UNIVERSITY OF COPENHAGEN
FACULTY OF SCIENCE

PUK Report

David Rasmussen Lolck <zgk438@alumni.ku.dk>

The Role of Classical Randomness in Self-Testing

Supervisor: Laura Mancinska

Pages: 30. Handed in: January 21, 2022

Contents

1 Introduction

As the capabilities of quantum computers grow, so does the interest in them. Quantum computers gives access to a different model of computation than our standard classical one. It is known that the commonly accepted model of quantum computation is capable of simulating the classical one, but whether the classical model is capable of simulating the quantum model of computation efficiently is an open problem [NC10]. While the fact that we are looking at a possibly superior model of computation is interesting in and of itself, this is further increased by the fact that multiple algorithms exists exclusively for quantum computers.

The most famous example of an quantum algorithm is Shor's algorithm, which is a randomized algorithm that efficiently solves the problems of factoring large integers [Sho97], a problem that is the basis of the RSA encryption. Another example is Grover's algorithm, which can perform a search over an unstructured search space in $O(\sqrt{N})$ [Gro96].

Both Shor's algorithm and Grover's algorithms are examples where it is easy to verify the correctness of the result. In Shor's algorithm you can simply check for divisibility with the computed factors, while Grover's algorithm return an element that corresponds to some search criteria.

It is however not always the case that solutions are easy to check for computational problems. Some types of problems does not have a easy way of verification. This could for example be some optimisation problems since you might not be able verify that a solution is optimal without recomputing the solution.

This problem of verification further compounds in the quantum case. When verifying a solution that is the result of some quantum computation, we might not even have access to a quantum computer. It is not far fetched to imagine not to have access to a quantum computer and instead having someone else

perform the calculation. But how can you trust the computation was done correctly if you aren't even able to validate just some of the results.

Say someone come to you and say they have prepared some quantum state as well as some way to measure this state. How would you be able to actually trust and verify this claim? It might be possible to go through the apparatus used to generate this state. It might be possible to check that the physical implementations correspond to the theoretical ones but this quickly becomes unreasonable for a non-expert third party.

This is where the concept of self-testing comes in. The idea is that to perform an experiment where we use the apparatus as a black box. It might then possible to check that the output of the experiment corresponds to what we would expect from the correct state.

The first strategy we could use is to look at where quantum systems act different from non-quantum system. It has before been shown that entanglement can't be explained by local hidden variables [Bel64]. This means that certain results of the experiment would be impossible to fake with classical systems. This would however only show that entanglement is present. It does not necessarily determine precisely which quantum system has actually been realised.

We will in this report primarily be considering a specific experimental setup. This setup will be equivalent to the one presented by Ivan Šupić and Joseph Bowles in [ŠB20]. We will consider a setup that consists of two apparatus that can share a quantum state. These apparatus are then physically separated such that they are unable to communicate. Each of these apparatus is then capable of receiving an input and returning an output, this based on the input and possibly measuring the shared state. Essentially the apparatus will correspond to black-boxes, where we do not concern ourselves with their inner workings.

We will model this interaction as a game. In this setup we have two players, Alice and Bob, corresponding to the apparatus. We will furthermore be modelling a judge which is distributes the input for the apparatus in the form of questions. After Alice and Bob each receives a question from the judge they will each return an answer. The result of the game is then decided based on the answers of the players as well as the questions that was asked. Before the game starts the players are allowed to communicate and decide on a strategy while after receiving their questions they are not allowed to communicate in any way. We furthermore allow Alice and Bob to share a quantum state, and this is the state we want to determine through this game.

If we follow this setup, for certain games and outcomes we can determine which state Alice and Bob must necessarily share up to some inevitable degrees of freedom [ŠB20]. While the described experiment and setup does not fully determine the shared state, for the right outcomes it does show that Alice and Bob acted in a way that directly corresponds to some idealised way to play the game. This gives us an options for how we can verify third-party apparatus for states and measurements. We simply require the apparatus to play a game in a way where it is possible to verify the condition of no communication, and afterwards inspecting the outcome. This is the concept of self-testing.

Without diving too deeply into the technical details of self-testing that will come laater, this report will look at the role of classical randomness in the self-testing scenario. The question we will be investigating is whether allowing the two players in our scenario to access randomness or not will change the guarantees our setup gives. Specifically, we will look into whether there exist a game which has the properties:

- If Alice and Bob does not have access to shared randomness then we can determine the strategy they used.
- If Alice and Bob does have access to shared randomness then we cannot determine the strategy they used.

The first case is what we will later define as pure self-testing. The second will be what we define as mixed self-testing. What we will show is that these are very closely related and quite possibly the same.

1.1 Structure of the report and the project itself

The primary purpose of this report and the project itself is to examine the relationship between pure and mixed self-testing. The report is split into three general sections. Section 2 contains the necessary background in quantum information theory to get an idea about the content of the report. In Section 3 the concept of self-testing is motivated, defined and explained. Section 4 contains the original research that is the result of this project. This section contains among others the proof that pure self-testing with the canonical strategy having full Schmidt-rank implies mixed self-testing, and that pure POVM self-testing implies mixed POVM self-testing.

The project was conducted with Laura Mančinska as the supervisor and through discussions with Thor Gabelgaard Nielsen.

2 Background and Notation

As quantum information is a subject with a lot of very specific notation, that often differ from other ways you typically describe linear algebra, we are going to have a quick overview over the basic mathematical building blocks used in this report.

2.1 Quantum Systems

When discussing quantum information, we are interested in being able to model the system where the information lives. To abstract away the physical implementation of the quantum system, we will instead describe the system as a Hilbert space $\mathcal{H}$, a vector space with an inner product $(\cdot,\cdot)$ that is complete with respect to that product. We will only be considering finite-dimensional spaces, and any system mentioned from this point onwards will be finite unless otherwise specified.

Elements in these spaces are vectors, for which we will be using Dirac's Bra-ket notation in accordance to other texts on the topic of quantum information [NC10; ŠB20]. This means that a vector will be written as $|\psi\rangle$ for some label ψ. This is called a *ket*. The dual of a vector $|\psi\rangle$ will be written as $\langle\psi|$ which is called a *bra*. Using this notation we will be writing the inner product as $(|\phi\rangle, |\psi\rangle) = \langle\phi|\psi\rangle$.

We will be operating on the quantum systems using linear operators. We define $\mathrm{Hom}(\mathcal{H},\mathcal{H}')$ as the set homomorphisms from $\mathcal{H}$ to $\mathcal{H}'$, and $\mathrm{End}(\mathcal{H}) = \mathrm{Hom}(\mathcal{H},\mathcal{H})$, the set of endomorphisms on $\mathcal{H}$.

We define the Hermitian conjugate of of an operator $S \in \mathrm{Hom}(\mathcal{H},\mathcal{H}')$ as $S^* \in \mathrm{Hom}(\mathcal{H}',\mathcal{H})$ such that $(|\phi\rangle, S|\psi\rangle) = (S^*|\phi\rangle, |\psi\rangle)$ for any vectors $|\psi\rangle \in \mathcal{H}$ and $|\phi\rangle \in \mathcal{H}'$. For matricies, this corresponds to complex conjugating every element and transposing the matrix [NC10].

For any operator $S \in \mathrm{End}(\mathcal{H})$ we make the following definitions

- S is normal if $S^*S = SS^*$
- S is hermitian if $S = S^*$
- S is positive semidefinite if $\langle\psi|S|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$
- S is a projector if $S^2 = S$ and S is hermitian
- S is unitary if $S^*S = SS^* = \mathbb{1}$, where $\mathbb{1}$ is the identity operator.

Furthermore for $S \in \mathrm{Hom}(\mathcal{H},\mathcal{H}')$, we say S is an isometry if $\mathrm{rank}\,\mathcal{H} \leq \mathrm{rank}\,\mathcal{H}'$ and $S^*S = \mathbb{1}$. If $\mathrm{rank}\,\mathcal{H} \geq \mathrm{rank}\,\mathcal{H}'$ and S^* is an isometry, we call S a co-isometry.

We also have the following theorem for normal operators, proved at [NC10].

Theorem 2.1 (Spectral theorem)**.** *Any normal operator M on a Hilbert space $\mathcal{H}$ is diagonal with respect to some orthonormal basis for $\mathcal{H}$. Conversely, any diagonalisable operator is normal.*

This means that any normal operator M can be decomposed to the sum

$$M = \sum_i \lambda_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right|$$

where $\{|\psi_i\rangle\}_i$ denotes an orthonormal basis that M is diagonal in. This structure also called the spectral decomposition of M, and $\{|\psi_i\rangle\}_i$ also a set of eigenvectors for M. It should be noted that $\{|\psi_i\rangle\}_i$ is not unique but that the set $\{\lambda_i\}_i$ is, up to potential reordering.

Finally, we have the trace operator. We define the trace of an operator $S \in \mathrm{End}(\mathcal{H})$ as

$$\operatorname{tr} S = \sum_i \langle i|S|i\rangle$$

where $\{|i\rangle\}_i$ is an orthonormal basis of $\mathcal{H}$, called the computational basis. The value of the trace is independent of the actual basis taken [NC10], and is therefore also well defined.

2.2 Quantum states

Following our ability to abstract the quantum systems themselves, we will now be looking at how to describe the state the systems are in. We will be using two different descriptions, one a subset of the other. For this, the concept of density operators is central:

Definition 2.2 (Density operator)**.** *$\rho \in \mathrm{End}(\mathcal{H})$ is a density operator if ρ is positive semidefinite and has $\operatorname{tr}\rho = 1$.*

This is the fundamental way we will represent the state of a system. However, in some contexts density operators are a bit too general and we might be interested in only a subset of the possible states of the system. This specifically will be the states $\rho \in \mathrm{End}(\mathcal{H})$ where $\operatorname{rank}\rho = 1$. We call these states pure. If a state is not pure we call it mixed.

Since a pure state has $\operatorname{rank}\rho = 1$ it can be written as $\rho = |\psi\rangle\!\langle\psi|$ for some vector $|\psi\rangle \in \mathcal{H}$. Abusing this notation a bit, we will mostly be writing pure states on vector form. Specifically, we will write $|\psi\rangle$ instead of $|\psi\rangle\!\langle\psi|$.

A question one might have is how does the density operator representation and the vector representations differ. The answer to this is that a pure state is enough to precisely describe the quantum system, as long as we only have a single possible quantum state it could be in. We can, in some sense, describe the quantum structure of the state using the pure representation. However, as soon as we introduce classical randomness about which state we actually are looking at, e.g. through measurements or faulty quantum sources, we often have to replace the notation to use mixed states [NC10]. This can possibly be avoided through the concept of purification. This concept will be introduced in Subsection 2.6.

If we look at the spectral decomposition of some mixed state $\rho \in \mathrm{End}(\mathcal{H})$, we get

$$\rho = \sum_i \lambda_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right|$$

This can be seen as the system has a probability λ_i of being in state $|\psi_i\rangle\!\langle\psi_i|$ for all i [NC10]. This gives a well defined probability distribution from the condition of density operators having a trace of 1, $\sum_i \lambda_i = 1$.

It should be noted that since the spectral decomposition is not necessarily unique, there might be multiple different states that have the same mixed representation. This suggests that these types of states are indistinguishable.

Lets look at an example of this in $\mathbb{C}^2$. We identify the computational basis $\{|0\rangle, |1\rangle\}$. We then define the states

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

It is easy to check that these states are orthogonal. Now considering them as density operators, we get the following representation in the computation basis

$$|+\rangle\langle+| = \frac{1}{4}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|)$$
$$|-\rangle\langle-| = \frac{1}{4}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|).$$

From this we get the combined mixed representation of them to be

$$\frac{1}{2}(|+\rangle\langle+| + |-\rangle\langle-|) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|).$$

This shows that the mixed representation of $|+\rangle$ and $|-\rangle$ is the same as that of $|0\rangle$ and $|1\rangle$. They are therefore indistinguishable.

2.3 Measurements

Next, we will define the process of how we might inspect the state of a system. This is what we aim to do through measuring it. Measurements are a way for us to determine the current state of the system and in many cases modify the actual state. Like quantum states, we will be working with two similar but different representations of measurements.

The first measurement representation is a positive operator valued measurements (POVM).

Definition 2.3 (POVM)**.** *A collection of operators $\{E_m\}$ indexed over the set of outcomes is called a POVM if for all outcomes m, E_m is positive semidefinite and they fulfill the completeness relation:*

$$\sum_m E_m = \mathbb{1}$$

The notion of POVM is the most general way to describe measurements though in some cases they are a bit too abstract. POVMs also have the issue that after performing a measurement, this definition of POVM does not determine what the system looks like post-measurement, as this depends on the actual implementation. In actuality, the post measurement state of using the POVM $\{E_m\}_m$ and observing the outcome m, the post measurement state for measuring some pure state $|\psi\rangle$ will be $\frac{M_m|\psi\rangle}{\|M_m|\psi\rangle\|}$, for some operator M_m whith the only condition being that $M_m^* M_m = E_m$ [NC10]. The outcome m will furthermore happen with probability $\langle\psi|E_m|\psi\rangle$. Here it is especially important to recognise that the operator M_m is not necessarily unique, and therefore implementation dependent.

This issue also shows why we might want to work with something other than POVMs. This is what the concept projective measurements fixes.

Definition 2.4 (Projective Measurement)**.** *A collection $\{P_m\}$ of projectors is called a projective measurement (PVM) if*

1. *for all m and m', $P_m P_{m'} = \delta_{mm'} P'_m$, or in other words, P_m and $P_{m'}$ are orthogonal if $m \neq m'$,*

2. $\sum_m P_m = \mathbb{1}$.

For projective measurements, if a system is in the state ρ before the measurement then the probability $p(m)$ of getting outcome m is given as

$$p(m) = \mathrm{tr}(\rho P_m).$$

The post-measurement state will then be $P_m \rho P_m$, but normalised to a trace of 1 [NC10].

2.4 Composite systems

One of the central concepts in quantum information is the idea of composite systems. We will later be interested in looking at systems that are to some degree separate systems, but still can experience entanglement. Composite systems are especially important in self-testing. The primary idea behind self-testing is that we can see correlations on composite systems, that are not possible without some degree of entanglement.

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces. Then $\mathcal{H}_A \otimes \mathcal{H}_B$ is an Hilbert space. Furthermore if $\{|i\rangle_A\}_i$ is an orthonormal basis of $\mathcal{H}_A$ and $\{|j\rangle_B\}_j$ is an orthonormal basis for $\mathcal{H}_B$, then $\{|i\rangle_A \otimes |j\rangle_B\}_{i,j}$, is an orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$. Sometimes $|i\rangle_A \otimes |j\rangle_B$ will be written as $|i\rangle_A |j\rangle_B$, $|i,j\rangle_{AB}$ or even $|ij\rangle_{AB}$ [NC10]. The subscript will typically be used to denote which space a vector belongs to.

On a composite system, we define the inner product as follows.

$$\left(\sum_i \alpha_i |v_i\rangle_A \otimes |w_i\rangle_B , \sum_j \beta_j |v'_j\rangle_A \otimes |w'_i\rangle_B \right) = \sum_{i,j} \bar{\alpha}_i \beta_i \langle v_i | v'_j \rangle \langle w_i | w'_j \rangle$$

Finally operators on this system can be defined much the same way, where if $V_A \in \mathrm{Hom}(\mathcal{H}_A, \mathcal{H}_{A'})$ and $W_B \in \mathrm{Hom}(\mathcal{H}_B, \mathcal{H}_{B'})$ then $V_A \otimes W_B \in \mathrm{Hom}(\mathcal{H}_A \otimes \mathcal{H}_B, \mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$ is defined as

$$(V_A \otimes W_B)(|\phi\rangle_A \otimes |\psi\rangle_B) = V_A |\phi\rangle_A \otimes W_B |\psi\rangle_B$$

and such that the operator $V_A \otimes W_B$ is linear.

2.5 Partial Trace

The partial trace is used when looking at subsystems of a composite system. Let $|\phi\rangle\langle\phi| \otimes |\psi\rangle\langle\psi| \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a vector. Then we define the partial trace operator such that

$$\mathrm{tr}_B(|\phi\rangle\langle\phi|_A \otimes |\psi\rangle\langle\psi|_B) = |\phi\rangle\langle\phi|_A \,\mathrm{tr}\, |\psi\rangle\langle\psi|$$

and extend the operation so the operator is linear[NC10].

2.6 Purification

The idea behind purification is that sometimes it is a simpler to work with pure states than mixed states. An important issue with pure states is that we are not able to represent classical randomness. This is what we try to get around with the concept of purification. We have the following definition of purification:

Definition 2.5 (Purification)**.** *Let $\rho_R \in \mathrm{End}(\mathcal{H}_R)$ be a density operator. $|\psi\rangle_{RP} \in \mathcal{H}_R \otimes \mathcal{H}_P$, for some hilbert space $\mathcal{H}_P$, is a purification of ρ_R if and only if*

$$\mathrm{tr}_P |\psi\rangle_{RP} = \rho_R.$$

As an example, lets say we have a state $\rho \in \mathrm{End}(\mathcal{H}_R)$ with spectral decomposition $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$. The idea is that we create a new Hilbert space $\mathcal{H}_P$. We can then represent the classical randomness in ρ as entanglement to the $\mathcal{H}_P$ system. An example of a purification to ρ would be the pure state

$$|\psi\rangle = \sum_i |\psi_i\rangle_R |i\rangle_P$$

where $|\psi\rangle \in \mathcal{H}_R \otimes \mathcal{H}_P$ though this purification is not necessarily unique.

2.7 Schmidt decomposition

Finally, we have an additional decomposition. Opposed to the spectral decomposition, the Schmidt decomposition is a decomposition over two composite systems, for pure states. It has the following formulation, proven in [NC10]:

Theorem 2.6 (Schmidt decomposition)**.** *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a pure state on a composite system. Then there exists orthonormal states $\{|e_i\rangle_A\}_i \subseteq \mathcal{H}_A$ and $\{|f_i\rangle_B\}_i \subseteq \mathcal{H}_B$ such that*

$$|\psi\rangle = \sum_i \lambda_i |e_i\rangle_A |f_i\rangle_B$$

where λ_i is a non-negative real number for all i and $\sum_i \lambda_i^2 = 1$. The λ_i's are called the Schmidt coefficients.

The idea with this theorem is that we can decompose an entangled state over a bipartite system into states of each of these systems. It also shows what the outcome of taking the partial trace over this system is. If $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ has the Schmidt decomposition

$$|\psi\rangle = \sum_i \lambda_i |e_i\rangle_A |f_i\rangle_B ,$$

then tracing out system $\mathcal{H}_B$ gives

$$\begin{aligned}
\mathrm{tr}_B(|\psi\rangle\langle\psi|) &= \mathrm{tr}_B(\sum_{i,j} \lambda_i\lambda_j |e_i\rangle\langle e_j|_A \otimes |f_i\rangle\langle f_j|_B) \\
&= \sum_i \lambda_i^2 |e_i\rangle\langle e_i|_A \otimes \mathrm{tr}(|f_i\rangle\langle f_i|_B) \\
&= \sum_i \lambda_i^2 |e_i\rangle\langle e_i|_A
\end{aligned}$$

where we in equation 2 uses that $\mathrm{tr}\,|f_i\rangle\langle f_j| = \delta_{ij}$, since the set $\{|f_i\rangle\}_i$ is an orthonormal basis.

3 Self-testing

We will now look at the central concept of the project and this report, namely self-testing. The idea behind self-testing is to be able to validate or test arbitrary quantum devices. We want to be able to do this without knowing their underlying mechanisms and physical implementation, and only by knowing the correlations produced by measurements.

3.1 Non-local games

The concept of self-testing is tied closely to non-local games. Non-local games are played by two persons, typically named Alice and Bob. It is a cooperative game where Alice and Bob work together to win the game. This is overseen by a judge, that controls the game itself.

The game works the following way: Before the game starts, Alice and Bob are allowed to agree on a strategy, including possibly sharing a quantum state. Then during the game they are not allowed to communicate. Alice then receives a question s from some predetermined set of questions $\mathcal{S}$, and Bob equally receives a question t from some set of questions $\mathcal{T}$. Each of them then answers their question, such that Alice answers some a from a set of possible answers $\mathcal{A}$ and Bob an answer b from a set of possible answers $\mathcal{B}$. A sketch of the setup can be seen in Figure 1.

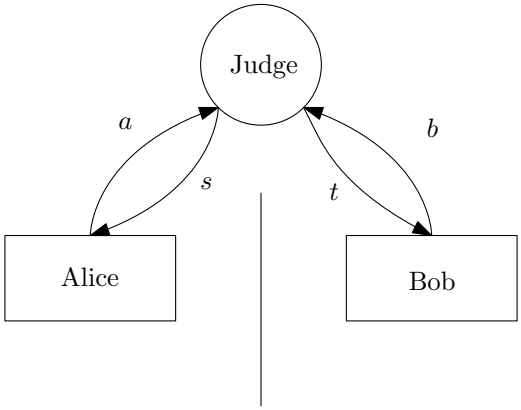

Figure 1: Non-local game. Alice receives the question $s \in \mathcal{S}$ and answers with the answer $a \in \mathcal{A}$. Bob receives the question $t \in \mathcal{T}$ and answers with the answer $b \in \mathcal{B}$.

To make this description a bit more formal, we introduce the following definition of non-local games:

Definition 3.1 (Non-local game)**.** *A non-local game G is a tuple $(p, \mathcal{V}, \mathcal{S}, \mathcal{T}, \mathcal{A}, \mathcal{B})$ of a probability distribution of the questions p, a scoring function $\mathcal{V}$ defined over*

$$p : \mathcal{S} \times \mathcal{T} \to [0, 1]$$

$$\mathcal{V} : \mathcal{A} \times \mathcal{B} \times \mathcal{S} \times \mathcal{T} \to \{0, 1\},$$

$\mathcal{S}$ and $\mathcal{T}$ are finite sets of questions for Alice and Bob respectively, $\mathcal{A}$ the finite set of answers for Alice and $\mathcal{B}$ the finite set of answers for Bob.

From this definition, we also want to be able to play the game. For this, we define the score of a game the following way:

Definition 3.2 (Score of non-local game)**.** *Let $G = (p, \mathcal{V}, \mathcal{S}, \mathcal{T}, \mathcal{A}, \mathcal{B})$ be a non-local game, and let*

$$q : \mathcal{A} \times \mathcal{B} \times \mathcal{S} \times \mathcal{T}$$

be a function such that $q(a, b|s, t)$ is a valid probability distribution for any $s, t \in \mathcal{S} \times \mathcal{T}$, and $q(a, b|s, t)$ gives the probability that for some strategy S, Alice answers a when given the question s and Bob answers b given the question t. The score of the strategy S when playing the game G, $\mathcal{W}(S, G)$ is then the probability of winning the game, defined as

$$\mathcal{W}(S, G) = \sum_{a,b,s,t} p(s, t)q(a, b|s, t)\mathcal{V}(a, b|s, t)$$

In the quantum case, we explicitly allow Alice and Bob to share a quantum state, such that each of them can perform measurements on their part of the state. This corresponds to them being able to communicate before beginning the game but not during, since it is impossible to communicate using the shared state. Sharing a state however allows the answers Alice and Bob produce to be correlated in ways that are impossible to replicate without sharing a state.

Definition 3.3 (Quantum strategy)**.** *A quantum strategy for a game G with question sets $\mathcal{S}, \mathcal{T}$ and answer sets $\mathcal{A}, \mathcal{B}$, is a tuple*

$$S = (\rho_{AB}, \{A_{sa}\}_{s\in\mathcal{S},a\in\mathcal{A}}, \{B_{tb}\}_{t\in\mathcal{T},b\in\mathcal{B}}), \tag{1}$$

consisting of a shared density operator $\rho_{AB} \in \mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B)$, where $\mathcal{H}_A$ is the state space of Alice and $\mathcal{H}_B$ is the state space of Bob. Furthermore, $\{A_{sa}\}_{s\in\mathcal{S},a\in\mathcal{A}} \subset \mathrm{End}(\mathcal{H}_A)$ is a set of POVMs on Alice's system, and $\{B_{tb}\}_{t\in\mathcal{T},b\in\mathcal{B}} \subset \mathrm{End}(\mathcal{H}_B)$ a set of POVMs on Bob's system. We will define the following special cases:

- *If $\rho_{AB} = |\psi\rangle\langle\psi|$ for some state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, we call the strategy **pure**. In this case, we may replace ρ_{AB} with $|\psi\rangle$ in* (1)*. Otherwise we may call the strategy **mixed***
- *If all POVMs for both Alice and Bob are projectors, then we refer to the strategy as **projective**.*

Often we will be suppressing the subscript of the measurements. This means we will be writing $\{A_{sa}\}_{s\in\mathcal{S},a\in\mathcal{A}}$ as $\{A_{sa}\}$ when it from context is clear that the set is index over the sets $\mathcal{S}$ and $\mathcal{A}$. The symmetric notation will be used Bob's measurements $\{B_{tb}\}$.

From this definition, we can calculate the probability $q(a, b|s, t)$ for the Alice answering a and Bob answering b given questions s and t respectively. If Alice and Bob are using the strategy $S = (\rho_{AB}, \{A_{sa}\}_{s\in\mathcal{S},a\in\mathcal{A}}, \{B_{tb}\}_{t\in\mathcal{T},b\in\mathcal{B}})$, the probability then becomes

$$q(a, b|s, t) = \mathrm{tr}((A_{st} \otimes B_{tb})\rho_{AB}).$$

The following proposition gives a useful method to calculate the game score

Proposition 3.4. *Let $G = (p, \mathcal{V}, \mathcal{S}, \mathcal{T}, \mathcal{A}, \mathcal{B})$ be a non-local game and $S = (\rho_{AB}, \{A_{sa}\}, \{B_{tb}\})$ a strategy for G. Define W as*

$$W = \sum_{a,b,s,t} p(s, t)\mathcal{V}(a, b|s, t)(A_{sa} \otimes B_{tb}).$$

Then the score of the game $\mathcal{W}(S, G)$ using strategy S can be found as

$$\mathcal{W}(S, G) = \mathrm{tr}(W\rho_{AB}).$$

Proof. We show this by rewriting $\mathcal{W}(S, G)$ using the definition of W and linearity of the trace,

$$\begin{aligned}
\mathcal{W}(S, G) &= \sum_{s,t} p(s, t) \sum_{a,b} \mathcal{V}(a, b|s, t)\, \mathrm{tr}((A_{st} \otimes B_{tb})\rho_{AB}) \\
&= \mathrm{tr}\left(\left(\sum_{s,t}\sum_{a,b} p(s, t)\mathcal{V}(a, b|s, t)(A_{st} \otimes B_{tb})\right)\rho_{AB}\right) \\
&= \mathrm{tr}(W\rho).
\end{aligned}$$

□

This exact representation will be important later on. The important part is that we for some collections of operators $\{A_{sa}\}, \{B_{tb}\}$, without being dependent on the state itself, can define an operator which can be used to evaluate the score. This in turn means the maximum possible score using the measurements $\{A_{sa}\}, \{B_{tb}\}$ in some pure strategy can be written as

$$\max_{|\psi\rangle \in \mathcal{H}} \langle\psi|W|\psi\rangle \, , s.t. \, \langle\psi|\psi\rangle = 1.$$

3.2 The CHSH game

Before we get into the core of self-testing, we will start looking at an example of a non-local game. The CHSH game is based on an experiment first proposed by Clauser, Horne, Shimony and Holt in [Cla+69]. In this game, Alice and Bob both have the question and answer sets

$$\mathcal{S} = \mathcal{T} = \mathcal{A} = \mathcal{B} = \{0, 1\}.$$

The game has the validation function

$$\mathcal{V}(a, b|s, t) = \begin{cases} 1 & \text{if } a \oplus b = s \cdot t \ , \end{cases}$$

where $\oplus$ denotes the XOR operation. Finally, the probability distribution over the questions is uniform:

$$p(s, t) = \frac{1}{4} \quad \text{for all } s \in \mathcal{S}, t \in \mathcal{T}.$$

The game boils down to that Alice and Bob must answer differently if they both receive 1, and otherwise answer the same.

We will start with considering the case where Alice and Bob doesn't share a quantum state. If we consider any randomised strategy, the probability of winning can be seen as an average over a collection of deterministic strategies [Cle+10]. Therefore the best score by any randomised strategy is score of winning with any deterministic strategy.

It is however fairly easy to bound the probability of winning with deterministic strategies. We define $a(s)$ as the answer Alice gives when receiving the question s. Symmetrically, we define $b(t)$ as the answer Bob gives when receiving the question t. From the validation function $\mathcal{V}$ of the CHSH game, for a deterministic strategy to win it must satisfy the following four equations:

$$\begin{aligned} a(0) \oplus b(0) &= 0, \\ a(0) \oplus b(1) &= 0, \\ a(1) \oplus b(0) &= 0, \\ a(1) \oplus b(1) &= 1. \end{aligned}$$

For any value $v \in \{0, 1\}$, it holds that $v \oplus v = 0$. This means if we XOR the left-hand side of the four equations together and the right-hand side of the four equations together, we get the equation $0 = 1$, which implies no deterministic strategy can satisfy all four equations at the same time. Therefore no deterministic strategy can win every time. It is however possible to win with a probability of 0.75 with the strategy $a(0) = a(1) = b(0) = b(1) = 0$, since this satisfy the first 3 equations.

The previous analysis however only holds when Alice and Bob does not share a quantum state. When they do share a quantum state it is possible to reach a score of the game. By sharing the pure state

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

and a set of appropriate measurements, it is possible to reach a probability of winning of $\cos^2(\pi/8) \approx 0.85$ [Cle+10].

3.3 The self-testing definition

We can finally get to the actual notion of self-testing. The idea behind self-testing is that we make Alice and Bob to play some non-local game and make them repeat this a large number of times. We then look at the probability of them winning. If we observe a certain probability of winning then we will know that Alice and Bob must have used some particular quantum strategy. What we furthermore will be able to is that if we can show some game self-tests a strategy $\tilde{S}$, then if Alice and Bob shows the same probability of winning as $\tilde{S}$ would, then they must have used a strategy that is equivalent S, in some sense that will be defined next.

Definition 3.5 (Self-testing)**.** *We say a game $G = (p, \mathcal{V})$,*

$$p : \mathcal{S} \times \mathcal{T} \to \{0, 1\}$$

$$\mathcal{V} : \mathcal{A} \times \mathcal{B} \times \mathcal{S} \times \mathcal{T} \to \{0, 1\}$$

self-tests the strategy

$$\tilde{S} = (\, |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}\, , \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\}), \quad |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}} \in \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}},$$

if for any strategy $S = (\rho, \{A_{sa}\}, \{B_{tb}\})$, $\rho_{AB} \in \mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B)$ for which $\mathcal{W}(S, G) = \mathcal{W}(\tilde{S}, G)$, there exists local isometries V_A, V_B

$$V_A \otimes V_B : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{\tilde{B}} \otimes \mathcal{H}_{B'}$$

such that

$$(V_A \otimes V_B)(A_{sa} \otimes B_{tb})\rho_{AB}(A_{sa} \otimes B_{tb})(V_A^* \otimes V_B^*) = ((\tilde{A}_{sa} \otimes \tilde{B}_{tb})\, |\tilde{\psi}\rangle\langle\tilde{\psi}|_{\tilde{A}\tilde{B}}\, (\tilde{A}_{sa} \otimes \tilde{B}_{tb})) \otimes \sigma_{A'B'}$$

for some state $\sigma_{\tilde{A}\tilde{B}} \in \mathrm{End}(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$ and all $a, b, s, t \in \mathcal{A} \times \mathcal{B} \times \mathcal{S} \times \mathcal{T}$

We furthermore identify the following special cases which are not mutually exclusive:

- *If the statement hold only for any pure strategy S, then we call it **pure** self-testing. If it holds for any strategy we may specify it as **mixed** self-testing*
- *If the statement only holds for any projective strategy S, we refer to it as a **projective** self-test, and otherwise as a **POVM** self-test.*

It should be noted that with the special case of pure, this is the defining property used for self-testing in among others [GKK18] and [MS13].

We will typically refer to the strategy $\tilde{S}$ as the canonical strategy. This can be seen as a baseline strategy. All strategies that achieve the same score as the canonical strategy must be able to extract the canonical strategy.

From the definition of self-testing, we might have some questions about why self-testing is interesting at all. What this definition tells is that Alice and Bob can extract the canonical strategy through only local changes and that the measurements acted on the states they have extracted. One might wonder if it would be possible to somehow further restrict the possible strategies for a given score, such that it is more specific than up to local isometries. This is however not possible.

Lets say we have a strategy $S = (|\psi\rangle\, , \{A_{sa}\}, \{B_{tb}\})$, as well as any local isometries V_A and V_B. Then the strategy $S' = ((V_A \otimes V_B)\, |\psi\rangle\, , \{V_A A_{sa} V_A^*\}, \{V_B B_{tb} V_B^*\})$, has the same probabilities of all the same outcomes. This can be seen by

$$\langle\psi|(V_A \otimes V_B)^*(V_A A_{sa} V_A^* \otimes V_B B_{tb} V_B^*)(V_A \otimes V_B)|\psi\rangle = \langle\psi|(A_{sa} \otimes B_{tb})|\psi\rangle$$

for any a, b, s, t, using the definition of isometries. In this way, self-testing is the closest we can get to specifying the actual strategy without knowing anything about the system the implemented strategy lives on.

It should be obvious from the definitions that if some game G mixed self-tests a strategy $\tilde{S}$, then G also pure self-tests the strategy $\tilde{S}$. Whether there exists equivalences in the opposite directions is less clear and the goal of this project. For example, the difference between pure and mixed self-testing lies in whether we allow the arbitrary strategy S to be mixed. This, as explained earlier, boils down to whether we allow the arbitrary strategy to use classical randomness. While this does make them seem different, this report aims to show that they in fact very close to each other, and might possibly be the same.

The topic of whether pure and mixed self-testing is mostly of interest when proving self-testing statements. If pure self-testing implied mixed self-testing, it would mean that when attempting to prove a self-testing statement you are able to simply assume the purity of the state Alice and Bob shares. This could potentially simplify proofs since you wouldn't have to consider randomness for Alice and Bob.

As an example, the CHSH game pure self-tests the optimal strategy for the game [ŠB20]. That it in fact is the optimal strategy is the one that is self-tested is no coincidence, which can be seen from the following proposition:

Proposition 3.6. *Let G be a non-local game which pure self-tests the strategy S. Then S attains either the minimal or maximal quantum value of G.*

This proposition is proven in [Lol21], and the proof is for convenience restated in Appendix A.

A different way one might define self-testing is instead of defining it in terms of a non-local game, you instead define it in terms of a probability distribution. This is how it is defined in [ŠB20] and [Goh+18]. The idea here is instead of requiring two strategies to reach the same score in a non-local game, it requires the two strategies to exhibit the same probability distribution over the outcomes. The issue with this definition is that an equivalent statement to Proposition 3.6 doesn't exist for pure self-testing. Here, an equivalent statement would be one that shows the self-testable probability distributions are extremal in the set of achievable probability distributions. One such statement does exist for mixed self-testing in [Goh+18] appendix C, but this does not easily translate to the case of only having a statement of pure self-testing. It is therefore an open question whether the results of this project applies to self-testing stated in terms of probability distributions.

4 Results

This is the part of the report that contains the results of the original research conducted as part of this project.

One thing we notice with mixed self-testing is that a mixed state inherently is a collection of pure states together with a probability distribution. This corresponds to the spectral decomposition

$$\rho = \sum_i \lambda_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right|$$

What we however immediately realise, is that for some strategy $S = (\rho, \{A_{sa}\}, B_{\{}tb\})$, the score of any game G using S can by Proposition 3.4 be written as

$$\begin{aligned}\mathcal{W}(G, S) &= \operatorname{tr}(W\rho) \\ &= \sum_i \lambda_i \operatorname{tr}(W \left|\psi_i\right\rangle\!\left\langle\psi_i\right|)\end{aligned}$$

This is the weighted average of the strategies $S_i = (|\psi_i\rangle, \{A_{sa}\}, \{B_{tb}\})$. This however gives a key insight. Since S must be optimal for self-testing to hold, by Proposition 3.6 so must each of the S_i strategies. Each of these strategies somehow shares the same operators, even though the $\{|\psi_i\rangle\}_i$ are orthogonal. This seems to suggest that we might want to look at for a given set of operators, which states can use the operators $\{A_{sa}\}$ and $\{B_{tb}\}$ to realise the optimal score for a game.

The first part of this focus on the operators is that we are able to take linear combinations of states to create new states that still are optimal with respect to the operators.

Lemma 4.1. *Let $G = (p, \mathcal{V}(a, b|s, t))$ be a non-local game that pure self-tests the strategy $\tilde{S}$, and let $S = (|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{A_{sa}\}, \{B_{tb}\})$ be any other strategy satisfying $\mathcal{W}(S, G) = \mathcal{W}(\tilde{S}, G)$. Furthermore, define the set $Q \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$ such that $|\phi\rangle \in Q$ if and only if $\mathcal{W}((|\phi\rangle, \{A_{sa}\}, \{B_{tb}\}), G) = \mathcal{W}(\tilde{S}, G)$. For the operator*

$$W = \sum_{a,b,s,t} \mathcal{V}(a, b|s, t)(A_{sa} \otimes B_{tb}),$$

it holds that W is self-adjoint, implying the set of eigenvalues $\{\lambda_i\}$ are real, that span Q *is the* $\max_i \lambda_i$*-eigenspace of W, and that for every non-zero vector $|\varphi\rangle$ in the* $\max_i \lambda_i$*-eigenspace, $|\varphi\rangle / \||\varphi\rangle\| \in Q$.*

Proof. The self-adjointness of W is clear from the definition, and since the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are assumed finite-dimensional, the number if eigenvalues is finite, and thus the maximum is well-defined. Let L be the eigenspace spanned by the eigenvectors with the largest eigenvalue in V. Let Q be the set of all states that achieves optimality of G using the measurements $\{A_{sa}\}$ and $\{B_{tb}\}$.

We first show that span $Q \subseteq L$, so take $|\psi'\rangle \in (\text{span } Q) \setminus \{0\}$ and let $|\psi\rangle := \frac{|\psi'\rangle}{\||\psi'\rangle\|} \in Q$. By Proposition 3.4 the probability of S winning G is given as

$$\mathcal{W}(S) = \langle\psi|W|\psi\rangle.$$

Writing W out using its spectral decomposition we get $W = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$. Let $k := \text{argmax}_i \lambda_i$ be a index of the largest eigenvalue (which is not necessarily unique). Then the strategy $|\phi_k\rangle$ with the same measurements would get the score λ_k, so we know that the optimal score for G is at least λ_k:

$$\langle\psi|W|\psi\rangle \geq \lambda_k \tag{2}$$

Writing $|\psi\rangle$ out in the eigenbasis of W we have $|\psi\rangle = \sum_i \mu_i |\phi_i\rangle$, with

$$\sum_i |\mu_i|^2 = 1. \tag{3}$$

As the winning probability of S using $|\psi\rangle$ is given by $\langle\psi|W|\psi\rangle$, we can use the decompositions of W and $|\psi\rangle$ in the eigenbasis of W to obtain

$$\langle\psi|W|\psi\rangle = \sum_i \lambda_i |\mu_i|^2 \leq \sum_i \lambda_k |\mu_i|^2 = \lambda_k, \tag{4}$$

in the equality using that λ_k is the largest eigenvalue, and that the $|\mu_i|^2$'s sum to 1. We can therefore conclude by (2) and (4) that

$$\lambda_k = \langle\psi|W|\psi\rangle = \sum_i \lambda_i |\mu_i|^2,$$

which by (3) implies

$$\sum_i \lambda_k |\mu_i|^2 = \sum_i \lambda_i |\mu_i|^2 \iff \sum_i (\lambda_k - \lambda_i)|\mu_i|^2 = 0.$$

Since λ_k is the maximal eigenvalue, $\lambda_k - \lambda_i \geq 0$, and obviously $|\mu_i|^2 \geq 0$. Since the sum is 0, each term must be zero, and thus for each i, either $\lambda_k = \lambda_i$ or $\mu_i = 0$. Defining the set $I = \{i : \mu_i \neq 0\}$, we can now, evaluate $W|\psi\rangle$, which gives

$$\begin{aligned} W|\psi\rangle &= \sum_i \lambda_i \mu_i |\phi_i\rangle \\ &= \sum_{i \in I} \lambda_i \mu_i |\phi_i\rangle \\ &= \lambda_k \sum_{i \in I} \mu_i |\phi_i\rangle = \lambda_k |\psi\rangle \end{aligned}$$

using the fact that for all $i \notin I$, $\mu_i = 0$. This shows $|\psi\rangle$ is a λ_k-eigenvector of W and therefore $|\psi\rangle \in L$. Thus, $Q \subseteq L$.

We then show $L \subseteq \operatorname{span} Q$. Let $|\psi\rangle \in L$. It will be enough to show that $|\psi\rangle \in Q$ with the additional assumption that $|\psi\rangle$ is normalised. Evaluating the strategy for $|\psi\rangle$ using Proposition 3.4 we get a score $\langle\psi|W|\psi\rangle = \lambda_k$. To show this is the maximally attainable score, we use Cauchy-Schwarz, which for any pure state $|\phi\rangle$, $|\langle\phi|W|\phi\rangle| \leq \||\phi\rangle\|\|W|\phi\rangle\| \leq \||\phi\rangle\|\|W\|\||\phi\rangle\| = \lambda_k$. This implies $|\psi\rangle \in Q$, and conclusively that $L = \operatorname{span} Q$ □

We now have an initial sense about how the different states that are able to use a set of measurements are related. In particular, when we have a game G that self-tests some canonical strategy $\tilde{S} = (|\tilde{\psi}\rangle, \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\})$ it is relevant to consider which strategies that might self-test using the same set of measurements. What you might realise is that since G self-tests $\tilde{S}$, any other optimal strategy using the same measurements must be able to extract the strategy $\tilde{S}$. However, if we use the Schmidt rank as an measure for entanglement, we can't increase entanglement through local isometrics, so necessarily our canonical strategy must have the lowest possible amount of all optimal strategies. This is formalised in the following lemma:

Lemma 4.2. *Let G be non-local game that pure self-tests the strategy $\tilde{S} = (|\tilde{\psi}\rangle, \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\})$. Define the set $Q \subseteq \tilde{\mathcal{H}}_A \otimes \tilde{\mathcal{H}}_B$ such that $|\phi\rangle \in Q$ if and only if $\mathcal{W}(\left(|\phi\rangle, \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\}\right), G) = \mathcal{W}(\tilde{S}, G)$. Then $|\tilde{\psi}\rangle$ has minimum Schmidt rank across all states in Q.*

Proof. Let $|\tilde{\psi}\rangle$ have Schmidt rank t. For the purpose of contradiction, assume that there exists a state $|\tilde{\phi}\rangle$ with Schmidt rank s where $s < t$. By the definition of pure self-testing, there exists local isometries V_A, V_B and a state $|junk\rangle$ such that

$$(V_A \otimes V_B)|\tilde{\phi}\rangle = |\tilde{\psi}\rangle \otimes |junk\rangle$$

However, since applying a local isometry preserves the Schmidt rank, the left side has strictly smaller Schmidt rank than the right side. This is a contradiction. Therefore no such state can exist. □

The following lemma and proof is attributed to [CMW08], but is restated and proven here for the purpose of completeness and since it wasn't organised into a formal lemma in the original article.

Lemma 4.3. *Let Q be a subspace of the bipartite space $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$. If every nonzero state in Q has Schmidt rank d, then $\dim Q = 1$.*

Proof. Consider any two-dimensional subspace spanned by unit vectors $|\varphi\rangle, |\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$. We want to show that at least one superposition $|\phi_x\rangle = |\varphi\rangle + x|\psi\rangle$ has Schmidt rank less than d. The crucial observation is that we can arrange the coefficients of a state vector $|\phi\rangle$ in the computational basis

$\{|i\rangle |j\rangle\}_{i,j=1,\dots,d}$, into a $d \times d$ matrix $M(\phi)$, and that the Schmidt rank of the state vector equals the linear rank of the associated matrix. In other words, the statement that $|\psi_x\rangle$ has Schmidt rank less than d is captured by the vanishing of the determinant $\det M(\phi_x)$. But the latter is a non-constant polynomial in x of degree d. Hence, it must have a root in the complex field, and the corresponding $|\phi_x\rangle$ has Schmidt rank $d-1$ or less. □

Lemma 4.3 is especially interesting because it bounds the dimension of a space where every state has full Schmidt rank. This ties really well together with Lemma 4.2 since this statement gives a bound on the Schmidt rank for a subspace of states that normalised can be part of an optimal strategy. In particular, consider the case were have some canonical strategy $S = (|\tilde{\psi}\rangle, \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\})$ where $|\tilde{\psi}\rangle$ has full Schmidt rank. In this case, Lemma 4.2 and Lemma 4.3 combined shows that $|\tilde{\psi}\rangle$ is the unique state, up to global phase, that is able to utilise the same measurements to achieve an optimal score of the game.

Finally, we will be working with the following two lemmas, which are simply observations to be used later

Lemma 4.4. *Let $\rho_{ST} \in \mathrm{End}(\mathcal{H}_S \otimes \mathcal{H}_T)$ be a density matrix. If $\mathrm{tr}_T\, \rho_{ST} = |\psi\rangle\langle\psi|$ for some pure state $|\psi\rangle \in \mathcal{H}_S$ then $\rho_{ST} = |\psi\rangle\langle\psi|_S \otimes \sigma_T$, for some state σ_T.*

Proof. Consider the spectral decomposition,

$$\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$$

Each of these $|\phi_i\rangle$ has some Schmidt decomposition,

$$|\phi_i\rangle = \sum_j \alpha_{ij} |e_{ij}\rangle_S |f_{ij}\rangle_T$$

, which means that $\mathrm{tr}_T |\phi_i\rangle\langle\phi_i| = \sum_j \alpha_{ij}^2 |e_{ij}\rangle\langle e_{ij}|$, and so

$$|\psi\rangle\langle\psi|_S = \mathrm{tr}_T(\rho_{ST}) = \mathrm{tr}_T \sum_i p_i |\phi_i\rangle\langle\phi_i|_{ST} = \sum_i \sum_j p_i \alpha_{ij}^2 |e_{ij}\rangle\langle e_{ij}|_S .$$

However, since $|\psi\rangle\langle\psi|$ is pure and therefore rank 1, as well as p_i and α_{ij} being positive, we have for all i, j that $|e_{ij}\rangle\langle e_{ij}| = |\psi\rangle\langle\psi|$. This implies $|\phi_i\rangle\langle\phi_i| = |\psi\rangle\langle\psi|_S \otimes |\eta_i\rangle\langle\eta_i|_T$ for some state $|\eta_i\rangle\langle\eta_i|$, and therefore $\rho = |\psi\rangle\langle\psi|_S \otimes \sigma_T$. □

Lemma 4.5. *Let $T = (|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{A_{sa}\}, \{B_{tb}\})$ and $T' = (|\psi'\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}, \{A'_{sa}\}, \{B_{tb}\})$ be two quantum strategies such that there exist local isometries*

$$V_A \otimes V_B : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_{A'} \otimes \mathcal{H}_{\hat{A}} \otimes \mathcal{H}_{B'} \otimes \mathcal{H}_{\hat{B}}$$

and a state $|junk\rangle \in \mathcal{H}_{\hat{A}} \otimes \mathcal{H}_{\hat{B}}$ such that for all s, a, t, b,

$$V_A \otimes V_B (A_{sa} \otimes B_{tb}) |\psi\rangle = [A_{sa} \otimes B_{tb} |\psi'\rangle] \otimes |junk\rangle .$$

Then for all s, a,

$$\mathrm{supp}_A (A_{sa} \otimes \mathbb{1}_B |\psi\rangle) \subseteq \mathrm{supp}_A(|\psi\rangle) \tag{5}$$

if and only if

$$\mathrm{supp}_{A'}(A'_{sa} \otimes \mathbb{1}_{B'}) |\psi'\rangle \subseteq \mathrm{supp}_{A'}(|\psi'\rangle) \tag{6}$$

and for all t, b,

$$\mathrm{supp}_B(\mathbb{1}_A \otimes B_{tb}) |\psi\rangle \subseteq \mathrm{supp}_B(|\psi\rangle) \tag{7}$$

if and only if

$$\mathrm{supp}_{B'}(\mathbb{1}_{A'} \otimes B'_{tb}) |\psi'\rangle \subseteq \mathrm{supp}_{B'}(|\psi'\rangle). \tag{8}$$

Proof. We start by proving that if (5) holds, then so does (6). Applying V_A to both sides of (5), we get

$$\mathrm{supp}_{A',\hat{A}}((A'_{sa} \otimes \mathbb{1}_{B'} |\psi'\rangle) \otimes |junk\rangle) \subseteq \mathrm{supp}_{A',\hat{A}}(|\psi'\rangle \otimes |junk\rangle) \tag{9}$$

Now consider the Schmidt decompositions of $A'_{sa} \otimes \mathbb{1}_{B'} |\psi'\rangle$ and $|junk\rangle$,

$$A'_{sa} \otimes \mathbb{1}_{B'} |\psi'\rangle = \sum_i \alpha_i |e_i\rangle_{A'} |f_i\rangle_{B'},$$
$$|junk\rangle = \sum_j \beta_j |g_j\rangle_{\hat{A}} |h_j\rangle_{\hat{B}}.$$

This means $(A'_{sa} \otimes \mathbb{1}_{B'} |\psi'\rangle) \otimes |junk\rangle$ has Schmidt decomposition

$$(A'_{sa} \otimes \mathbb{1}_{B'} |\psi'\rangle) \otimes |junk\rangle = \sum_{i,j} \alpha_i \beta_j |e_i\rangle_{A'} |g_j\rangle_{\hat{A}} |f_i\rangle_{B'} |h_j\rangle_{\hat{B}}$$

Now consider any indexes x, y. From (9), $|e_x\rangle_{A'} |g_y\rangle_{\hat{A}} \in \mathrm{supp}_{A',\hat{A}}(|\psi'\rangle \otimes |junk\rangle)$, which directly implies $|e_x\rangle_{A'} \in \mathrm{supp}_{A'}(|\psi'\rangle)$.

For the converse, that if (5) is false then (6) is also false, we follow mostly the same structure, except with a negation. We apply V_A to both sides of (5) and look at the Schmidt decompositions. Since

$$\mathrm{supp}_{A',\hat{A}}((A'_{sa} \otimes \mathbb{1}_{B'} |\psi'\rangle) \otimes |junk\rangle) \not\subseteq \mathrm{supp}_{A',\hat{A}}(|\psi'\rangle \otimes |junk\rangle), \tag{10}$$

this implies that there exist indexes x, y such that $|e_x\rangle_{A'} |g_y\rangle_{\hat{A}} \notin \mathrm{supp}_{A',\hat{A}}(|\psi'\rangle \otimes |junk\rangle)$ However, since $|g_y\rangle_{\hat{A}} \in \mathrm{supp}_{\hat{A}} |junk\rangle$, this means $|e_x\rangle_{A'} \notin \mathrm{supp}_{A'}(|\psi'\rangle)$, completing the proof.

The argument for (7) and (8) being equivalent is symmetric. □

Finally, we will be using a statement about how measurements that act equivalently on some state must be equivalent for all states in the support of the state.

Lemma 4.6. *Suppose X, Y are two finite sets, that we have collections $\{A_x\}_{x\in X}, \{A'_x\}_{x\in X} \subseteq \mathrm{End}(\mathcal{H}_A)$, and $\{B_y\}_{y\in Y}, \{B'_y\}_{y\in Y} \subseteq \mathrm{End}(\mathcal{H}_B)$, for some Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. Furthermore, suppose $\sum_{x\in X} A_x = I_A = \sum_{x\in X} A'_x$, and symmetrically $\sum_{y\in Y} B_y = I_B = \sum_{y\in Y} B'_y$. Then, for any state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ which satisfies*

$$A_x \otimes B_y |\psi\rangle = A'_x \otimes B'_y |\psi\rangle \qquad \textit{for all } x \in X, \textit{ and } y \in Y,$$

it holds that

$$A_x |\phi\rangle_A = A'_x |\phi\rangle_A, \quad \textit{for all } |\phi\rangle_A \in \mathrm{supp}_A(|\psi\rangle), \quad \textit{and}$$
$$B_x |\phi\rangle_B = B'_y |\phi\rangle_B, \quad \textit{for all } |\phi\rangle_B \in \mathrm{supp}_B(|\psi\rangle).$$

Proof. We start with the observation

$$A_x \otimes \mathbb{1}_B |\psi\rangle = \sum_y A_x \otimes B_y |\psi\rangle = \sum_y A'_x \otimes B'_y |\psi\rangle = A'_x \otimes \mathbb{1}_B |\psi\rangle$$

for any x by completeness. If we now consider the Schmidt decomposition of $|\psi\rangle$

$$|\psi\rangle = \sum_i \alpha_i |e_i\rangle_A |f_i\rangle_B$$

we observe that

$$\sum_i \alpha_i A_x \left|e_i\right\rangle_A \left|f_i\right\rangle_B = A_x \otimes \mathbb{1}_B \left|\psi\right\rangle = A'_x \otimes \mathbb{1}_B \left|\psi\right\rangle = \sum_i \alpha_i A'_x \left|e_i\right\rangle_A \left|f_i\right\rangle_B$$

which by orthogonality of $\{|f_i\rangle\}$ implies that $A_x \left|e_i\right\rangle_A = A'_x \left|e_i\right\rangle_A$ for all i. Since $\{\left|e_i\right\rangle_A\}$ constitutes a basis for $\mathrm{supp}_A \left|\psi\right\rangle$, and so $A_x \left|\phi\right\rangle_A = A'_x \left|\phi\right\rangle_A$, for all $\left|\phi\right\rangle_A \in \mathrm{supp}_A(\left|\psi\right\rangle)$. A symmetric argument holds for operators on $\mathcal{H}_B$. □

This statement is especially important, since it gives us a way to substitute measurements that act identically. We might for example know that for some strategy $S = (\left|\psi\right\rangle, \{A_{sa}\}, \{B_{tb}\})$, the local isometries V_A and V_B extract the reference strategy $\tilde{S}$

$$(V_A \otimes V_B)(A_{sa} \otimes B_{tb}) \left|\psi\right\rangle = (\tilde{A}_{sa} \otimes \tilde{B}_{tb}) \left|\tilde{\psi}\right\rangle$$

This however doesn't tell anything about e.g what $V_A A_{sa} V_A^*$ actually is. What Lemma 4.6 however tells is that it act identically to $\tilde{A}_{sa}$ on the support of the canonical strategy.

4.1 Main Result

We now get to the main results. These results attempts to show how pure and mixed self-testing is related, and in doing so, POVM and projective self-testing is also set in relation to pure and mixed self-testing.

Following the realisations from Section 4, we saw that canonical strategies with full Schmidt rank had some nice properties with uniqueness among the strategies that can use the same measurements. This turns out to be especially important, since it gives a way to uniquely determine what state we must have, given the measurements and the score of a strategy. This motivates the next lemma, since it shows how we can create a strategy that achieves the same score for the game, while at the same time obtaining the desired full Schmidt rank.

Lemma 4.7. *Let G be a non-local game that pure POVM self-tests the POVM strategy $\tilde{S} = (\left|\tilde{\psi}\right\rangle, \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\})$, $\left|\tilde{\psi}\right\rangle \in \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}$. Then there exists a POVM strategy $S' = (\left|\psi'\right\rangle, \{A'_{sa}\}, \{B'_{tb}\})$, such that G pure POVM self-tests S', $\mathcal{W}(G, S') = \mathcal{W}(G, \tilde{S})$, and $\left|\psi'\right\rangle$ has full Schmidt rank.*

Proof. We show this by constructing such a state. Consider the Schmidt decomposition of $\left|\tilde{\psi}\right\rangle$,

$$\left|\tilde{\psi}\right\rangle = \sum_{i=0}^{d-1} \lambda_i \left|e_i\right\rangle \left|f_i\right\rangle.$$

We will then consider the coisometries

$$U_A = \sum_{i=0}^{d-1} |i\rangle\langle e_i|_A \qquad \text{and} \qquad U_B = \sum_{i=0}^{d-1} |i\rangle\langle f_i|_B$$

onto the space $\mathbb{C}^d$. We will from this define POVMs $\{A'_{sa}\}$ and $\{B'_{tb}\}$, and a new state by

$$\begin{aligned} A'_{sa} &= U_A \tilde{A}_{sa} U_A^*, \\ B'_{tb} &= U_B \tilde{B}_{tb} U_B^*, \\ \left|\psi'\right\rangle &= U_A \otimes U_B \left|\tilde{\psi}\right\rangle. \end{aligned}$$

We first show that this is indeed a well-defined POVM strategy. For any s, the set $\{A'_{sa}\}_{a\in\mathcal{A}}$ is indeed a POVM since

$$\begin{aligned}\sum_{a\in\mathcal{A}} A'_{sa} &= \sum_{a\in\mathcal{A}} U_A \tilde{A}_{sa} U_A^* \\ &= U_A \left(\sum_{a\in\mathcal{A}} \tilde{A}_{sa}\right) U_A^* \\ &= U_A \mathbb{1}_{\tilde{\mathcal{H}}_A} U_A^* = \mathbb{1}_d\end{aligned}$$

using that U_A is a coisometry. This is symmetric for U_B and $\{B'_{tb}\}_{b\in\mathcal{B}}$.

We now show that this strategy exhibits the same behaviour as our original one. We first note that

$$U_A^* U_A = \sum_{i=0}^{d-1} |e_i\rangle\langle e_i| \qquad \text{and} \qquad U_B^* U_B = \sum_{i=0}^{d-1} |f_i\rangle\langle f_i|\,,$$

and therefore

$$(U_A^* U_A) \otimes \mathbb{1}_B |\psi\rangle = |\psi\rangle\,, \tag{11}$$

$$\mathbb{1}_B \otimes (U_B^* U_B) |\psi\rangle = |\psi\rangle\,, \tag{12}$$

since we act with identity on the support of the state in each case. Fixing a pair of questions (s,t) we see that the probability of attaining answers (a,b) by using this strategy is

$$\begin{aligned}\langle\psi'|A'_{sa}\otimes B'_{tb}|\psi'\rangle &= \langle\psi|(U_A\otimes U_B)^*(U_A\tilde{A}_{sa}U_A^*)\otimes(U_B\tilde{B}_{tb}U_B^*)(U_A\otimes U_B)|\psi\rangle \\ &= \langle\psi|(U_A^*U_A\tilde{A}_{sa}U_A^*U_A)\otimes(U_B^*U_B\tilde{B}_{tb}U_B^*U_B)|\psi\rangle \\ &= \langle\psi|\tilde{A}_{sa}\otimes\tilde{B}_{tb}|\psi\rangle\end{aligned}$$

using (11) and (12) for the last equality. This shows $\tilde{S}$ and S both have the same probability for the same outcomes, and thus in particular they have the same winning probability. This means that by POVM self-testing, there exists local isometries V_A, V_B and a state $|junk\rangle$ such that for all s,t,a,b, it holds that

$$V_A\otimes V_B(A'_{sa}\otimes B'_{tb})|\psi'\rangle = \left[\tilde{A}_{sa}\otimes\tilde{B}_{tb}|\tilde{\psi}\rangle\right]\otimes|junk\rangle\,. \tag{13}$$

As $|\psi'\rangle$ has full Schmidt rank, $\mathrm{supp}_A(A'_{sa}\otimes\mathbb{1}_B|\psi'\rangle) \subseteq \mathrm{supp}_A(|\psi'\rangle)$ and symmetrically for Bob's system. By Lemma 4.5 we therefore have

$$\mathrm{supp}_{\tilde{A}}(\tilde{A}_{sa}\otimes\mathbb{1}_{\tilde{B}}|\tilde{\psi}\rangle) \subseteq \mathrm{supp}_{\tilde{A}}(|\tilde{\psi}\rangle). \tag{14}$$

We can now define a new map. We extend $\{|e_i\rangle\}$ to be a basis for $\mathcal{H}_{\tilde{A}}$ such that the first d vectors corresponds to a basis for the support of $|\tilde{\psi}\rangle$ on $\mathcal{H}_{\tilde{A}}$, and do symmetrically for $\{|f_i\rangle\}$ and $\mathcal{H}_{\tilde{B}}$. We then define the local isometry $W_A\otimes W_B$ by:

$$\begin{aligned}W_A &= \sum_{i=0}^{\dim\mathcal{H}_{\tilde{A}}-1} (|i \bmod d\rangle\,|\lfloor i/d\rfloor\rangle)\,\langle e_i| \\ W_B &= \sum_{i=0}^{\dim\mathcal{H}_{\tilde{B}}-1} (|i \bmod d\rangle\,|\lfloor i/d\rfloor\rangle)\,\langle f_i|\end{aligned}$$

Observe that for a basis vector $|e_i\rangle \in \mathrm{supp}_A(|\tilde{\psi}\rangle)$, it holds that $W_A|e_i\rangle = |i\rangle|0\rangle = (U_A|e_i\rangle)|0\rangle$. Recalling (14), we can apply this and a similar relation between W_B and U_B to obtain:

$$\begin{aligned} W_A \otimes W_B(\tilde{A}_{st} \otimes \tilde{B}_{tb})|\tilde{\psi}\rangle &= \left[U_A \otimes U_B(\tilde{A}_{st} \otimes \tilde{B}_{tb})|\tilde{\psi}\rangle\right] \otimes |00\rangle \\ &= \left[(U_A \otimes U_B)(\tilde{A}_{st} \otimes \tilde{B}_{tb})(U_A \otimes U_B)^*(U_A \otimes U_B)|\tilde{\psi}\rangle\right] \otimes |00\rangle \\ &= A'_{sa} \otimes B'_{tb}|\psi'\rangle \otimes |00\rangle \end{aligned}$$

by using (11) and (12) for the second to last equation. This directly shows that G pure self-tests S', since we can compose an isometry mapping to $\tilde{S}$ with $W_A \otimes W_B$ to gain an isometry directly mapping our strategy to S'. □

Sadly, this statement requires the self-testing statement to be stated in terms of a pure POVM self-test. The issue is that the measurements of the newly created strategy isn't necessarily projective, even if we start with projective measurements. This would mean the isometry that enables the extraction would no longer be guaranteed to exist from the self-testing statement since the strategy isn't covered.

That there might in general be issues with this construction doesn't mean that it won't work in specific cases. If you can perform the procedure outlined and afterwards show that your measurements still are projective, then you would get the full Schmidt rank strategy that G self-tests. Whether there actually exists cases where a game projective self-test a strategy S, but applying the the transformation described before doesn't result in a projective strategy is to the authors knowledge an open problem.

We now reach the central theorem of this report. In this theorem we neatly tie the concept of pure self-testing to mixed self-testing, showing that we only need the additional condition of full Schmidt rank, which is a very concrete thing to show as part of any self-testing statement.

One thing that should be specified in the following theorem is that whether it is POVM or projective self-testing is not specified, since the proof holds either way. At no point in the proof is there made any assumption about the orthogonality of the measurements, neither on the side of the canonical strategy nor on the side of the arbitrary strategy considered.

Theorem 4.8. *Let G be a non-local game that pure self-tests a quantum strategy $\tilde{S} = \left(|\tilde{\psi}\rangle, \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\}\right)$. If $|\tilde{\psi}\rangle$ has full Schmidt rank, then G mixed self-tests $\tilde{S}$.*

Proof. Let $S = (\rho_{AB}, \{A_{sa}\}, \{B_{tb}\})$, with $\rho_{AB} \in \mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a strategy that achieves the optimal value of G. Consider a purification of ρ, $|\psi\rangle_{ABP} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_P$.

Initially we observe that this state has two natural Schmidt decompositions, namely both across $H_A \otimes (H_B \otimes H_P)$ and $(H_A \otimes H_P) \otimes H_B$, which clearly only depends upon who we give access to the purification space:

$$|\psi\rangle_{ABP} = \sum_{i=0}^{k_b-1} \alpha_i |e_i\rangle_{AP}|f_i\rangle_B = \sum_{i=0}^{k_a-1} \beta_i |g_i\rangle_A |h_i\rangle_{BP}.$$

Here, k_b is the Schmidt rank of the state when giving Alice access to the purification space, while k_a is the Schmidt rank when giving Bob access to the purification space.

From this we will create some new strategies S_A and S_B, with the subscript signifying who has control over the purification space

$$S_A = (|\psi\rangle_{ABP}, \{A_{sa} \otimes \mathbb{1}_P\}, \{B_{tb}\})$$

$$S_B = (|\psi\rangle_{ABP}, \{A_{sa}\}, \{B_{tb} \otimes \mathbb{1}_P\})$$

which achieve $\mathcal{W}(S_A, G) = \mathcal{W}(S_B, G) = \mathcal{W}(S, G)$. The strategies S_A and S_B both achieves the optimal value for G, and so from the fact that G pure self-tests $\tilde{S}$, there exists local isometries V_{AP}, V_B, W_A, W_{BP} and states $|junk_1\rangle$ and $|junk_2\rangle$ such that

$$(V_{AP} \otimes V_B)(A_{sa} \otimes B_{tb} \otimes \mathbb{1}_P) |\psi\rangle = ((\tilde{A}_{sa} \otimes \tilde{B}_{tb}) |\tilde{\psi}\rangle) \otimes |junk_1\rangle$$

$$(W_A \otimes W_{BP})(A_{sa} \otimes B_{tb} \otimes \mathbb{1}_P) |\psi\rangle = ((\tilde{A}_{sa} \otimes \tilde{B}'_{tb}) |\tilde{\psi}\rangle) \otimes |junk_2\rangle$$

From these strategies, by Lemma 4.6, for all $|\phi\rangle_A \in \text{supp}_{\tilde{A},\hat{A}} \ (W_A \otimes \mathbb{1}_B |\psi\rangle)$
and $|\phi\rangle_B \in \text{supp}_{\tilde{B},\hat{B}} \ (\mathbb{1}_A \otimes W_B |\psi\rangle)$

$$W_A A_{sa} W_A^* |\phi\rangle_A = \tilde{A}_{sa} \otimes \mathbb{1}_{\hat{A}} |\phi\rangle_A \tag{15}$$

$$V_B B_{tb} V_B^* |\phi\rangle_B = \tilde{B}_{tb} \otimes \mathbb{1}_{\hat{B}} |\phi\rangle_B . \tag{16}$$

We can now finally look at what the result of applying W_A and V_B to ρ_{AB} is. We define $X = W_A \otimes V_B$ for ease of notation. This isometry is simply a combination of the two, from definition, unrelated isometries. The idea is to take the isometries, that from the perspective of each of Alice and Bob, extracts the canonical strategy. While they together doesn't have any guarantee to work together, we will show that they actually end up extracting the canonical strategy.

$$\begin{aligned} &X(A_{sa} \otimes B_{tb})\rho_{AB}(A_{sa} \otimes B_{tb})X^* \\ =&X(A_{sa} \otimes B_{tb})X^* X \rho_{AB} X^* X (A_{sa} \otimes B_{tb})X^* \\ =&(\tilde{A}_{sa} \otimes \tilde{B}_{tb} \otimes \mathbb{1}_{\hat{A}\hat{B}})X\rho_{AB}X^*(\tilde{A}_{sa} \otimes \tilde{B}_{tb} \otimes \mathbb{1}_{\hat{A}\hat{B}}) \end{aligned} \tag{17}$$

Where we used (15) and (16) in the last line. We can finally trace out the ancilla systems of (17):

$$\begin{aligned} &\text{tr}_{\hat{A}\hat{B}}((\tilde{A}_{sa} \otimes \tilde{B}_{tb} \otimes \mathbb{1}_{\hat{A}\hat{B}})X\rho_{AB}X^*(\tilde{A}_{sa} \otimes \tilde{B}_{tb} \otimes \mathbb{1}_{\hat{A}\hat{B}})) \\ =&(\tilde{A}_{sa} \otimes \tilde{B}_{tb}) \,\text{tr}_{\hat{A}\hat{B}} \left(X\rho_{AB}X^*\right) (\tilde{A}_{sa} \otimes \tilde{B}_{tb}) \end{aligned}$$

From which we are motivated to define $\rho'_{\tilde{A}\tilde{B}} = \text{tr}_{\hat{A}\hat{B}} \left(X\rho_{AB}X^*\right)$. One thing that is important to note is that $\rho'_{\tilde{A}\tilde{B}}$ is not dependent on a, b, s or t, but instead only on the original mixed state and the isometries used in constructing X. Obviously, the isometries themselves might depend on the measurements, but only on the measurements as a whole, and not the individual one selected for the current question and answer. We will now consider the strategy $S' = (\rho'_{\tilde{A}\tilde{B}}, \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\})$. This strategy achieves the following probability for the elements s, a, t, b

$$\begin{aligned} &\text{tr}\Big((\tilde{A}_{sa} \otimes \tilde{B}_{tb})\rho'_{\tilde{A}\tilde{B}}\Big) \\ &= \text{tr}\Big(\text{tr}_{\hat{A}\hat{B}}((\tilde{A}_{sa} \otimes \tilde{B}_{tb} \otimes \mathbb{1}_{\hat{A}\hat{B}})X\rho_{AB}X^*)\Big) \\ &= \text{tr}((A_{sa} \otimes B_{tb})\rho_{AB}). \end{aligned}$$

so S' achieves the same probability over the different s, t, a, b as S, implying that S' is optimal since S is by Proposition 3.6. If we look at the spectral decomposition, we have

$$\rho'_{\tilde{A}\tilde{B}} = \sum_{i=0}^{\text{rank}\,\rho'-1} p_i \, |\psi'_i\rangle\langle\psi'_i|_{A'B'}$$

However, since S' has optimal probability of winning G using the operators $\{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\}$ by Proposition 3.6, then so must each of the $|\psi'_i\rangle$.

We now consider the set of states Q that achieves the optimal value of G using the measurements $\{\tilde{A}_{sa}\}$ and $\{\tilde{B}_{tb}\}$. By Lemma 4.1, $\operatorname{span} Q$ is a vector space that includes every state thay after normalisation achieves the optimal probability of winning G using the measurements . To show that $\operatorname{span} Q$ is 1 dimensional, consider that $|\tilde{\psi}\rangle$ has maximum Schmidt rank. By Lemma 4.2, every state in $\operatorname{span} Q$ must then have maximum Schmidt rank. This means that by Lemma 4.3 $\operatorname{span} Q$ has dimension 1, and therefore it is spanned by $|\tilde{\psi}\rangle$, so Q can only contain states that are equivalent to $|\tilde{\psi}\rangle$ up to global phase.

This implies that for all $i = 0, \dots, \operatorname{rank} \rho'_{\tilde{A}\tilde{B}} - 1$, $|\psi'_i\rangle\langle\psi'_i| = |\tilde{\psi}\rangle\langle\tilde{\psi}|$, and so $\rho'_{\tilde{A}\tilde{B}} = |\tilde{\psi}\rangle\langle\tilde{\psi}|_{\tilde{A}\tilde{B}}$. By Lemma 4.4, since the partial state is pure then it must be a product state

$$X\rho_{AB}X^* = |\tilde{\psi}\rangle\langle\tilde{\psi}| \otimes \sigma_{\hat{A}\hat{B}}.$$

And therefore

$$X(A_{sa} \otimes B_{tb})\rho_{AB}(A_{sa} \otimes B_{tb})X^* = \left[(\tilde{A}_{sa} \otimes \tilde{B}_{tb}) |\tilde{\psi}\rangle\langle\tilde{\psi}|_{\tilde{A}\tilde{B}} (\tilde{A}_{sa} \otimes \tilde{B}_{tb})\right] \otimes \sigma_{\hat{A}\hat{B}}.$$

This shows that G mixed self-tests $\tilde{S}$. □

This theorem also seems to suggest that pure and mixed self-testing are very close. Essentially, the only thing that would be necessary from here to show an equivalence between pure and mixed self-testing is to show that we always can extract a full Schmidt rank strategy.

With the conditions of Theorem 4.8, a point of interest is if we can have strategies that are pure self-tests but not full Schmidt rank. We can in fact fairly easily create an example of this. As previously discussed, the CHSH game pure self-test some strategy $\tilde{S} = (|\tilde{\psi}\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B, \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\})$, where $|\tilde{\psi}\rangle_{AB}$ is full Schmidt rank [ŠB20]. We will now consider the strategy $S' = (|\tilde{\psi}\rangle |0\rangle_{A'} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'}, \{\tilde{A}_{sa} \otimes \mathbb{1}_{A'}\}, \{\tilde{B}_{tb}\})$. We define $\mathcal{H}_{A'} \cong \mathbb{C}^2$. This means that $|\tilde{\psi}\rangle \otimes |0\rangle_{A'}$ does not have full Schmidt rank. The strategy S' essentially the same strategy as $\tilde{S}$, but we add a new space to ensure it is not full Schmidt rank.

If we now define the isometry $V_A : |i\rangle_A \mapsto |i\rangle_A |0\rangle_{A'}$, then it is immediate that

$$V_A \otimes \mathbb{1}_B(\tilde{A}_{sa} \otimes \tilde{B}_{tb}) |\tilde{\psi}\rangle = (\tilde{A}_{sa} \otimes \mathbb{1}_{A'} \otimes \tilde{B}_{tb}) |\tilde{\psi}\rangle$$

for any s, t, a, b. This means that the CHSH game pure self-tests the strategy S'. This can be seen from the fact that if $\tilde{S}$ can be extracted, then we can immediately extract S' using the local isometries V_A and $\mathbb{1}_B$.

It should however be noted that this S' strategy is not a counter example for equivalence between pure and mixed self-testing. If we were to use the method described in Lemma 4.7, we would be able to extract a projective strategy with a full Schmidt rank from S', so we would be able to use Theorem 4.8 in this case.

This could also be shown by shown by showing an equivalence between POVM and projection self-testing, should one such statement be possible. The following corollary shows how this works.

Corollary 4.9. *If G is a non-local game which pure self-tests a POVM strategy $\tilde{S} = \left(|\tilde{\psi}\rangle, \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\}\right)$, there exists some POVM strategy $S' = (|\psi'\rangle, \{A'_{sa}\}, \{B'_{tb}\})$ such that G mixed self-tests S'.*

Proof. Apply Lemma 4.7 to obtain the strategy S', and as $|\psi'\rangle$ then has full Schmidt rank, Theorem 4.8 yields the desired result. □

Another point of interest that is worth considering in Theorem 4.8 is that while the proof doesn't go through without having a full Schmidt rank canonical strategy, by applying the two unrelated isometries, we end up with a mixed state that decomposes into optimal strategies for G using the same operators as the canonical strategy. In this way, we essentially reduced the question of the general pure-mixed equivalence to a question of pure-mixed equivalence on the canonical system, using the canonical measurements.

5 Conclusion

In this project we have looked at the concept of self-testing, at its definition as well as what types of properties must necessarily hold for a self-testing statement. While these general statements doesn't necessarily give a complete equivalence relation between the two types of statement, it does show that under the assumption of full Schmidt rank of the canonical state, pure self-testing implies mixed self-testing.

Building on this, we showed that pure POVM self-testing implies mixed POVM self-testing, which hints towards the relationship between POVM self-testing and projective self-testing having a possibly strange relationship.

All in all, we have partly answered the question of how pure and mixed self-testing are related, though in doing this opened the question of how POVM and projective self-testign are related. It is furthermore still an open question if there actually exists games that POVM self-tests some strategies.

References

[Bel64] J. S. Bell. "On the Einstein Podolsky Rosen paradox". In: *Physics Physique Fizika* 1 (3 1964), pp. 195–200. DOI: 10.1103/PhysicsPhysiqueFizika.1.195. URL: https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195.

[Cla+69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. "Proposed Experiment to Test Local Hidden-Variable Theories". In: *Phys. Rev. Lett.* 23 (15 Oct. 1969), pp. 880–884. DOI: 10.1103/PhysRevLett.23.880. URL: https://link.aps.org/doi/10.1103/PhysRevLett.23.880.

[Cle+10] Richard Cleve, Peter Hoyer, Ben Toner, and John Watrous. *Consequences and Limits of Nonlocal Strategies*. 2010. arXiv: quant-ph/0404076 [quant-ph].

[CMW08] Toby Cubitt, Ashley Montanaro, and Andreas Winter. "On the dimension of subspaces with bounded Schmidt rank". In: *Journal of Mathematical Physics* 49.2 (Feb. 2008), p. 022107. ISSN: 1089-7658. DOI: 10.1063/1.2862998. URL: http://dx.doi.org/10.1063/1.2862998.

[GKK18] Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. "Verification of Quantum Computation: An Overview of Existing Approaches". In: *Theory of Computing Systems* 63.4 (2018), pp. 715–808. ISSN: 1433-0490. DOI: 10.1007/s00224-018-9872-3. URL: http://dx.doi.org/10.1007/s00224-018-9872-3.

[Goh+18] Koon Tong Goh, Jędrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani. "Geometry of the set of quantum correlations". In: *Physical Review A* 97.2 (Feb. 2018). ISSN: 2469-9934. DOI: 10.1103/physreva.97.022104. URL: http://dx.doi.org/10.1103/PhysRevA.97.022104.

[Gro96] Lov K. Grover. *A fast quantum mechanical algorithm for database search*. 1996. arXiv: 9605043 [quant-ph].

[Lol21] David Rasmussen Lolck. *Bachelors Project: Comparing Pure Self-testing to Mixed Self-testing*. 2021.

[MS13] Carl A. Miller and Yaoyun Shi. *Optimal robust quantum self-testing by binary nonlocal XOR games*. 2013. arXiv: 1207.1819 [quant-ph].

[NC10] Michael A. Nielsen and Isaac L. Chuang. "Introduction to quantum mechanics". In: *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010, pp. 60–119. DOI: 10.1017/CBO9780511976667.006.

[ŠB20] Ivan Šupić and Joseph Bowles. "Self-testing of quantum systems: a review". In: *Quantum* 4 (Sept. 2020), p. 337. ISSN: 2521-327X. DOI: 10.22331/q-2020-09-30-337. URL: http://dx.doi.org/10.22331/q-2020-09-30-337.

[Sho97] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509. ISSN: 1095-7111. DOI: 10.1137/s0097539795293172. URL: http://dx.doi.org/10.1137/S0097539795293172.

A Extremality of self-testing

This appendix includes the proof of Proposition 3.6. This proof is attributed to [Lol21], and is restated here purely for convenience:

Proposition A.1. *Let G be a game that pure self-tests the strategy*

$$\tilde{S} = (\,|\tilde{\psi}\rangle\,, \{\tilde{A}_{sa}\}, \{\tilde{B}_{tb}\}).$$

Then for any strategy

$$S = (|\psi\rangle\,, \{A_{sa}\}, \{B_{tb}\})$$

that achieves the same probability of winning G as $\tilde{S}$, the probability distribution over the answers conditioned on the questions of the game is equivalent. In other words

$$\langle\tilde{\psi}|\tilde{A}_{sa} \otimes \tilde{B}_{tb}|\tilde{\psi}\rangle = \langle\psi|A_{sa} \otimes B_{tb}|\psi\rangle$$

for all a, b, s, t

Proof. Since G self-tests $\tilde{S}$ and S achieves the same probability of winning as G, by the definition of pure self-testing there exists local isometries $V_A \otimes V_B$ such that

$$V_A \otimes V_B(A_{sa} \otimes B_{tb})\,|\psi\rangle_{AB} = \left[(\tilde{A}_{sa} \otimes \tilde{B}_{tb})\,|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}\right] \otimes |\xi\rangle_{A'B'} \tag{18}$$

for all a, b, s, t and some state $|\xi\rangle_{A'B'}$. Taking the inner product of the left-hand side with itself gives

$$\begin{aligned}\langle\psi|(A_{sa} \otimes B_{tb})^*(V_A \otimes V_B)^*(V_A \otimes V_B)(A_{sa} \otimes B_{tb})|\psi\rangle &= \langle\psi|(A_{sa} \otimes B_{tb})^*(A_{sa} \otimes B_{tb})|\psi\rangle \\ &= \langle\psi|(A_{sa} \otimes B_{tb})(A_{sa} \otimes B_{tb})|\psi\rangle \\ &= \langle\psi|A_{sa} \otimes B_{tb}|\psi\rangle \end{aligned} \tag{19}$$

where line 1 comes from $(V_A \otimes V_B)$ being a isometry, line 2 from $(A_{sa} \otimes B_{tb})$ being a projector and therefore Hermitian and line 3 from $(A_{sa} \otimes B_{tb})$ being a projector.

Taking the inner product of the right-hand side of (18) with itself gives

$$\begin{aligned}\langle\tilde{\psi}|(\tilde{A}_{sa} \otimes \tilde{B}_{tb})^*(\tilde{A}_{sa} \otimes \tilde{B}_{tb})|\tilde{\psi}\rangle * \langle\xi|\xi\rangle &= \langle\tilde{\psi}|(\tilde{A}_{sa} \otimes \tilde{B}_{tb})^*(\tilde{A}_{sa} \otimes \tilde{B}_{tb})|\tilde{\psi}\rangle \\ &= \langle\tilde{\psi}|(\tilde{A}_{sa} \otimes \tilde{B}_{tb})|\tilde{\psi}\rangle \end{aligned} \tag{20}$$

with line 1 from $|\xi\rangle$ having a norm of 1 and line 2 from $\tilde{A}_{sa} \otimes \tilde{B}_{tb}$ being a projector. By combining the equations (18), (19), and (20), we get the desired result

$$\langle\tilde{\psi}|\tilde{A}_{sa} \otimes \tilde{B}_{tb}|\tilde{\psi}\rangle = \langle\psi|A_{sa} \otimes B_{tb}|\psi\rangle\,,$$

completing the proof. □

Lemma A.2. *Let G be a non-local game and let S and S' be strategies for G with*

$$S = (|\psi\rangle_{AB}\,, \{A_{sa}\}, \{B_{tb}\})$$
$$S' = (\,|\psi'\rangle_{A'B'}\,, \{A'_{sa}\}, \{B'_{tb}\})$$

Define isometries

$$V_A \otimes V_B : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}$$
$$V_A \otimes V_B : |i,j\rangle_{AB} \mapsto |i,j\rangle_{\tilde{A}\tilde{B}}$$
$$V'_A \otimes V'_B : \mathcal{H}_{A'} \otimes \mathcal{H}_{B'} \to \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}$$
$$V'_A \otimes V'_B : |k,l\rangle_{A'B'} \mapsto |d_A + k, d_B + l\rangle_{\tilde{A}\tilde{B}}\,,$$

writing $V = V_A \otimes V_B$ and $V' = V'_A \otimes V'_B$. Then

$$\tilde{S} = (\,|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}\,, \{\tilde{A}_{sa}\}, \{B_{tb}\})$$

defined as

$$\begin{aligned}
|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}} &= \sqrt{q}V\,|\psi\rangle_{AB} + \sqrt{1-q}V'\,|\psi'\rangle_{A'B'} \\
\tilde{A}_{sa} &= V_A A_{sa} V_A^* + V'_A A'_{sa}\; {V'_A}^* \\
\tilde{B}_{tb} &= V_B B_{tb} V_B^* + V'_B B'_{tb}\; {V'_B}^*
\end{aligned}$$

is a strategy for G for any $q \in [0,1]$.

Proof. First we note that for any states $|\phi\rangle \in \mathcal{H}_A, |\xi\rangle \in \mathcal{H}_{A'}$, we can calculate the inner product between the states after applying the isometries V and V' as

$$\langle\phi|V^*V'|\xi\rangle$$

Writing $|\phi\rangle$ and $|\psi\rangle$ out in their respective computational basis and applying the isometries, we have

$$\begin{aligned}
\langle\phi|V^*V'|\xi\rangle &= \left(\sum_{i=0}^{d_A-1} \alpha_i^*\,\langle i|_A\right) V_A^* V'_A \left(\sum_{j=0}^{d_{A'}-1} \beta_j\,|i\rangle_{A'}\right) \\
&= \left(\sum_{i=0}^{d_A-1} \alpha_i^*\,\langle i|_A\, V_A^*\right) \left(\sum_{j=0}^{d_{A'}-1} \beta_j V'_A\,|j\rangle_{A'}\right) \\
&= \left(\sum_{i=0}^{d_A-1} \alpha_i^*\,\langle i|_{\tilde{A}}\right) \left(\sum_{j=0}^{d_{A'}-1} \beta_j\,|j+d_A\rangle_{\tilde{A}}\right) \\
&= \sum_{i=0,j=0}^{d_A-1,d_{A'}-1} \alpha_i^*\beta_j\,\langle i|j+d_A\rangle
\end{aligned}$$

By the limits of the sum, $i < j + d_A$ for all possible values of i and j, so $\langle i|j+d_A\rangle = 0$ from orthogonality. We can therefore infer that $\langle\phi|V^*V'|\xi\rangle = 0$. Since this holds for arbitrary vectors in the two systems and we have symmetry between the systems of Alice and Bob, we can conclude

$$V^*V' = 0 \tag{21}$$

and taking the adjoint on both sides of the equation that

$$V'^{\,*}\,V = 0 \tag{22}$$

We start by showing that $|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}$ is a valid quantum state. This simply amounts to show that it has a norm of one, which is seen by

$$\begin{aligned}
\langle\tilde{\psi}|\tilde{\psi}\rangle &= q\,\langle\psi|V^*V|\psi\rangle + \sqrt{q}\sqrt{1-q}\,\langle\psi|V^*V'|\psi'\rangle + \sqrt{q}\sqrt{1-q}\,\langle\psi'|\,V'^{\,*}\,V|\psi\rangle + (1-q)\,\langle\psi|\,V'^{\,*}\,V'|\psi\rangle \\
&= q\,\langle\psi|\psi\rangle + (1-q)\,\langle\psi|\psi\rangle = 1
\end{aligned}$$

with line 1 from distributivity of the inner product and line 2 from (21) and (22). Line 3 is by V and V' being isometries. Therefore $|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}$ is a quantum state.

Using (21) and (22) we can show that $\tilde{A}_{sa}$ is a projector for all $a \in \mathcal{A}$ and $s \in \mathcal{S}$ as

$$\begin{aligned}
\tilde{A}_{sa}^2 &= \left(V_A A_{sa} V_A^* + V_A' A_{sa}' \, {V_A'}^*\right)\left(V_A A_{sa} V_A^* + V_A' A_{sa}' \, {V_A'}^*\right) \\
&= (V_A A_{sa} V_A *)^2 + \left(V_A' A_{sa}' \, {V_A'}^*\right)^2 + V_A A_{sa} V_A^* V_A' A_{sa}' \, {V_A'}^* + V_A' A_{sa}' \, {V_A'}^* V_A A_{sa} V_A^* \\
&= (V_A A_{sa} V_A^*)^2 + \left(V_A' A_{sa}' \, {V_A'}^*\right)^2 \\
&= V_A A_{sa} V_A^* + V_A' A_{sa}' \, {V_A'}^* \\
&= \tilde{A}_{sa},
\end{aligned}$$

line 3 being from (21) and (22), and line 4 from A_{sa} and A_{sa}' being projectors, satisfying $A_{sa}^2 = A_{sa}$ and ${A_{sa}'}^2 = A_{sa}'$.

Fixing any s, we show $\{\tilde{A}_{sa}\}_{a\in\mathcal{A}}$ describes a projective measurements. This is simply showing completeness holds for $\{\tilde{A}_{sa}\}_{a\in\mathcal{A}}$

$$\begin{aligned}
\sum_a \tilde{A}_{sa} &= \sum_a V_A A_{sa} V_A^* + V_A' A_{sa}' \, {V_A'}^* \\
&= V_A \left(\sum_a A_{sa}\right) V_A^* + V_A' \left(\sum_a A_{sa}'\right) {V_A'}^* \\
&= V_A \mathbb{1}_A V_A^* + V_A' \mathbb{1}_{A'} \, {V_A'}^*
\end{aligned}$$

with line 3 from the completeness of $\{A_{sa}\}_{a\in\mathcal{A}}$ and $\{A_{sa}'\}_{a\in\mathcal{A}}$. Writing the identities out in the computational basis, we get

$$\begin{aligned}
\sum_a \tilde{A}_{sa} &= \sum_{i=0}^{d_A-1} \left(V \, |i\rangle\langle i|_A \, V^*\right) + \sum_{j=0}^{d_{A'}-1} \left(V' \, |j\rangle\langle j|_{A'} \, {V'}^*\right) \\
&= \sum_{i=0}^{d_A-1} |i\rangle\langle i|_{\tilde{A}} + \sum_{j=0}^{d_{A'}-1} |d_A + j\rangle\langle d_A + j|_{\tilde{A}} \\
&= \sum_{i=0}^{d_A+d_{A'}-1} |i\rangle\langle i|_{\tilde{A}} = \mathbb{1}_{\tilde{A}}
\end{aligned} \tag{23}$$

where line 2 is from the definitions of V and V'. This shows completeness of $\{\tilde{A}_{sa}\}_{a\in\mathcal{A}}$. A symmetric argument shows that $\{\tilde{B}_{tb}\}_{b\in\mathcal{B}}$ describes a projective measurement for all $t \in \mathcal{T}$. Combined with $|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}$ being a valid quantum state this shows that $\tilde{S}$ is a valid strategy. □

Lemma A.3. *Let G be a non-local game and let S and S' be strategies for G that uses a pure state. Let $\mathcal{W}(G, \hat{S})$ be the probability of winning game G using strategy $\hat{S}$. Let $p_{G,\hat{S}}(a, b|s, t)$ be the probability of strategy $\hat{S}$ outputting (a, b) when receiving (s, t). Then for any $c \in [0, 1]$ for which*

$$\mathcal{W}(G, S') \leq c \leq \mathcal{W}(G, S), \tag{24}$$

there exists a strategy $\tilde{S}$ such that

$$\mathcal{W}(G, \tilde{S}) = c$$

$$p_{G,\tilde{S}}(a, b|s, t) = q p_{G,S}(a, b|s, t) + (1 - q) p_{G,S'}(a, b|s, t)$$

for all $a \in \mathcal{A}, b \in \mathcal{B}, s \in \mathcal{S}, t \in \mathcal{T}$ where q is defined by the equation

$$q\mathcal{W}(G, S) + (1 - q)\mathcal{W}(G, S') = c \tag{25}$$

Proof. We show this by construction. Let

$$S = (|\psi\rangle_{AB}, \{A_{sa}\}, \{B_{tb}\})$$

$$S' = (|\psi'\rangle_{A'B'}, \{A'_{sa}\}, \{B'_{tb}\})$$

for $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $|\psi'\rangle_{A'B'} \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$. Let

$$d_A = \dim \mathcal{H}_A,\ d_B = \dim \mathcal{H}_B,$$

$$d_{A'} = \dim \mathcal{H}_{A'},\ d_{B'} = \dim \mathcal{H}_{B'},$$

Additionally, q can be isolated in (25) as,

$$q = \frac{c - \mathcal{W}(G, S')}{\mathcal{W}(G, S) - \mathcal{W}(G, S')}$$

which by (24) implies $q \in [0, 1]$.

Then we can combine these Hilbert spaces as follows: Let $\{|ij\rangle_{AB}\}_{i=0,j=0}^{d_A-1,d_B-1}$ be the computational basis for $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\{|kl\rangle_{A'B'}\}_{k=0,l=0}^{d_{A'}-1,d_{B'}-1}$ the computational basis for $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$. Then we can create the Hilbert space $\mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}$ with $\dim \mathcal{H}_{\tilde{A}} = d_A + d_{A'}$ and $\dim \mathcal{H}_{\tilde{B}} = d_B + d_{B'}$

Defining isometries

$$V_A \otimes V_B : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}$$

$$V_A \otimes V_B : |i, j\rangle_{AB} \mapsto |i, j\rangle_{\tilde{A}\tilde{B}}$$

$$V'_A \otimes V'_B : \mathcal{H}_{A'} \otimes \mathcal{H}_{B'} \to \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}$$

$$V'_A \otimes V'_B : |k, l\rangle_{A'B'} \mapsto |d_A + k, d_B + l\rangle_{\tilde{A}\tilde{B}},$$

writing $V = V_A \otimes V_B$ and $V' = V'_A \otimes V'_B$. We will show that the strategy

$$\tilde{S} = (\,|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_{sa}\}, \{B_{tb}\})$$

defined as

$$\begin{aligned} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}} &= \sqrt{q} V |\psi\rangle_{AB} + \sqrt{1-q} V' |\psi'\rangle_{A'B'} \\ \tilde{A}_{sa} &= V_A A_{sa} V_A^* + V'_A A'_{sa} {V'_A}^* \\ \tilde{B}_{tb} &= V_B B_{tb} V_B^* + V'_B B'_{tb} {V'_B}^*. \end{aligned}$$

achieves the desired results. By lemma A.2, this is a valid strategy.

We will start by considering the expression

$$\begin{aligned} \langle\psi| V^* \left(\tilde{A}_{sa} \otimes \tilde{B}_{tb}\right) V |\psi\rangle &= \langle\psi| V^* \left(\left(V_A A_{sa} V_A^* + V'_A A'_{sa} {V'_A}^*\right) \otimes \left(V_B B_{tb} V_B^* + V'_B B'_{tb} {V'_B}^*\right)\right) V |\psi\rangle \\ &= \langle\psi| ((V_A^* V_A A_{sa} V_A^* V_A) \otimes (V_B^* V_B B_{tb} V_B^* V_B)) |\psi\rangle \\ &= \langle\psi| (A_{sa} \otimes B_{tb}) |\psi\rangle \\ &= p_{G,S}(a, b|s, t) \end{aligned} \tag{26}$$

with line 2 from (21) and line 3 from V_A and V_B being isometries. A similar calculation shows that

$$\langle\psi|\, {V'}^* \left(\tilde{A}_{sa} \otimes \tilde{B}_{tb}\right) V' |\psi\rangle = p_{G,S'}(a, b|s, t) \tag{27}$$

Calculating the probability of seeing the answers (a, b) for questions (s, t) for strategy $\tilde{S}$ we get

$$\begin{aligned} p_{G,\tilde{S}}(a,b|s,t) = & \langle\tilde{\psi}|\Big(\tilde{A}_{sa}\otimes\tilde{B}_{tb}\Big)|\tilde{\psi}\rangle \\ & = q\,\langle\psi|V^*\left(\tilde{A}_{sa}\otimes\tilde{B}_{tb}\right)V|\psi\rangle + (1-q)\,\langle\psi|\,{V'}^*\left(\tilde{A}_{sa}\otimes\tilde{B}_{tb}\right)V'|\psi\rangle \end{aligned} \tag{28}$$

using (21) and (22) on line two when expanding the expression.

Combining (26), (27) and (28) we get that

$$p_{G,\tilde{S}}(a,b|s,t) = qp_{G,S}(a,b|s,t) + (1-q)p_{G,S'}(a,b|s,t)$$

Calculating $\mathcal{W}(G,\tilde{S})$ is then found simply as

$$\mathcal{W}(G,\tilde{S}) = q\mathcal{W}(G,S) + (1-q)\mathcal{W}(G,S') = c$$

which equals c by the definition of q. □

Proposition A.4. *Let G be a non-local game that pure self-tests the strategy S. Then the probability of S winning is extremal among all possible quantum strategies.*

Proof. Assume for the purpose of contradiction that S is not extremal. Let $\mathcal{W}(G,S)$ be the probability of winning game G using strategy S. Let $\mathcal{A}$ denote the answer space of Alice for G and $\mathcal{B}$ denote the answer space for Bob for G.

Since S is not extremal, there exists two strategies $\tilde{S}$ and $\hat{S}$ such that

$$\mathcal{W}(G,\tilde{S}) < \mathcal{W}(G,S) < \mathcal{W}(G,\hat{S})$$

We can furthermore ensure that $\tilde{S}$ and $\hat{S}$ contain pure states as if they contained mixed states we could simply consider their purifications, which are pure and give the same probability distributions.

By definition 3.1, $|\mathcal{A}| \geq 2$ and $|\mathcal{B}| \geq 2$. Let $a', a'' \in \mathcal{A}$ be two different elements from $\mathcal{A}$ and $b', b'' \in \mathcal{B}$ two different elements from $\mathcal{B}$. Then we can create at least four different strategies. Let

$$\hat{S}_{\hat{a}\hat{b}} = (\,|\hat{\phi}\rangle\,, \{\hat{A}^{\hat{a}}_{sa}\}_{s\in\mathcal{S},a\in\mathcal{A}}, \{B^{\hat{b}}_{tb}\}_{t\in\mathcal{T},b\in\mathcal{B}}), \quad \hat{a}\in\mathcal{A}, \hat{b}\in\mathcal{B}$$

defined as

$$\begin{aligned} |\hat{\phi}\rangle &= |00\rangle \\ \hat{A}^{\hat{a}}_{sa} &= \delta_{a\hat{a}}\mathbb{1} \\ \hat{B}^{\hat{b}}_{tb} &= \delta_{b\hat{b}}\mathbb{1} \end{aligned}$$

It is clear that using strategy $\hat{S}_{\hat{a}\hat{b}}$ in G, Alice and Bob always answers $(\hat{a},\hat{b})$ regardless of the questions (s,t) they received. This means that the strategies $S_{a'b'}$, $S_{a'b''}$, $S_{a''b'}$ and $S_{a''b''}$ all have different probability distributions over the answers they give conditioned on the question they received, $p_{\hat{a}\hat{b}}(a,b|s,t)$ when used for G. By proposition A.1, since the probability distributions differ, at most one of these achieve the same probabilities of winning as S.

By the pigeonhole principle either two of the strategies $S_{a'b'}$, $S_{a'b''}$, $S_{a''b'}$ and $S_{a''b''}$ have higher probability of winning G than S or two have a lower probability of winning G. Each of these cases is similar except for swapping minimum and maximum, so we will only show for the case of two strategies having a smaller probability of winning than S.

Let $S', S'' \in \{S_{a'b'}, S_{a'b''}, S_{a''b'}S_{a''b''}\}$ be the different strategies for which $\mathcal{W}(G,S') \leq \mathcal{W}(G,S)$ and $\mathcal{W}(G,S'') \leq \mathcal{W}(G,S)$. And let $p_{G,\bar{S}}(a,b|s,t)$ be the probability of Alice and Bob answering (a,b) on the question (s,t) using the strategy $\bar{S}$.

By lemma A.3 there exists strategies $\hat{S}'$ and $\hat{S}''$ created by combining $\hat{S}$ and S', and $\hat{S}$ and S'' that have the same probability of winning as using S to play G and are pure. These strategies by lemma A.3 both achieve the same probability of winning as S, but they differ in their probability distribution, which can be seen by considering the $\hat{a}$ and $\hat{b}$ for which

$$p_{G,S'}(\hat{a},\hat{b}|s,t) = 1, \quad p_{G,S''}(\hat{a},\hat{b}|s,t) = 0 \tag{29}$$

If $\hat{S}'$ and $\hat{S}''$ where to have same probability distribution, then it would mean that

$$p_{G,\hat{S}'}(a,b|s,t) = p_{G,\hat{S}''}(a,b|s,t)$$

But with the strategies being defined in terms of

$$p_{G,\hat{S}'}(a,b|s,t) = q' p_{G,S'}(a,b|s,t) + (1-q')p_{G,\hat{S}}(a,b|s,t)$$

$$p_{G,\hat{S}''}(a,b|s,t) = q'' p_{G,S''}(a,b|s,t) + (1-q'')p_{G,\hat{S}}(a,b|s,t)$$

But setting these two to be equivalent by the uniqueness of the distribution gives

$$q' p_{G,S'}(a,b|s,t) + (1-q')p_{G,\hat{S}}(a,b|s,t) = q'' p_{G,S''}(a,b|s,t) + (1-q'')p_{G,\hat{S}}(a,b|s,t) \tag{30}$$

Considering the specific $\hat{a}$ and $\hat{b}$ from (29) we can consider two cases. If $p_{G,\hat{S}}(\hat{a},\hat{b}|s,t) = 0$, then $q' = 0$ since the (30) has to hold. This would however mean that $p_{G,\hat{S}'}(a,b|s,t) = p_{G,\hat{S}}(a,b|s,t)$ for all a,b,s,t. This is a contradiction since $\hat{S}$ does not achieve the same probability distribution as S.

The second case is that $p_{G,\hat{S}}(\hat{a},\hat{b}|s,t) \neq 0$, we can rewrite (30) to

$$q' = q'' - \frac{q''}{p_{G,\hat{S}}(\hat{a},\hat{b}|s,t)} \tag{31}$$

However since $0 \leq p_{G,\hat{S}}(\hat{a},\hat{b}|s,t) \leq 1$ from being a probability distribution, (31) means $q' \leq 0$. But we have already concluded that $q' = 0$ leads to a contradiction and $q' \in [0,1]$. We can therefore conclude that S must be extremal, as otherwise we would be able to create strategies that achieve the same probability of winning, but not the same probability distribution, leading to a contradiction of proposition A.1. □