B_1 + B_1 B_0 + B_1^* B_0^*\big)|\psi\rangle \\ &= (-2I + A_0^*(B_1 B_0^* + B_0^* B_1) + A_0(B_0 B_1^* + B_1^* B_0) + B_0^* B_1^* + B_0 B_1 + B_1 B_0 + B_1^* B_0^*)|\psi\rangle, \quad (5.7.15) \end{aligned}$$

where in the last line, we used $(3I - P)|\psi\rangle = 0$. Using identities (5.7.13) and (5.7.14)

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

Transferring Bob's operators to Alice using identities (5.7.3-5.7.6)

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

Plugging these back in (5.7.15)

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

where in the first line we used $1 + \omega + \omega^* = 0$, and in the second line we used identities (5.7.11) and (5.7.12). □

Proposition 5.7.2. $(H+I)|\psi\rangle = (H^*+I)|\psi\rangle = 0$.

Proof. First note

$$\begin{aligned}\langle\psi|H^*H|\psi\rangle = \langle\psi|(3I + A_0^*A_1^*A_0A_1 + A_1^*A_0^*A_1A_0 + A_1^*A_0A_1A_0^* + A_0A_1^*A_0^*A_1 \\ + A_0^*A_1^*A_0^*A_1A_0^* + A_0A_1^*A_0A_1A_0)|\psi\rangle. \qquad (5.7.16)\end{aligned}$$

Using (5.7.11) and (5.7.12), we have

$$\begin{aligned}\langle\psi|A_0A_1^*A_0^*A_1|\psi\rangle &= \omega\langle\psi|A_0A_1^*A_1^*A_0|\psi\rangle = \omega\langle\psi|A_0A_1A_0|\psi\rangle,\\ \langle\psi|A_0^*A_1^*A_0^*A_1A_0^*|\psi\rangle &= \omega\langle\psi|A_0^*A_1^*A_0^*A_0A_1^*|\psi\rangle = \omega\langle\psi|A_0^*A_1|\psi\rangle,\end{aligned}$$

and using (5.7.5) and (5.7.7)

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

and taking conjugate transpose of these three we obtain

$$\begin{aligned}\langle\psi|A_1^*A_0A_1A_0^*|\psi\rangle &= \omega^*\langle\psi|A_0^*A_1^*A_0^*|\psi\rangle,\\ \langle\psi|A_0A_1^*A_0A_1A_0|\psi\rangle &= \omega^*\langle\psi|A_1^*A_0|\psi\rangle,\\ \langle\psi|A_1^*A_0^*A_1A_0|\psi\rangle &= \omega^*\langle\psi|A_0A_1^*|\psi\rangle.\end{aligned}$$

Plugging these back in (5.7.16), 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 5.7.1. 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 5.7.3. $A_0A_1A_0|\psi\rangle = \omega A_0^*A_1^*A_0^*|\psi\rangle$.

Proof. By Proposition 5.7.2, $H|\psi\rangle = H^*|\psi\rangle$, and by identities (5.7.11), (5.7.12), $(\omega A_0^*A_1 + \omega A_1A_0^*)|\psi\rangle = (\omega^*A_1^*A_0 + \omega^*A_0A_1^*)|\psi\rangle$. Putting these together, we obtain $A_0A_1A_0|\psi\rangle = \omega A_0^*A_1^*A_0^*|\psi\rangle$. □

Proposition 5.7.4. $A_0A_1^*A_0^*A_1|\psi\rangle = A_0^*A_1A_0A_1^*|\psi\rangle$ *in other words* $A_0A_1^*$ *and* $A_0^*A_1$ *commute on* $|\psi\rangle$

Proof. To see this write

$$\begin{aligned}A_0A_1^*A_0^*A_1|\psi\rangle &= \omega A_0A_1^*A_1^*A_0|\psi\rangle\\ &= \omega A_0A_1A_0|\psi\rangle\\ &= \omega^*A_0^*A_1^*A_0^*|\psi\rangle\\ &= \omega^*A_0^*A_1A_1A_0^*|\psi\rangle\\ &= A_0^*A_1A_0A_1^*|\psi\rangle,\end{aligned}$$

where in the first line we used 5.7.11, in the third line we used 5.7.3, and in the fifth line we used 5.7.12.

□

5.7.3 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 5.6.7, we know that the optimal operators of Alice defined in section 5.4.1 generate the group

$$G_3 = \left\langle J, P_0, P_1 : J^3, P_0^3, P_1^3, [J, P_0], [J, P_1], J(P_0P_1^{-1})^2 \right\rangle,$$

The same group is generated by Bob's operators as in Remark 5.6.8. We apply Corollary 5.2.5 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 5.7.5. *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 5.6.3. 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 uniquly 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

$$\begin{aligned} &f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})f_A(J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'})|\psi\rangle \\ &\quad= f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2}J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'})|\psi\rangle \end{aligned} \tag{5.7.17}$$

for all $i, j, i', j' \in [3]$ and $q_1, q_2, q_1', q_2' \in [2]$.

Claim 9. *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 5.6.3, there exist $i'', j'' \in [3], q_1'', q_2'' \in [2]$ such that

$$\left(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2}\right)\left(J^{i'}P_0^{j'}\right) = J^{i''}P_0^{j''}(P_0P_1^{-1})^{q_1''}(P_0^{-1}P_1)^{q_2''}.$$

So it also holds that

$$\left(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2}\right)\left(J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'}\right) = J^{i''}P_0^{j''}(P_0P_1^{-1})^{q_1''+q_1'}(P_0^{-1}P_1)^{q_2''+q_2'}$$

since by Lemma 5.6.2, $P_0P_1^{-1}$ and $P_0^{-1}P_1$ commute. So the right-hand-side of (5.7.17) can be written

$$\begin{aligned} &f_A(J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2}J^{i'}P_0^{j'}(P_0P_1^{-1})^{q_1'}(P_0^{-1}P_1)^{q_2'})|\psi\rangle \\ &\quad= f_A(J^{i''}P_0^{j''}(P_0P_1^{-1})^{q_1''+q_1'}(P_0^{-1}P_1)^{q_2''+q_2'})|\psi\rangle \\ &\quad= \omega^{i''}A_0^{j''}(A_0A_1^{-1})^{q_1''+q_1'}(A_0^{-1}A_1)^{q_2''+q_2'}|\psi\rangle \\ &\quad= (B_0B_1)^{q_2'}(B_0^*B_1^*)^{q_1'}\omega^{i''}A_0^{j''}(A_0A_1^{-1})^{q_1''}(A_0^{-1}A_1)^{q_2''}|\psi\rangle \\ &\quad= (B_0B_1)^{q_2'}(B_0^*B_1^*)^{q_1'}f_A(J^{i''}P_0^{j''}(P_0P_1^{-1})^{q_1''}(P_0^{-1}P_1)^{q_2''})|\psi\rangle \\ &\quad= (B_0B_1)^{q_2'}(B_0^*B_1^*)^{q_1'}f_A((J^iP_0^j(P_0P_1^{-1})^{q_1}(P_0^{-1}P_1)^{q_2})(J^{i'}P_0^{j'}))|\psi\rangle, \end{aligned}$$

where in the fourth equality, we used (5.7.5) and (5.7.6) and the fact that Alice and Bob's operators commute.

Also since Alice and Bob's operators commute

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

Therefore the left-hand-side of (5.7.17) can be written as

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

Since B_0, B_1 are unitaries, (5.7.17) is equivalent to the following identity

$$f_A(J^i P_0^j (P_0 P_1^{-1})^{q_1} (P_0^{-1} P_1)^{q_2}) f_A(J^{i'} P_0^{j'})|\psi\rangle = f_A((J^i P_0^j (P_0 P_1^{-1})^{q_1} (P_0^{-1} P_1)^{q_2})(J^{i'} P_0^{j'}))|\psi\rangle,$$

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

$$f_A((P_0 P_1^{-1})^{q_1} (P_0^{-1} P_1)^{q_2}) f_A(P_0^{j'})|\psi\rangle = f_A((P_0 P_1^{-1})^{q_1} (P_0^{-1} P_1)^{q_2} P_0^{j'})|\psi\rangle \tag{5.7.18}$$

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

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

  which allows us to write

  $$\begin{aligned} f_A((P_0^{-1} P_1)) f_A(P_0)|\psi\rangle &= A_0^* A_1 A_0 |\psi\rangle \\ &= A_0^* A_1^* A_1^* A_0 |\psi\rangle \\ &= \omega^* A_0^* A_1^* A_0^* A_1 |\psi\rangle \\ &= \omega^* A_0 (A_0 A_1^*)(A_0^* A_1)|\psi\rangle \\ &= f_A(J^2 P_0 (P_0 P_1^{-1})(P_0^{-1} P_1))|\psi\rangle \\ &= f_A((P_0^{-1} P_1) P_0)|\psi\rangle, \end{aligned}$$

  where in the third line we used (5.7.11).

- $q_1 = 1, q_2 = 0$:

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

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 (5.7.11).

- $q_1 = q_2 = 1$:

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

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 5.7.3 and in the second last line we used (5.7.12).

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

Theorem 5.7.6. *$\mathcal{G}_3$ 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

$$\begin{aligned} g_1(P_0) &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \; g_1(P_1) = \begin{pmatrix} 0 & 0 & \omega^* \\ -\omega^* & 0 & 0 \\ 0 & -\omega^* & 0 \end{pmatrix}, \; g_1(J) = \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{pmatrix}, \\ g_2(P_0) &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \; g_2(P_1) = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \; g_2(J) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \\ g_3(P_0) &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \; g_3(P_1) = \begin{pmatrix} 0 & \omega & 0 \\ 0 & 0 & -\omega \\ -\omega & 0 & 0 \end{pmatrix}, \; g_3(J) = \begin{pmatrix} \omega^* & 0 & 0 \\ 0 & \omega^* & 0 \\ 0 & 0 & \omega^* \end{pmatrix}. \end{aligned}$$

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 $\widetilde{A}_0 = g_1(P_0), \widetilde{A}_1 = g_1(P_1), \widetilde{B}_0 = g_1'(P_0)^*, \widetilde{B}_1 := g_1'(P_1)$ is the same strategy defined in example 5.4.2.

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 5.2.5.

□

Remark 5.7.7. 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.

5.8 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 [CLS17] 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 5.2.3 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:

$$\sum_{x:x \in S_i} E_{i,x} = \frac{1}{2}\left(I + (-1)^{b_i} \prod_{k \in V_i} A_k^{(i)}\right) \tag{5.8.1}$$

$$\sum_{x:y=x_j} E_{i,x} = \frac{1}{2}\left(I + yA_j^{(i)}\right) \tag{5.8.2}$$

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 5.8.1 and 5.8.2 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 $j\in V_i$,

$$
B_j|\psi\rangle = A_j^{(i)}|\psi\rangle \tag{5.8.3}
$$

$$
|\psi\rangle = (-1)^{b_i}\prod_{k\in v_i}A_k^{(i)}|\psi\rangle \tag{5.8.4}
$$

Using identities 5.8.3 and 5.8.4 it is possible to define a $|\psi\rangle$-representation for the solution group $G_{A,b}$.

5.9 A non-rigid pseudo-telepathic LCS game

The canonical example of a pseudo-telepathic LCS games is the Mermin-Peres magic square game [Mer90] defined in the following figure.

$$\begin{array}{ccccc}
e_1 & \text{—} & e_2 & \text{—} & e_3 \\
| & & | & & \| \\
e_4 & \text{—} & e_5 & \text{—} & e_6 \\
| & & | & & \| \\
e_7 & \text{—} & e_8 & \text{—} & e_9
\end{array}$$

Figure 5.3: 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 [WBMS15].

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

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 5.4.

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

Figure 5.4: 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 5.9.1. *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 $(\{A_i\}_i, \{B_j\}_j |\psi\rangle)$ that is rigid. Then there exist local isometries U_A, U_B and V_A, V_B such that

$$(U_A E_1 \otimes U_B)|\psi_1\rangle = ((A_1 \otimes I)|\psi\rangle)|\text{junk}_1\rangle \tag{5.9.1}$$

$$(U_A E_5 \otimes U_B)|\psi_1\rangle = ((A_5 \otimes I)|\psi\rangle)|\text{junk}_1\rangle \tag{5.9.2}$$

$$(V_A F_1 \otimes V_B)|\psi_2\rangle = ((A_1 \otimes I)|\psi\rangle)|\text{junk}_2\rangle \tag{5.9.3}$$

$$(V_A F_5 \otimes V_B)|\psi_2\rangle = ((A_5 \otimes I)|\psi\rangle)|\text{junk}_2\rangle. \tag{5.9.4}$$

From relation (5.9.2), 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 (5.9.1), we obtain the following relation between $E_5 E_1$ and $A_5^* A_1$

$$\langle\psi_1|(E_5 E_1 \otimes I)|\psi_1\rangle = \langle\psi|(A_5^* A_1 \otimes I)|\psi\rangle.$$

Similarly, we also obtain

$$\langle\psi_2|(F_5 F_1 \otimes I)|\psi_2\rangle = \langle\psi|(A_5^* A_1 \otimes I)|\psi\rangle,$$

and hence

$$\langle\psi_1|(E_5 E_1 \otimes I)|\psi_1\rangle = \langle\psi_2|(F_5 F_1 \otimes I)|\psi_2\rangle.$$

By first applying the adjoint to relation (5.9.1) and (5.9.3), we obtain

$$\langle\psi_1|(E_1 E_5 \otimes I)|\psi_1\rangle = \langle\psi_2|(F_1 F_5 \otimes I)|\psi_2\rangle.$$

Now, since F_1 and F_5 anti-commute, we get the following relation between $E_5 E_1$ and $E_1 E_5$

$$\langle\psi_1|(E_5 E_1 \otimes I)|\psi_1\rangle = -\langle\psi_1|(E_1 E_5 \otimes I)|\psi_1\rangle.$$

However, a direct computation of $\langle\psi_1|(E_5 E_1 \otimes I)|\psi_1\rangle$ shows that

$$\langle\psi_1|(E_5 E_1 \otimes I)|\psi_1\rangle = \frac{1}{8} \sum_{i=0}^{7} \langle i|E_5 E_1|i\rangle = \frac{1}{8} \operatorname{Tr}(E_5 E_1) = \frac{1}{8} \operatorname{Tr}(E_1 E_5) = \langle\psi_1|(E_1 E_5 \otimes I)|\psi_1\rangle,$$

and $\operatorname{Tr}(E_1 E_5) = \operatorname{Tr}(I_4) + \operatorname{Tr}(I \otimes \sigma_Z \sigma_X) = 4 \neq 0$. Hence, the glued magic square game is not rigid. □

Although this game is not a self-test, we know from Section 5.8 Alice's operators must provide a $|\psi\rangle$-representation for the solution group of glued magic square, and thus must satisfy particular group relations.

Bibliography

[ABG$^+$07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007.

[AH89] K. Appel and W. Haken. Every planar map is four colorable. *Contemporary Mathematics*, 98, 1989.

[AMR$^+$19] 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*, 136:289 – 328, 2019.

[Art27] E. Artin. Uber die zerlegung definiter funktionen in quadrate. *MAbhandlungen aus dem Mathematischen Seminar der Universat Hamburg*, 5:110–115, 1927.

[Ban77] P. Bankston. Ultraproducts in topology. *General Topology and it's Applications*, pages 283–308, 1977.

[Bel64] John Stewart Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1:195, 1964.

[BP15] Cédric Bamps and Stefano Pironio. Sum-of-squares decompositions for a family of clauser-horne-shimony-holt-like inequalities and their application to self-testing. *Phys. Rev. A*, 91(052111), 2015.

[BS15] Mohammad Bavarian and Peter W. Shor. Information causality, szemerédi-trotter and algebraic variants of chsh. In *Conference on Innovations in Theoretical Computer Science*, 2015.

[CE77] M.D Choi and E.G Effros. Injectivity and operator spaces. the general case. *Indiana Univ. Math J.*, 26, 1977.

[CGJV19a] Andrea Coladangelo, Alex B. Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: New schemes for verifiable delegated quantum computation, with quasilinear resources. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 247–277, Cham, 2019. Springer International Publishing.

[CGJV19b] Andrea Coladangelo, Alex B. Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: New schemes for verifiable delegated quantum computation, with quasilinear resources. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 247–277, Cham, 2019. Springer International Publishing.

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

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

[CHTW04] Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, CCC '04, pages 236–249, Washington, DC, USA, 2004. IEEE Computer Society.

[CL76] M.D Choi and T.Y Lam. an old question of hilbert. *Queens Papers in Pure and Appl. Math. (Proceedings of Quadratic Forms Conference, Queens University (G. Orzech ed.))*, pages 385–405, 1976.

[CL77] M.D Choi and T.Y Lam. Extremal positive semidefinite forms. *Math. Ann., 231*, pages 1–18, 1977.

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

[CM12] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. In *International Colloquium on Automata, Languages, and Programming (ICALP) 2012*, pages 320–331, 2012.

[CMMN20] David Cui, Arthur Mehta, Hamoon Mousavi, and Seyed Sajjad Nezhadi. A generalization of chsh and the algebraic structure of optimal strategies. In *QIP 2020, to appear in Quantum*, 2020.

[CN10] Isaac Chuang and Michael Nielsen. *Quantum Computation and Quantum Information.* Cambridge University Press, 2010.

[CN16] Matthew Coudron and Anand Natarajan. The parallel-repeated magic square game is rigid. arXiv:1609.06306 [quant-ph], 2016.

[CNM$^+$07] P.J. Cameron, M.W. Newman, A. Montanaro, S. Severini, and A. Winter. On the quantum chromatic number of a graph. *The electronic journal of combinatorics*, 14, 2007.

[Col16] Andrea Coladangelo. Parallel self-testing of (tilted) epr pairs via copies of (tilted) chsh. *Quantum Information and Computation*, 17:35, 2016.

[Coo71] Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, STOC '71, page 151–158. Association for Computing Machinery, 1971.

[CS78] J.F Clauser and A. Shimony. Bell's theorem. experimental tests and implications. *Reports on Progress in Physics*, 41(12):1881, 1978.

[CS18] Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games. In *QIP 2018*, 2018.

[CSUU07] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Perfect parallel repetition theorem for quantum xor proof systems. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 109–114, 2007.

[Dav96] K. Davidson. *C*-Algebras by Example*. Fields Institute Monograph Series volume 6, 1996.

[DSW13] R. Duan, S. Severini, and A. Winter. Zero-error communication via quantum channels, noncommutative graphs, and a quantum lovász number. *IEEE Transactions on Information Theory*, 59(2):1164–1174, 2013.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10), 1935.

[FJVY19] Joseph Fitzsimons, Zhengfeng Ji, Thomas Vidick, and Henry Yuen. Quantum proof systems for iterated exponential time, and beyond. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, pages 473–480, New York, NY, USA, 2019. ACM.

[GH17] William Timothy Gowers and Omid Hatami. Inverse and stability theorems for approximate representations of finite groups. *Sbornik: Mathematics*, 208(12):1784, 2017.

[GR16] C. Godsil, D. E. Roberson, R. Šámal, and S Severini. Sabidussi versus hedetniemi for three variations of the chromatic number. *Combinatorica*, 36(4):395–415, 2016.

[Hal13] B. C. Hall. *Quantum Theory for Mathematicians*. Springer, 2013.

[Hed66] S. Hedetniemi. Homomorphisms of graphs and automata. *Technical Report 03105-44-T*, 1966.

[Hel02] W Helton. "positive" noncommutative polynomials are sums of squares. *Annals of Mathematics*, 156:675–694, 2002.

[Hil88] D. Hilbert. Summ. *Math. Ann*, 32:342–350, 1888.

[HPP16] Samuel J. Harris, Satish K. Pandey, and Vern Paulsen. Entanglement and non-locality. Available at `https://www.math.uwaterloo.ca/~vpaulsen/EntanglementAndNonlocality_LectureNotes_7.pdf`, 2016.

[JNV$^+$20] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen. Mip*=re. 2020. https://arxiv.org/abs/2001.04383.

[Kar72] Richard M. Karp. *Reducibility among Combinatorial Problems*, pages 85–103. Springer US, Boston, MA, 1972.

[KKS17] M. Kennedy, T. Kolomatski, and D. Spivak. An infinite quantum ramsay theorem. 2017. perprint: https://arxiv.org/abs/1711.09526.

[KM17] S.J. Kim and A. Mehta. Chromatic numbers and a lovász type inequality for non-commutative graphs. 2017. https://arxiv.org/abs/1709.05595.

[KM19] S.J. Kim and A. Mehta. Chromatic numbers, sabidussi's theorem and hedetniemi's conjecture for non-commutative graphs. *Linear Algebra and its Applications*, 582:291–309, 2019.

[Knu94] Donald E. Knuth. The sandwich theorem. *Electronic Journal of Combinatorics: A1*, 1994.

[KvT$^+$18] Jędrzej Kaniewski, Ivan Šupić, Jordi Tura, Flavio Baccari, Alexia Salavrakos, and Remigiusz 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.

[Kö12] D. König. *Theory of finite and infinite graphs*. 2012. Translated by R. McCoart and commentary by W. Tutte.

[Lev73] L.A Levin. Universal sequential search problems. *Probl. Peredachi Inf.*, 9, 1973.

[Lov79] L. Lovász. On the shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25(1):1–7, 1979.

[LPT17] R. Levene, V. Paulsen, and I. Todorov. Complexity and capacity bounds for quantum channels. *IEEE Transactions on Information Theory*, 2017. Preprint available at https://arxiv.org/abs/1710.06456.

[Mac04] G. W. Mackey. *The Mathematical Foundations of Quantum Mechanics*. Dover Publications, 2004.

[Mck16] Matthew Mckague. Self-testing in parallel with chsh. *Quantum*, 1, 2016.

[Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65(27):3373, 1990.

[Mot67] T.S Motzkin. The arithmetic-geometric inequality. *Proc. Symposium on Inequalities, Academic Press, New York*, pages 205–224, 1967.

[MP05] S. McCullough and M. Putinar. Noncommutative sums of squares. *Pacific Journal of Mathematics*, pages 167–171, 2005.

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

[MYS12] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. Robust self-testing of the singlet. *Journal of Mathematical Physics*, 45:455304, 2012.

[NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008.

[NT13] T. Netzer and A. Thom. Real closed separation theorems and applications to group algebras. *Pacific Journal of Mathematics*, 2013.

[NV17] Anand Natarajan and Thomas Vidick. Robust self-testing of many-qubit states. In *STOC*, 2017.

[NV18] Anand Natarajan and Thomas 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)*, pages 731–742, 2018.

[NW19] Anand Natarajan and John Wright. Neexp in mip. *ArXiv*, abs/1904.05870, 2019.

[OP15] C. M. Ortiz and V. I. Paulsen. Lovász theta type norms and operator systems. *Linear Algebra and its Applications*, 477:128–147, 2015.

[Oza13] Narutaka Ozawa. About the connes embedding conjecture, algebraic approaches. *Jpn. J. Math.*, 8:147–183, 2013.

[Pau03] V. I. Paulsen. Completely bounded maps and operator algebras. *Cambridge Studies in Advanced Mathematics*, 78:Cambridge University Press, 2003.

[Ped89] G. K. Pedersen. *Analysis Now*. Springer, 1989.

[PHMS19] V. Paulsen, J.W. Helton, K.P. Meyer, and M. Satriano. Algebras, synchronous games and chromatic numbers of graphs. *New York J. Math.*, page 328–361, 2019.

[PNA10] S. Pironio, M. Navascués, and A. Antonio. Convergent relaxations of polynomial optimization problems with noncommuting variables. *Society for Industrial and Applied Mathematics*, 20, 2010.

[PT15] V. I. Paulsen and I. G. Todorov. Quantum chromatic numbers via operator systems. *Quarterly J. Math.*, 66:677–692, 2015.

[RM16] David E. Roberson and Laura Man˘cinska. Graph homomorphisms for quantum players. *Journal of Combinatorial Theory, Series B*, 2016.

[Rob69] R.M Robinson. Some definite polynomials which are not sums of squares of real polynomials. *Notices amer. Math. Soc*, 1969.

[Rud63] W. Rudin. The extension problem for positive-definite functions. *Illinois J. Math.*, 7:532–539, 1963.

[Sab57] G. Sabidussi. Graphs with given group and given graph-theoretical properties. *Canadian Journal of Mathematics*, 9:515–525, 1957.

[SB07] P.W. Shor and S. Beigi. On the complexity of computing zero-error and holevo capacity of quantum channels. *https://arxiv.org/abs/0709.2090*, 2007.

[SB19] Ivan Supić and Joseph Bowles. Self-testing of quantum systems: a review. Available at `https://arxiv.org/pdf/1904.10042.pdf`, 2019.

[SBG20] S.Harris, M. Brannan, and P. Ganesan. The quantum-to-classical graph homomorphism game. 2020. preprint available: https://arxiv.org/abs/2009.07229.

[Sch99] C. Scheiderer. Sums of squares of regular functions on real algebraic varie ties. *rans. Am. Math. Soc.*, 352:1039–1069, 1999.

[Sch06] C. Scheiderer. Sums of squares on real algebraic surfaces. *Manuscr. math*, 119:395–410, 2006.

[Sha48] C. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27, 1948.

[Sha56] C. E. Shannon. The zero-error capacity of a noisy channel. *IRE Trans. Inform. Theory*, IT-2(3):8–19, 1956.

[Shi19] Y. Shitov. Counterexamples to hedetniemi's conjecture. *Annals of Mathematics*, 2019. Preprint available at https://arxiv.org/abs/1905.02167.

[Slo19] William Slofstra. The set of quantum correlations is not closed. *Forum of Mathematics, Pi*, 7:e1, 2019.

[SSTW16] S. Severini, D. Stahlke, I. Todorov, and A. Winter. Estimating quantum chromatic numbers. *J. Funct. Anal.*, 270, 2016.

[Sta16] D. Stahlke. Quantum zero-error source-channel coding and non-commutative graph theory. *IEEE Transactions on Information Theory*, 62(1):554–577, 2016.

[SW87] Stephen J. Summers and Reinhard Werner. Maximal violation of bell's inequalities is generic in quantum field theory. *Comm. Math. Phys.*, 110(2):247–259, 1987.

[Tsi93] Boris Tsirelson. Some results and problems on quantum bell-type inequalities. *Hadronis Journal Supplement*, 8:320–331, 1993.

[Vid18] Thomas Vidick. A simplified analysis on robust self-testing of n epr pairs. Available at `http://users.cms.caltech.edu/~vidick/`, 2018.

[Vid19] Thomas Vidick. From operator algebras to complexity theory and back. *Notices of the American Mathematical Society*, 66:1, 11 2019.

[VV12] Umesh Vazirani and Thomas 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*, STOC '12, pages 61–76, New York, NY, USA, 2012. ACM.

[VV14] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014.

[Wat18] John Watrous. *The Theory of Quantum Information.* Cambridge University Press, 2018.

[WBMS15] Xingyao Wu, Jean-Daniel Bancal, Matthew Mckague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93, 2015.

[Wea17] N. Weaver. Quantum graphs as quantum relations. *https://arxiv.org/abs/1506.03892*, 2017.