University of Ottawa

Department of Mathematics

2021 Summer internship report

Non-local games and Self-testing

Author
Faouzi Al Haj Saeed

Supervisor
Phd. Arthur Mehta

September 4, 2021

Contents

Chapter 1

Introduction

1.1 Abstract

Self-testing has recently been a promising area of research in quantum information theory. It allows classical interactions with a quantum system, via non-local games, and to test that a specific entangled quantum state was used and a specific set of measurements were performed. Self-testing has also contributions to some remarkable results in complexity theory. In this report, we review the connection between non-local games, their Sum of squares (SOS) certifications and self-testing of certain groups. We introduce the idea of an SOS proof for a game and show what results it can give that may lead to self-testing.

1.2 Introduction

As stated in the abstract, we explore self-testing via non-local games and their SOS certificates. We start by introducing some of quantum information basics, in Chapter 2, following [1] and [2]. In chapter 3 we introduce non-local games. We provide a definition for a non-local game and describe the types of strategies the players can follow to win the game. We allude to 2 main examples of non local games, CHSH game [3] in Section 3.3, magic square [4] in Section 3.4.1. We provide a detailed analysis for both of these games. In Section 3.5, we introduce some algebra and group theory notions that are essential to the understanding of self-testing, we provide definitions and examples. In chapter 4, we introduce the idea of SOS proof for a game and how to conclude self-testing for certain groups. We treat the two examples introduced in Chapter 3 in detail. We provide the SOS proof and apply the condition that the players are playing optimally, this will lead to certain relations restricting the players' operators.

These restrictions describe a representation for a certain group. Having the players playing optimally if and only if their operators give a representation for a group, is a self-test for that group.

Chapter 2

Quantum Information Theory

In this chapter we introduce some of the fundamentals notions in quantum information theory that are crucial to inderstanding non-local games. The material is inspired by Henry Yuen's course notes [1] and Vern Paulsen's course notes [2].

2.1 Quantum states and Dirac Notation

In quantum information theory (QIT), we look at states as vectors of norm 1 in a complex vector space equipped with an inner product, generally called a Hilbert space.

Example 2.1.1 *Consider the vector space $\mathbb{C}^d$ of dimension d. We let $\{|0\rangle, |1\rangle, ..., |d\rangle\}$ be an orthonormal basis for $\mathbb{C}^d$. Then, a state $|\Phi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix}$ can be written as a linear combination of the basis vectors in the following $|\Phi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + ... + \alpha_d |d\rangle$. Where $\sum_{i=1}^{d} |\alpha_i|^2 = 1$.*

We call $|\psi\rangle$ a ket vector or a column vector. Note that the vecor space need not to be finite-dimensional, it can be infinite-dimensional.

The Dual/Hermitian conjugate of $|\psi\rangle$ is the vector $\langle\psi|$ such that if $|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ then $\langle\psi| = (\alpha^*, \beta^*) = \alpha^* \langle 0| + \beta^* \langle 1|$ where $\langle 0|, \langle 1|$ are row vectors and α^*, β^* are complex conjugates of α, β respectively.
$\langle\psi|$ is called a bra vector or a row vector

Definition 2.1.2 *(Inner Product)*
Let V be a vector space over a field F. An inner product is a function

$$\langle\cdot|\cdot\rangle : V \times V \to F$$

We define the inner product in the natural way. If $|\psi\rangle = \begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_d\end{pmatrix}$ *and* $|\phi\rangle = \begin{pmatrix}\beta_1\\ \vdots\\ \beta_d\end{pmatrix}$

then $\langle\phi|\psi\rangle = \alpha_1\beta_1^* + ... + \alpha_d\beta_d^*$
We note that the inner product on this vector space is a norm.

Definition 2.1.3 *(Outer Product)*
The outer product of two vectors is a matrix. It is defined in the following way:

$$|\psi\rangle = \begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_d\end{pmatrix}, |\phi\rangle = \begin{pmatrix}\beta_1\\ \vdots\\ \beta_d\end{pmatrix} \implies |\psi\rangle\langle\phi| = \begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_d\end{pmatrix}\begin{pmatrix}\beta_1^* & ... & \beta_d^*\end{pmatrix} = \begin{pmatrix}\alpha_1\beta_1^* & ... & \alpha_d\beta_1^*\\ \vdots & ... & \vdots\\ \alpha_1\beta_d^* & ... & \alpha_d\beta_d^*\end{pmatrix}$$

Where $|\psi\rangle, |\phi\rangle \in \mathbb{C}^d$.
We can take the Hermitian conjugate of an outer product: $(|\psi\rangle\langle\phi|)^\dagger = |\phi\rangle\langle\psi|$

2.2 Composite Quantum States And Tensor Products:

Tensor products are a way of taking two vector spaces and building a bigger one. For example let V and W be two complex vector spaces such that:
$\{|v_1\rangle, .. |v_r\rangle\}$ an orthogonal basis for V.
$\{|w_1\rangle, ..., |w_s\rangle\}$ an orthogonal basis for W.
Then $V \bigotimes W$ denotes the tensor product space with dimension $r \times s$ with orthogonal basis

$$\{|v_i\rangle \otimes |w_j\rangle\}_{1\leq i\leq r,\ 1\leq j\leq s}$$

Every vector $|\psi\rangle \in V \bigotimes W$ can be written as a linear combination:

$$|\psi\rangle = \sum_{i,j} \alpha_{ij} |v_i\rangle |w_j\rangle$$

Example 2.2.1 $|\psi\rangle = |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle \ \in \mathbb{C}^2 \bigotimes \mathbb{C}^2$ *is a vector in the tensor product.*

We can write vectors of tensor products more compactly in the following way: $|a\rangle \otimes |b\rangle = |ab\rangle$
Here are some of the properties of Tensor products: $\alpha(|v\rangle \otimes |W\rangle) = |\alpha v\rangle \otimes |w\rangle = |v\rangle \otimes |\alpha w\rangle$
$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$
Inner Product in $V \bigotimes W$:
The inner product is defined in the following way:

$$(\langle v_k| \otimes \langle w_l|)(|v_i\rangle \otimes |w_k\rangle) = \langle v_k|v_i\rangle \otimes \langle w_l|w_k\rangle$$

Operators in $V \bigotimes W$:
Let A be a linear operator on V, and B a linear operator on W. Then $A \otimes B$ is a linear operator on $V \bigotimes W$ where

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A\,|v\rangle \otimes B\,|w\rangle$$

Hermitian conjugate complex conjugate and Transpose:
$(A \otimes B)^* = A^* \otimes B^*, \ \ (A \otimes B)^T = A^T \otimes B^T, \ \ (A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$

Qubits:
A qubit's state lives in the two dimensional vector space $\mathbb{C}^2$, also called the Hilbert space. The hilbert space of 2 qubits is the tensor product $\mathbb{C}^2 \bigotimes \mathbb{C}^2$ which is Isomorphic to $\mathbb{C}^4$. $\mathbb{C}^2$ has an orthonormal basis $\{|0\rangle, |1\rangle\}$. Thus the basis for $\mathbb{C}^2 \bigotimes \mathbb{C}^2$ is:

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

The basis represents the classical states of 2 qubits.
In general a 2-qubit state is a unit vector in the tensor product $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$|\psi\rangle = \sum_{i,j} \alpha_{ij}\,|i\rangle \otimes |j\rangle \quad \sum_{i,j} |\alpha_{ij}|^2 = 1$$

Example: $|\psi\rangle = \frac{1}{\sqrt{3}}\,|00\rangle + \frac{1}{\sqrt{3}}\,|10\rangle + \frac{1}{\sqrt{3}}\,|11\rangle$
One of the most important 2-qubit states is the EPR state which we denote $|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ which was raised by the EPR paradox and which we will raise again in following chapters.

Measurements on 2-qubit states:
Measuring a 2-qubit state $|\psi\rangle = \sum_{i,j} \alpha_{ij}\,|i\rangle \otimes |j\rangle \ \in \mathbb{C}^2 \otimes \mathbb{C}^2$ yields a classical

outcome $(i,j) \in \{0,1\}^2$ with probability $|\alpha_{ij}|^2$. The post measurement state is $|ij\rangle$.
We can perform a measurement on the first qubit only, that is called a partial measurement. We get an outcome $i \in \{0,1\}$ with probability $p_i = \sum_j |\alpha_{i,j}|^2$. The post-measurement state conditioned on the outcome i is:

$$|\psi\rangle = \frac{1}{\sqrt{p_i}} |i\rangle \otimes \sum_j \alpha_{ij} |j\rangle$$

Example 2.2.2 *Let* $|\psi\rangle = \frac{1}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}}|10\rangle + \frac{1}{\sqrt{3}}|11\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$. *If we measure the 2-qubit state we have the same probability to get the outcomes* $|00\rangle, |10\rangle, |11\rangle$ *which is* $p = \frac{1}{3}$.
Performing a partial measurement on the first qubit will yield an outcome $|00\rangle$ *with probability* $p_0 = \frac{1}{3}$. *And we could have an the outcome* $|1\rangle$ *on the first qubit with probability* $p_1 = \frac{1}{3} + \frac{1}{3} = \frac{2}{3}$ *and the post-measurement state would be* $|\psi\rangle = \sqrt{\frac{3}{2}}|1\rangle \otimes (\frac{1}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle) = \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

2.3 Projective measurements:

states $|\psi\rangle \in \mathcal{H}$ are usually measured with respect to measurement systems.

Definition 2.3.1 *Let* $|\psi\rangle \in \mathbb{C}^d$. *An m-outcome projective measurement* $\mathcal{M}$ *is a set of matrices* $\{P_1, ..., P_m\}$ *where :*

1. $P_i \in \mathbb{C}^d \times \mathbb{C}^d$
2. $\sum_{i=1}^m P_i = I$
3. $P_i^2 = P_i$

Measuring $|\psi\rangle$ with respect to $\mathcal{M}$ yields outcome $1 \leq i \leq k$ with probability $\left\| P_i |\psi\rangle \right\|^2$ and the normalized post measurement state is $\frac{P_i|\psi\rangle}{\left\|P_i|\psi\rangle\right\|}$.
Measuring with respect to a different basis:
Measurement with respect to a basis $\{b_1, ..., b_d\}$ corresponds to projective measurements: $P_i = |b_i\rangle\langle b_i|$ and $\sum_{i=1}^k P_i = I$ where $1 \leq k \leq d$.

$$\begin{aligned}
\left\| P_i |\psi\rangle \right\|^2 &= \left\| |b_i\rangle \langle b_i| \ |\psi\rangle \right\|^2 \\
&= \left\| |b_i\rangle \langle b_i|\psi\rangle \right\|^2 \\
&= \left\| |b_i\rangle \right\|^2 \cdot \left\| \langle b_i|\psi\rangle \right\|^2 \\
&= \left\| \langle b_i|\psi\rangle \right\|^2
\end{aligned}$$

We can see from the calculation that the normalized post-measurement state is $|b_i\rangle$.

Partial measurements:
Consider $|\psi\rangle\, \mathbb{C}^m \otimes \mathbb{C}^n$ where $|\psi\rangle = \sum_{i,j} \alpha_{ij} |ij\rangle$.
If we want to measure the first qubit we get an outcome $i \in \{0, 1\}$ with probability $p_i = \sum_j |\alpha_{i,j}|^2$.
The post-measurement state conditioned on the outcome i is:

$$|\psi\rangle = \frac{1}{\sqrt{p_i}} |i\rangle \otimes \sum_j \alpha_{ij} |j\rangle$$

2.4 Pure and Mixed states

Pure states[5]
Consider two quantum systems A and B with their respective Hilbert spaces H_A and H_B. States of the composite system that can be represented in the following way $|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B$ are called separable, not entangled.
Not all states are separable, pick a basis $|i\rangle$ for H_A and a basis $|j\rangle$ for H_B then the most general state in $H_A \otimes H_B$ is of the form $|\Psi\rangle_{AB} = \sum_{i,j} c_{i,j} |i\rangle_A \otimes |j\rangle_B$.
A pure quantum state is a state which can be described by a single ket vector.

Mixed states[5]
A mixed state is a statistical ensemble of pure states.Mixed states inevitably arise from pure states when, for a composite quantum system $H_A \otimes H_B$ with an entangled state, the part H_B is inaccessible for the observer.The state of the part H_A is expressed then as the partial trace over H_B.
A mixed state can not be described by a single ket vector, instead it is represented by an associated density matrix. A density matrix can describe both a pure and a mixed state.Moreover, a mixed state on a given quantum system described by a hilbert space H can be expressed as the partial trace of a pure state on a larger bipartite system described by $H \otimes K$ for sufficiently large K. This is called purification. Mathematically the density matrix is given by

$$\rho = \sum_s p_s |\psi_s\rangle \langle\psi_s|$$

p_s is the fraction of the ensemble in each pure state $|psi_s\rangle$. One way to check if the density operator is describing a pure state or a mixed state is by checking the trace of ρ^2, if it is equal to 1 then we are dealing with a pure state, if the trace of ρ^2 is smaller than one then it is a mixed state.

Chapter 3

Non-Local games

Non-local games are of crucial importance to quantum information theory and quantum computing because they display the advantage of quantum processes over classical ones. For example, they helped solving the EPR paradox and refuted Einstein's classical model of hidden variables. They also play a role in complexity theory, as they contributed to many results in the field.

3.1 Finite input/output games

In a non-local game, two players interact with a referee, they play as a team. They agree on a strategy before the start of the game, but they are separated during the game. Each player receives a question from the referee and has to answer back. Depending on the set of questions and answers the referee decides if the players win or lose.
Formally, the definition of a non-local game is the following

Definition 3.1.1 *A non-local game is a tuple* $(I_A, I_B, O_A, O_B, \pi, v)$ *Where:*

1. I_A, I_B *are the input space for the first player (Alice) and the second player (Bob), respectively.* I_A, I_B *are finite.*
2. O_A, O_B *are the output spaces for Alice and Bob, respectively.* O_A, O_B *are finite.*
3. π *is the probability distribution on the space* $I_A \times I_B$*.*
4. $v : (I_A \times I_B \times O_A \times O_B) \to \{0, 1\}$*, a function, which is equal to 1 if Alice and Bob win, and 0 if they lose.*

3.2 Deterministic vs Quantum strategies

To play a non-local game, players agree upon a strategy before the game and follow it during the game. There are mainly 2 types of strategies, which are the following.

3.2.1 Deterministic strategies

Using a deterministic strategy we define the functions $f_A : I_A \to O_A$ for Alice and $f_B : I_B \to O_B$ for Bob.
The referee gives an input $(i, j) \in I_A \times I_B$ to the Alice and Bob. They answer with a pair $(x, y) = (f_A(i), f_B(j)) \in O_A \times O_B$. The winning probability is:

$$\omega = \sum_{i,j} \pi(i,j) v(i,j,f_A(i), f_B(j))$$

The supremum over all strategies, is the deterministic value of the game w^*.

3.2.2 Quantum strategies

A quantum strategy is given by

1. Hilbert spaces H_A, H_B for Alice and Bob, respectively.
2. a shared state $|\psi\rangle \in H_A \otimes H_B$ which is generally entangled.
3. Projective measurements $\{E_i^a\}_{a \in O_A}$ for input i for Alice and $\{F_j^b\}_{b \in O_B}$ for input j for Bob.

Alice and Bob receive inputs $(i, j) \in I_A \times I_B$ and measure their respective parts of the state $|\psi\rangle$ using $\{E_i^a\}_{a \in O_A}$ and $\{F_j^b\}_{b \in O_B}$, respectively. The probability of getting the outputs (a, b) given that the inputs are (i, j) is

$$P(a, b|i, j) = \langle \psi | E_i^a \otimes F_j^b | \psi \rangle$$

and the probability of winning is:

$$\omega = \sum_{i,j,a,b} \pi(i,j) \langle \psi | E_i^a \otimes F_j^b | \psi \rangle v(i,j,a,b)$$

The supremum over all winning probabilities is the quantum value of the game ω_q.

3.2.3 Commuting-operator strategies

A commuting operator strategy is the more general form of quantum strategies. They consist of 1 Hilbert space shared between the two players, a state $|\psi\rangle \in \mathcal{H}$, 2 collections of projective measurements, 1 for each player. Alice's and Bob's operators commute. Also, the dimension of the Hilbert space is arbitrary.

3.3 CHSH an example of a non-local game

We will examine the quantum strategy for the CHSH game[3] but first we will discuss the classical value briefly. The CHSH game is the tuple $G = (I_A, I_B, O_A, O_B, \pi, v)$ with the following characteristics:

$$I_A = I_B = \{0,1\} = O_A = O_B. \;\; \pi \text{ is Uniform} \rightarrow \pi = \frac{1}{4}$$

Let $(x, y) \in I$ the questions, $(a, b) \in O$ their answers, the condition to win is that $x \cdot y = a + b \; mod \; 2$
It is obvious that the best classical strategy Alice and Bob can work with is that they output $a = b = 0$ so they would win three out of the four times (The only scenario to lose is that if $x = y = 1$).
So, we can see that the classical value of the game $\omega(G) = 0.75$
Now if Alice and Bob use a quantum strategy then for each input, each Alice and Bob have 2 projection operators.
Alice: Input $0 \rightarrow \{P_0^0, P_0^1\}$ Input $1 \rightarrow \{P_1^0, P_1^1\}$.
Bob: Input0 $\rightarrow \{Q_0^0, Q_0^1\}$ Input $1 \rightarrow \{Q_1^0, Q_1^1\}$
Suppose that before the game starts, Alice and Bob get together in the lab and create a 2-qubit entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Alice takes one qubit and Bob takes the other one. Alice receives $x \in \{0,1\}$ and Bob receives $y \in \{0,1\}$. Depending on their questions, they perform different measurement on their respective qubits.

- If Alice receives the question 0, she will measure her qubit with respect to the basis $\{|0\rangle, |1\rangle\}$. Alice outputs 0 if the measurement result is 0, or 1 if the measurement result is 1.
- If Alice receives the question 1, she will measure her qubit with respect to the basis $\{|+\rangle, |-\rangle\}$. Where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Alice outputs 0 if the measurement result is $|+\rangle$, or is the measurement result is $|-\rangle$

- If Bob receives question 0, he will measure his qubit with respect to the basis $\{|a_0\rangle, |a_1\rangle\}$. Where $|a_0\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$ and the second vector $|a_1\rangle = -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle$.Bob outputs 0 if the measurement result is $|a_0\rangle$, or 1 if the measurement result is $|a_1\rangle$
- If Bob receives question 1, he will measure his qubit with respect to the basis $\{|b_0\rangle, |b_1\rangle\}$. Where $|b_0\rangle = \cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle$ and the second vector $|a_1\rangle = \sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle$. Bob outputs 0 if the measurement result is $|b_0\rangle$, or 1 if the measurement result is $|b_1\rangle$

The probability of winning is

$$Pr(win) = \sum_{i,j,a,b} \pi(i,j)\langle\psi|P_x^a \otimes Q_j^b|\psi\rangle v(i,j,a,b)$$

Now let's calculate this probability of winning

$$\begin{aligned}
&Pr(win) = \\
&= Pr(a=0,b=0|x=0,y=0)Pr(x=0,y=0) + Pr(a=1,b=1|x=0,y=0)Pr(x=0,y=0) \\
&+ Pr(a=0,b=0|x=1,y=0)Pr(x=1,y=0) + Pr(a=1,b=1|x=1,y=0)Pr(x=1,y=0) \\
&+ Pr(a=0,b=0|x=0,y=1)Pr(x=0,y=1) + Pr(a=1,b=1|x=0,y=1)Pr(x=0,y=1) \\
&+ Pr(a=1,b=0|x=1,y=1)Pr(x=1,y=1) + Pr(a=0,b=1|x=1,y=1)Pr(x=1,y=1)
\end{aligned}$$

We have a uniform distribution $\pi = \frac{1}{4} = Pr(x,y)\ \forall x,y$.
Let's calculate probability that Alice and Bob win when their question pair is $(x,y) = (0,0)$:

$$\begin{aligned}
Pr(a=0,b=0|x=0,y=0) &= |(\langle 0| \otimes \langle a_0|)|\psi\rangle|^2 \\
&= |(\langle 0| \otimes \langle a_0|)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|^2 \\
&= |\frac{1}{\sqrt{2}}\langle a_0|0\rangle|^2 \\
&= \frac{1}{2}\cos^2(\frac{\pi}{8})
\end{aligned}$$

Similarly:

$$\begin{aligned}
Pr(a=1,b=1|x=0,y=0) &= |(\langle 1| \otimes \langle a_1|)|\psi\rangle|^2 \\
&= |(\langle 1| \otimes \langle a_1|)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|^2 \\
&= |\frac{1}{\sqrt{2}}\langle a_1|1\rangle|^2 \\
&= \frac{1}{2}\cos^2(\frac{\pi}{8})
\end{aligned}$$

Thus, we have that $Pr(win|x=0,y=0) = \cos^2(\frac{\pi}{8})$. Similarly, we can calculate all other conditional probabilities, $Pr(a,b|x,y)$. In fact, it turns out that $Pr(win|x,y) = \cos^2(\frac{\pi}{8})$ irrespective of the question pairs (x,y). This implies that $Pr(win) = \cos^2(\frac{\pi}{8}) \approx 0.854$ which is greater than the classical value of the game. This proof is inspired by [1]
It is not possible to do better than $\cos^2(\frac{\pi}{8})$ with a quantum strategy playing CHSH. We will show this in a later chapter via a Sum of squares decomposition (SOS) from which we can conclude some relations on the players' operators that can self-test specific groups.
Thus, we can conclude from the CHSH example that quantum entanglement gives rise to correlations that can not be produced by classical randomness.

3.4 Binary constraint system games

A *linear constraint system* (LCS) is a non-local game in which Alice and Bob play with a referee to convince him that they know the solution to a linear system over $\mathbb{Z}_n$. The referee gives an equation to Alice and a variable from that equation to Bob, randomly. Alice responds by an assignment to all the variables in her equation, while Bob responds with an assignment to his variable. The two players win if Alice's assignments satisfy the equation, and Bob's assignment agrees with Alice's.
A binary constraint system games, BSC, is an LCS over Z_2. The most famous example is the magic square game [4].

3.4.1 Magic square game:

In the magic square game, we have 6 equations with 9 variables which we present:

$$x_1 + x_2 + x_3 = 0 \qquad x_1 + x_4 + x_7 = 0$$
$$x_4 + x_5 + x_6 = 0 \qquad x_2 + x_5 + x_7 = 0$$
$$x_7 + x_8 + x_9 = 0 \qquad x_3 + x_6 + x_9 = 1$$

Where the addition is over $\mathbb{Z}_2$ [4]. Classically the best winning probability is $\frac{17}{18}$. The surprising fact about this game is that it could be won, using quantum strategies, with probability 1.

3.4.2 Perfect quantum strategy

The system of equations could be equivalently written in multiplicative form. For example $x + y + z = b$ for $x, y, z, b \in \{0, 1\}$ translates to $xyz = (-1)^b$ for

$x, y, z \in \{1, -1\}$. The players also start with a higher dimensional analogue of the bell state [6]

$$|\psi\rangle = \Big(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\Big) \otimes \Big(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\Big)$$

We recall that Alice will receives an equation for which she has to provide an assignment for the free variables from $\{1, -1\}$ and Bob receives one variable for which he has to provide a value from $\{1, -1\}$. The following table shows which measurement should Alice/Bob apply depending on which equations/variables they receive.

$Z \otimes I$	$I \otimes Z$	$Z \otimes Z$
$I \otimes X$	$X \otimes I$	$X \otimes X$
$Z \otimes X$	$Z \otimes X$	$Y \otimes Y$

Where X, Y, Z are the Pauli matrices. If Alice receives row 1 as her question, she will measure her part of the state using $Z \otimes I,\ I \otimes Z,\ Z \otimes Z$. If Bob receives the top right cell as his question, he will measure his part of the state using $Z \otimes Z$. Since all the matrices have eigen values $\in \{1, -1\}$ Alice's and Bob's measurements will yield the outcomes $\{1, -1\}$.
It is important to note that Z, I, X are unitaries and not operator. Hence, the measurement that we are doing is on the space spanned by the eigenvectors of the unitary that we use in the measurement.
Why does this work? Suppose Alice receives row 1, then she measures with $Z \otimes I,\ I \otimes Z,\ Z \otimes Z$ obtaining 3 values from the set $\{1, -1\}$ the expected value of the product of these is given by

$$Tr((Z \otimes I)(\ I \otimes Z)(\ Z \otimes Z)|\psi\rangle\langle\psi|) = Tr((I \otimes I)|\psi\rangle\langle\psi|) = 1$$

Hence, Alice *always* outputs the value 1 whenever she is asked to whenever she is asked row 1. We could verify in a similar fashion that Alice always outputs 1 whenever she is asked any of the rows and the first two columns and -1 whenever she is asked the last column. This means that she always gives the correct answer.
What about Bob? By our definition of the operators, Bob *always* measures with the same operator as Alice. They will perform the same measurement. Here we use a fact which is that
For $|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$ and any observable A, we have that $(I \otimes A)|\psi\rangle = (I \otimes A^T)|\psi\rangle$.
Using this face the expected value of the product of Alice's and Bob's measurement of every cell is equal to 1. Thus, the players win every time they play the game.
We will introduce an SOS decomposition for the magic square game which will lead to self-testing the "Solution group" section 4.3.

3.5 Algebra

In order to understand more about non-local games, we need to define and understand some algebraic notions related to the next chapter.
First we start by defining the free group

Definition 3.5.1 *Let S be a set. F_S a free group, is the group that consists of "words" built from elements of S. The associated operation is concatenation[7].*

Example 3.5.2 *In this example we construct a free group F_s with free generating set S. S is a set of symbols and we suppose that $\forall s \in S \ \exists \ s^{-1}$ an "inverse" symbol for s in a set S^{-1}.*
Let $T = S \cup S^{-1}$, and define a word in S to be any written product of elements of T. The empty word is the word with no symbols.
For example let $S = \{a, b, c\}$ then $T = \{a, b, c, a^{-1}, b^{-1}, c^{-1}\}$ so a^2cb^{-1} is a word in S. If an element is immediately next to its inverse, the word can be simplified by eliminating the pair. The free group F_s is defined to be the group of all reduced words in S. Concatenation is the group operation.

Secondly, we briefly introduce the group presentation.
Let S be a generating set and R be a set of relations. Formally, a group G has the presentation $G =< S|R >$ if it is isomorphic to the quotient of the free group generated by S (i.e F_s) by the smallest subgroup of F_s containing R.

Example 3.5.3 *The cyclic group of order n has a presentation $G =< a|a^n = e >$ where e is the identity [8].*
$\mathbb{Z} \times \mathbb{Z} =< x, y|xy = yx >$*[8].*
$\mathbb{Z}/_n\mathbb{Z} \times \mathbb{Z}/_m\mathbb{Z} =< x, y|x^n, x^m, xy = yx >$*[8].*
The Dihedral group D_{2n}, where n is odd has presentation

$$D_{2n} \coloneqq < a, x|a^n = x^2 = e, xax = a^{-1} >$$

Next, we look at the free product of two (or more) groups.

Definition 3.5.4 *Let G, H be two groups. $G * H$, the free product, is the group that contains G and H as subgroups and generated by the elements of these subgroups.*
We can also look at the free product as the group whose elements are the words in G and H, under the operation of concatenation[9].

If $s_1 s_2 ... s_n$ is a word with $s_i \in G \cup H$ then a reduced word in G and H is of the form $g_1 h_1 g_2 h_2 ... g_k h_k$ where $g_i \in G$, $h_i \in H$. The free product $G * H$ is the

group whose elements are the reduced words in G and H, under the operation of concatenation.
In terms of group presentations, we can conclude the presentation of a free product of two groups in the following manner.
If $G =< S_G|R_G >$ and $H =< S_H|R_H >$, then $G * H =< S_G \cup S_H|R_G \cup R_H >$.

Finally, and most importantly, we look at group representations

Definition 3.5.5 *A representation of a group G over a vector space V of dimension n over a field K is a map*

$$\rho : G \to GL(V)$$

such that $\rho(g_1g_2) = \rho(g_1)\rho(g_2)\ \forall g_1, g_2 \in G$, i.e ρ is a homomorphism [10].

Where $GL(V)$ is the general linear group of V which is the set of $n \times n$ invertible matrices, together with the operation of matrix multiplication. This forms a group.

Example 3.5.6 *Consider the complex number $e^{\frac{2\pi i}{3}}$ which has the property $u^3 = 1$. The cyclic group $C_3 = \{1, u, u^2\}$ has a representation ρ on $\mathbb{C}^2$ given by*

$$\rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \rho(u) = \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix} \quad \rho(u^2) = \begin{pmatrix} 1 & 0 \\ 0 & u^2 \end{pmatrix}$$

Group representations are not unique, we can have the representation τ for the previous example [10], such that

$$\tau(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \tau(u) = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \quad \tau(u^2) = \begin{pmatrix} u^2 & 0 \\ 0 & 1 \end{pmatrix}$$

We also mention a specific type of representations, an irreducible representation. Let ρ be a representation of a group G on a vector space V. A linear subspace $W \subset V$ is called G-invariant if $\rho(g)w \in W$ for all $g \in G$ and all $w \in W$. The co-restriction of ρ to the general linear group of a G-invariant subspace is known as a subrepresentation.

Definition 3.5.7 *Let $\rho : G \to GL(V)$ where V is a vector space over a field F. ρ is said to be irreducible if it has only trivial subrepresentations. Meaning that the only $G-$invariant subspaces of V are V and $\{0\}$. Otherwise, ρ is reducible.*

Example 3.5.6 is an example of a reducible representation.
An example of an irreducible representation would be the representation of $\mathbb{Z}_n$ is the map that sends $1 \to n$-th root if unity.

3.6 Projections, unitaries

Let $G = (I_A, I_B, O_A, O_B, \pi, v)$ be a non-local game. P is a commuting operator strategy if there exists a tuple $(H, |\psi\rangle, P_x^a, Q_y^b)$ where H is a Hilbert space $|\psi\rangle \in H$ is a unit vector and $\{P_x^a\}, \{Q_y^b\}$ are projections such that :

1. $\sum_a P_x^a = I. \;\; x \in I_A$
2. $\sum_b Q_y^b = I. \;\; y \in I_B$
3. $P_x^a Q_y^b = Q_y^b P_x^a$ Alice's and Bob's operators commute.
4. $P(a, b|x, y) = \langle P_x^a Q_y^b \psi | \psi \rangle$

For each input for Alice and Bob we can construct a unitary operator. If $|I_A| = n$ and $|O_A| = m$. We label $I_A = \{0, 1, 2, .., n-1\}$ and $O_A = \{0, 1, ..., m-1\}$. If we let $\omega = e^{\frac{2\pi i}{m}}$ then we can define the order m unitary in the following way:

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

The collection of n such unitaries defines a representation for the group

$$\mathbb{F}(n, m) := Z_m * Z_m * ... * Z_m$$

where this group is the free product of n copies of order m groups. We can see that $\{U_i\}_{i=1}^n$ gives a representation for $\mathbb{F}(n, m)$ in the following way:
Consider the presentation of $\mathbb{F}(n, m) =< z_1, z_2, ..., z_n | z_1^m, z_2^m, ..., z_n^{m>}$, then we know that $\{U_i\}_{i=1}^n$ are order m unitaries. So it follows naturally that there is a homomorphism : $\mathbb{F}(n, m) \to \{U_i\}_{i=1}^n$, i.e this is a representation for $\mathbb{F}(n, m)$.
Similarly for Bob, if $|I_B| = r$ and $|O_B| = s$ we can define the unitaries

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

Where $\mu = e^{\frac{2\pi i}{s}}$.
The collection $\{U_x, V_y\}$ defines a unitary representation for $\mathbb{F}(n, m) \times \mathbb{F}(r, s)$. We can work the other way, where we define projections starting from unitaries. This is done in similar fashion.
For each $x \in I$ we have the unitary $U_x \in \mathbb{C}[\mathbb{F}(n, m)]$ such that $U_x^m = 1$. If we set $\omega = e^{\frac{2i\pi}{m}}$, then the set of eigenvalues of each U_x is $\{\omega^a \;\; : 0 \leq a \leq m-1\}$. The orthogonal projection onto the eigenspace corresponding to ω^a is defined as

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

A similar reasoning gives Bob's projections:

$$Q_y^b \coloneqq \frac{1}{s}\sum_{k=0}^{m-1}(\mu^{-b}V_y)^k$$

Where $\mu = e^{\frac{2i\pi}{s}}$.

3.7 Commuting strategies and representations

If $G = (I_A, I_B, O_A, O_B, \pi, v)$ is a non-local game and $P = P(a,b|x,y)$ a strategy the probability of winning is

$$\omega_p = \sum_{x,y,a,b} v(x,y,a,b)\pi(x,y)P(x,y|a,b)$$

The commuting operator value of the game is the supremum over all commuting operator strategies. For each game we can define an element of the group algebra $\mathbb{C}[\mathbb{F}(n,m)\times\mathbb{F}(r,s)]$ which we call *the game polynomial* f_G defined by:

$$f_G \coloneqq \sum_{x,y,a,b} v(x,y,a,b)\pi(x,y)P_x^aQ_y^b \quad \in \mathbb{C}[\mathbb{F}(n,m)\times\mathbb{F}(r,s)]$$

We can obtain the following result using the correspondence between commuting operator strategies and unitary representations of the associated groups.

Theorem 3.7.1 *Given a non-local game $G = (I_A, I_B, O_A, O_B, \pi, v)$, λ is an upper bound for the commuting operator value of the game if for all unitary representations, π of $\mathbb{C}[\mathbb{F}(n,m)\times\mathbb{F}(r,s)]$, we have that $\pi(\lambda I - f_G)$ is a positive semi-definite operator.[11]*

Proof:
Let G be a non-local game, P a commuting operator strategy for G. If P is a commuting operator strategy, then π is some unitary representation.
Suppose $\pi(\lambda I - f_G)$ is a positive-semi definite operator. Then $\forall\,|\psi\rangle \in H$ we have that

$$\begin{aligned}\langle\psi|\pi(\lambda I - f_G)|\psi\rangle &\geq 0\\ \rightarrow \langle\psi|\lambda I - f_G|\psi\rangle &\geq 0\\ \rightarrow \langle\psi|\lambda I|\psi\rangle &\geq \langle|\psi f_g|\psi\rangle\\ \lambda &\geq \omega_p\end{aligned}$$

The first step is justified because π is a unitary representation.
Hence, we have that $\lambda \geq \omega_p \ \forall \, |\psi\rangle \in H$ where ω_p is the probability of winning the game using the strategy P. Hence, λ is an upper bound for the commuting operator value of the game.
Now let's assume that λ is an upper bound for the commuting operator value of the game. Then we have that

$$\begin{aligned} \langle\psi|\lambda I|\psi\rangle &\geq \langle\psi|f_g|\psi\rangle \ \forall \, |\psi\rangle \in H \\ \langle\psi|\lambda I - f_G|\psi\rangle &\geq 0 \\ \langle\psi|\pi(\lambda I - f_G)|\psi\rangle \ \forall \, |\psi\rangle &\in H \end{aligned}$$

Then we have, by definition, that $\pi(\lambda I - f_G)$ is a positive semi-definite operator. Which completes the proof.

Let M be an $n \times n$ Hermitian self-adjoint complex matrix. Then we have that :

$$M \text{ is positive semi-definite} \iff x^* M x \geq 0 \ \forall x \in \mathbb{C}^n$$

We can also define it in terms of eigenvalues. Recall that if a matrix is Hermitian then all of its eigenvalues are real. Let M be an $n \times n$ Hermitian matrix, then M is positive semi-definite if and only if all of its eigenvalues are non-negative. A natural question to ask is that if λ is the commuting operator value for a game $\mathcal{G}$, then is $\lambda I - f_G$ necessarily expressible as a sum of hermitian squares? We propose this as a conjecture.[11]

Conjecture 3.7.2 *Given a non-local game $G = (I_A, I_B, O_A, O_B, \pi, v)$, λ is an upper bound for the commuting operator value of the game if and only if $\lambda I - f_G$ can be written as a sum of hermitian squares.*

It is worth mentioning that we can ask the same question for λ a *strict* upper bound for the commuting operator strategy. And the answer is, actually, yes. Hence, we have the following theorem from [11].

Theorem 3.7.3 *Given a non-local game $\mathcal{G}$, λ is a strict upper bound for the commuting operator value of the game if and only if $\lambda I - f_G$ is expressible as a sum of hermitian squares.*

The proof of Theorem 3.7.3 is beyond the scope of this report.

Chapter 4

Self-testing and SOS proofs

In this chapter, we look at the SOS method for the CHSH and Magic square games. We will show their respective upper bounds for the quantum values of the game. We will also explore the connection between SOS and self-testing, and how the former leads to the latter.

4.1 CHSH's SOS example

We remind the reader that the CHSH has the following characteristics:

$$I_A = I_B = \{0,1\} \;\; \pi \text{ is uniform} \rightarrow \pi = \frac{1}{4}$$

We define the following unitaries $A_{0,1}$ for Alice and $B_{0,1}$ for Bob such that:

$$A_0 = P_0^0 - P_0^1 \qquad A_1 = P_1^0 - P_1^1 \tag{4.1.1}$$

$$B_0 = Q_0^0 - Q_0^1 \qquad B_0 = Q_1^0 - Q_1^1 \tag{4.1.2}$$

And we consider the bias $P' = A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1$. We can conclude the probability of winning from the bias since:

$$\langle\psi|P'|\psi\rangle = 4[2(P_{win} - P_{lose})] = 8\omega - 4$$

Using the sum of squares proof [11] we can show that the commuting operator value for the CHSH game is $\frac{1}{4}(\sqrt{2}+2)$ since:

$$2\sqrt{2}I - (A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1) = \frac{\sqrt{2}}{4}(A_0 + A_1 - \sqrt{2}B_0)^2 + \frac{\sqrt{2}}{4}(A_0 - A_1 - \sqrt{2}B_1)^2 \geq 0 \tag{4.1.3}$$

Thus we see that $2\sqrt{2}$ is an upper bound for the bias which means that

$$8\omega - 4 \leq 2\sqrt{2} \implies \omega \leq \frac{1}{4}(\sqrt{2} - 2) \approx 0.854$$

This SOS line shows that $\cos^2 \frac{\pi}{8} \approx 0.854$ is actually the best Alice and Bob can do using a quantum commuting-operator strategy.
An interesting fact is that for the CHSH game there is a unique state and set of operators that Alice and Bob can use to win the game optimally. The SOS decomposition can be used to show this fact. If this upper bound is saturated with the state ψ then we get that

$$\Big[\frac{\sqrt{2}}{4}(A_0 + A_1 - \sqrt{2}B_0)^2 + \frac{\sqrt{2}}{4}(A_0 - A_1 - \sqrt{2}B_1)^2\Big] |\psi\rangle = 0$$

which implies that

$$(A_0 + A_1 - \sqrt{2}B_0) |\psi\rangle = 0 \quad \text{, and} \quad (A_0 - A_1 - \sqrt{2}B_1) |\psi\rangle = 0 \tag{4.1.4}$$

Thus we have that

$$B_0 |\psi\rangle = \frac{1}{\sqrt{2}}(A_0 + A_1) |\psi\rangle \quad \text{, and} \quad B_1 |\psi\rangle = \frac{1}{\sqrt{2}}(A_0 - A_1) |\psi\rangle \tag{4.1.5}$$

Using the identities 4.1.5 we can conclude that B_0 and B_1 anti-commute in the following way:

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

Thus B_0 and B_1 anti-commute, that is $B_0B_1 = -B_1B_0 \iff (B_0B_1)^2 = -I$, with respect to a semi-norm induced by $|\psi\rangle$ Similarly we can get from identities (3.1.4) that

$$A_0 |\psi\rangle = \frac{1}{\sqrt{2}}(B_0 + B_1) |\psi\rangle \quad \text{, and} \quad A_1 |\psi\rangle = \frac{1}{\sqrt{2}}(B_0 - B_1) |\psi\rangle \tag{4.1.6}$$

And by similar computation and using 4.1.6 we get that $(A_0A_1)^2 = -I$.
Now let's consider the group

$$M =< X, Y, J | X^2, Y^2, J^2, J(YX)^2, JXJ^{-1}X^{-1}, JYJ^{-1}Y^{-1} > \tag{4.1.7}$$

Keeping in mind that A_0, A_1 are order 2 unitaries and that they anti-commute. Then, when Alice and Bob are playing optimally (meaning that they are using $A_0, A_1, B_0, B_1, |\psi\rangle$ that win the game with probability $\cos^2 \frac{\pi}{8}$), we can define a

map $(X, Y, J) \to (A_0, A_1, -I)$. This map determines what we call a $|\psi\rangle$ representation.
A $|\psi\rangle$ representation can be thought of as a representation of G in the usual sense. If we let $\mathcal{K}$ the subspace of H that is generated by words in A_0, A_1 applied on $|\psi\rangle$, then the map $(X, Y, J) \to (A_0|_{\mathcal{K}}, A_1|_{\mathcal{K}}, -I)$ determines a representation of M on $\mathcal{K}$.
Similarly, a map $(X, Y, J) \to (B_0|_{\mathcal{K}}, B_1|_{\mathcal{K}}, -I)$ determines a representation of M on $\mathcal{K}$. Since Bob's operators are also order 2 unitaries, and they anti-commute.
To explain in detail how this map defines a representation for the group M, let's look at the relations in the presentation of the group M 4.1.7.
If we denote the map, which is a homomorphism, $\rho : (X, Y, J) \to (A_0|_{\mathcal{K}}, A_1|_{\mathcal{K}}, -I)$ then The first 3 relations $X^2 = Y^2 = J^2 = I$ tell us that

$$\rho^2(X) = \rho^2(Y) = \rho^2(J) = I^2 = I$$

Which is the case for $(A_0|_{\mathcal{K}}, A_1|_{\mathcal{K}}, -I)$.
Furthermore, The second relation tells us that $\rho(J(YX)^2) = \rho(J)\rho^2(Y)\rho^2(X) = I$ which is exactly the anti-commutation relation for Alice and Bob's operators.
As for the last two relations in 4.1.7, The are just telling us that Alice and Bob's operators commute with $\rho(J) = -I$. Hence, we can conclude that ρ determines a $|\psi\rangle$-representation for M, or just a representation of M on $\mathcal{K}$.
One detail to note, is that there is a specific entangled state that Alice and Bob have to use if they want to win the game optimally. It turns out that this state is the eigenstate of the matrix in the LHS of 4.1.3.

To summarize the above discussion, the SOS proof leads to the conclusion that if Alice and Bob want to win a game optimally then they are highly constrained in terms of the strategy they want to use. First of all, they need to use a quantum strategy, and this quantum strategy consists of a unique shared entangled state with a unique set of measurement operators. Outstandingly, exchanging classical information (questions (x, y) and answers (a, b)) through a game between two players and a referee is sufficient to determine all the information above. These constraints on the players' operators and the shared state lead to relations that can describe a $|\psi\rangle$-representation for some groups, which is a self-test for these groups.

4.2 SOS proof theory

As we have seen in the previous section, SOS proofs are powerful in the sense that they are a 1 line proof that give an upper bound for the quantum value of a game. Secondly, they give a way to self-test a group and determine the constraints on which Alice and Bob have to play in order to win the game with optimal quantum value.

Definition 4.2.1 *We say a non-local game G is a self-test for a group $\mathcal{G}$ if*

the playing with an optimal quantum strategy is equivalent to Alice and Bob's operators determining a representation for $\mathcal{G}$

Consider we have a game G, then to determine an upper bound for commuting-operator value and find a self-test we proceed as follows :

1. Determine the "game polynomial", f_G, and the suspected commuting-operator value of the game, λ.
2. Find an SOS decomposition $\lambda I - f_G$ if it exists.
3. Apply the decomposition on $|\psi\rangle$ and set the decomposition equal to 0 (This is to say that the players are playing optimally).
4. Each term in the sum will be equal to 0, this will give certain relations on the players' operators.
5. Determine the group for which the players' operators determine a representation, then the game is a self-test for that group (if it exists).

In next section we explore another example of a non-local game, the magic square game. We will show the SOS decomposition for this game and find relations on the operators that Alice and Bob have to use to win optimally.

4.3 SOS proof for Magic square

In this section, we present the SOS proof [11] for the magic square game over $\mathbb{Z}_2$. We will consider a strategy with a state $|\psi\rangle \in H$, where H is a Hilbert space shared by Alice and Bob, and a set of commuting measurement systems $\{E_{i,x}\}$ and $\{F_{j,y}\}$.
Consider a system of linear equations $Ax = b$ where $A \in \mathbb{Z}_n^{r\times s}$ and $b \in \mathbb{Z}_n^r$. Let V_i be the set of variables occurring in equation i:

$$V_i = \{j \in [s] : \ a_{ij} \neq 0\}$$

Using this notation we can define the following set 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 that $A_j^{(i)}$ 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 satifsy the following identities:

$$\sum_{x:x\in S_i} E_{i,x} = \frac{1}{2}(I + (-1)^b \prod_{k\in V_i})A_k^{(i)} \tag{4.3.1}$$

$$\sum_{x:y=x_j} E_{i,x} = \frac{1}{2}(I + yA_j^{(i)}) \tag{4.3.2}$$

Using the identities above we can now find an SOS decomposition in the following way:

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

which implies that 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 when the following identities hold for all i and $j \in V_i$:

$$B_j\,|\psi\rangle = A_j^{(i)}\,|\psi\rangle \tag{4.3.3}$$

$$|\psi\rangle = (-1)^{b_i}\prod_{k\in V_i} A_k^{(i)}\,|\psi\rangle \tag{4.3.4}$$

Identities (3.3.3) and (3.3.4) can be used to determine a $|\psi\rangle$-representation for the "solution group" of the linear system for this game. We will explore the solution group and how to relate the identities that resulted from the SOS decomposition to it.

4.4 Perfect commuting operator strategies for BCS games

In this section we will define what operator solutions[6] are, what the solution group is and what is the relationship between these concepts and perfect com-

muting operator strategies.
A vector $x \in \{\pm 1\}^n$ satisfies the equation number l if and only if

$$x_1^{M_{l,1}} x_2^{M_{l,2}} ... x_n^{M_{l,n}} = (-1)^{b_l}$$

The equation l could be equivalently written in the form

$$x_{k_1}, ... x_{k_n} = (-1)^{b_l}$$

where $V_l = \{k_1, ..., k_r\} = \{1 \leq k \leq n \ : \ M_{l,k} = 1\}$ is the set of indices of variables in equation l.

Definition 4.4.1 *[6] An operator solution to a binary linear system $Mx = b$ is a sequence of bounded self-adjoint operators $A_1, ..., A_n$ on a Hilbert space $\mathcal{H}$ such that:*

1. $A_i^2 = I \ \ \forall \ 1 \leq i \leq n$
2. *If x_i, x_j two variables such that $i, j \in V_l \quad 1 \leq l \leq n$ then A_i and A_j commute.*
3. *For each equation of the form $x_{k_1} ... x_{k_r} = (-1)^{b_l}$ the operators satisfy $A_{k_1} ... A_{k_r} = (-1)^{b_l} I$.*

Definition 4.4.2 *[6] The solution group of a binary linear system $Mx = b$ is the group Γ generated by $g_1, ..., g_n$ and J satisfying the following relations:*

1. $J^2 = e$ *and* $g_i^2 = e$ *for all* $1 \leq i \leq n$.
2. $[g_i, J] = e$ *or all* $1 \leq i \leq n$ *(J commutes with each generator).*
3. *If $i, j \in V_l$ for some l then g_i, g_j commute.*
4. $g_1^{M_{l,1}} ... g_n^{M_{l,n}} = J^{b_l}$ *for all* $1 \leq l \leq m$.

Definition 4.4.3 *[6] Let $mx = b$ be an $m \times n$ system. A commuting operator strategy for the system consists of a Hilbert space $\mathcal{H}$ a state $|\psi\rangle \in \mathcal{H}$, 2 collections $\{A_i^l, \ 1 \leq l \leq m, \ 1 \leq i \leq n\}$ and $\{B_j, \ 1 \leq j \leq n\}$ of self-adjoint operators such that:*

1. $(A_i^l)^2 = (B_j)^2 = I$ *for all* $1 \leq l \leq m \ \ i \in V_l$ *and* $1 \leq j \leq n$.
2. $A_i^l B_j = B_k A_i^l$ *for all* l, i, j.
3. $A_j^l = A_i^l \ \forall \ 1 \leq l \leq m$ *and* $i, j \in V_l$.

Theorem 4.4.4 *Let $Mx = b$ be a linear system. The following are equivalent:*

1. *There is a perfect commuting operator strategy for the non-local game associated with $Mx = b$.*
2. *There is an operator solution for $Mx = b$.*
3. *The solution group for $Mx = b$ has the property that $J \neq e$.*

The full proof of the theorem can be found in [6]. But for our purpose of self-testing, we are only interested in the implication $2 \implies 3$ in Theorem4.4.4.
From [6] proposition 7, we have that a commuting-operator strategy $(\mathcal{H}, |\psi\rangle, \{A_i^l\}, \{B_j\})$ is perfect if and only if:

- $A_i^l |\psi\rangle = B_j |\psi\rangle$ for all $1 \leq l \leq m$ and all $i \in V_l$.
- $\prod_{i \in V_l} |\psi\rangle = (-1)^{b_l} |\psi\rangle$ for all $1 \leq l \leq m$.

These are the exact same identities that we had at the end of the last section, 4.3.3 and 4.3.4.
By definitions 4.4.1 and 4.4.2, since $Mx = b$ has an operator solution $A_1, ..., A_n$, then we can define a map ρ sending

$$g_i \to A_i, \ 1 \leq i \leq n \text{ and } \ J \to -I$$

Which is a representation of the solution group with $\rho(J) \neq I$. It follows that $J \neq e$ in the solution group.

Acknowledgements

I would like thank and acknowledge Arthur Mehta for supervising me through this summer project, and helping me understand the concepts presented in this report and guiding me through the writing of this report. I thank Dr. Anne Broadbent for providing the opportunity to work with her group this summer, and for supervising me.

This work would not have been possible without the help of Mitacs and the government of Canada which funded the work through "Early Researcher Award".

To my late grand father, Mekideche Omar, who passed away earlier this year.

Bibliography

[1] Henry Yuen's Introduction to Quantum Computing COMS4281.

[2] Vern Paulsen's Entanglement and Non-locality PMATH990/QIC890.

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

[4] Quantum pseudo-telepathy-Wikipedia

[5] Quantum state-Wikipedia

[6] Rcihard Cleve, Li Liu and William Slofstra. Perfect commuting-operator strategies for linar system games. *Journal of Mathematics Physics*,58(012202),2017.

[7] The Free Group-Wikipedia

[8] Presentation of a Group-Wikipedia

[9] Free Product-Wikipedia

[10] Group Representation-Wikipedia

[11] Arthur Mehta-Entanglement and Non-Locality in Games and Graphs.2021