Tsirelson's Bound and Beyond: Verifiability and Complexity in Quantum Systems

by

Yuming Zhao

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2024

© Yuming Zhao 2024

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Jurij Volčič Assistant Professor, Dept. of Mathematics, Drexel University
Supervisor(s):	William Slofstra Associate Professor, Dept. of Pure Mathematics, University of Waterloo
Internal Member:	Michael Brannan Associate Professor, Dept. of Pure Mathematics, University of Waterloo
Internal-External Member:	Richard Cleve Professor, Cheriton School of Computer Science, University of Waterloo
Other Member(s):	Matthew Kennedy Professor, Dept. of Pure Mathematics, University of Waterloo

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

This thesis is based on the following works:

- [PSZZ23] Connor Paddock, William Slofstra, Yuming Zhao, and Yangchen Zhou. An operator-algebraic formulation of self-testing. *Annales Henri Poincaré*, 2023.
- [Zha] Yuming Zhao. Robust self-testing for nonlocal games with stable game algebras. In preparation.
- [BMZ23] Anne Broadbent, Arthur Mehta, and Yuming Zhao. Quantum delegation with an off-the-shelf device. *arXiv:2304.03448*, 2023.
- [MSZ23] Arthur Mehta, William Slofstra, and Yuming Zhao. Positivity is undecidable in tensor product of free algebras. *arXiv:2312.05617*, 2023.

More specifically, the contents of Chapter 3 are based on [PSZZ23]; the contents of Chapter 4 are based on [Zha]; the contents of Chapters 5 and 6 are based on [BMZ23]; the contents of Chapter 7 are based on [MSZ23].

Contributions during doctoral program not included in this thesis:

- [NTZ+24] Shlok Nahar, Devashish Tupkary, Yuming Zhao, Norbert Lütkenhaus, and Ernest Y.-Z. Tan. Postselection technique for optical Quantum Key Distribution with improved de Finetti reductions. *arXiv:2403.11851*, 2024.

Abstract

This thesis employs operator-algebraic and group-theoretical techniques to study verifiability and complexity in bipartite quantum systems. A bipartite Bell scenario consists of two non-interacting parties, each can make several quantum measurements. If the two parties share an entangled quantum state, their measurement outcomes can be correlated in surprising ways. In general, we do not directly observe the entangled state and measurement operators (which are referred to as a quantum model), only the resulting statistics (which are referred to as a "correlation") — there are typically many different models achieving a given correlation. Hence it is remarkable that some correlation has a unique quantum model. A correlation with this property is called a self-test. In the first part of this thesis, we give a new definition of self-testing in terms of abstract states on C^*-algebras. We show that this operator-algebraic definition of self-testing is equivalent to the standard one and naturally extends to the commuting operator framework for nonlocal correlations.

We also propose an operator-algebraic formulation of robust self-testing. For many nonlocal games of interest, including synchronous games and XOR games, their optimal strategies correspond to tracial states on the associated game algebras. We show that for such nonlocal games, our operator-algebraic definition of robust self-testing is equivalent to the standard one. This, in turn, yields an implication from the uniqueness of tracial states on C^*-algebras to robust self-testing for nonlocal games. To address how to compute the robustness function of a self-test explicitly, we provide an enhanced version of a well-known stability result due to Gowers and Hatami and show how it completes a common argument used in self-testing.

Self-testing provides a powerful tool for verifying quantum computations. Given that reliable cloud quantum computers are becoming closer to reality, the concept of verifiability of delegated quantum computations is of central interest. Many models have been proposed, each with specific strengths and weaknesses. In the second part of this thesis, we put forth a new model where the client trusts only its classical processing, makes no computational assumptions, and interacts with a quantum server in a single round. In

addition, during a set-up phase, the client specifies the size n of the computation and receives an untrusted, off-the-shelf (OTS) device that is used to report the outcome of a single measurement. We show how to delegate polynomial-time quantum computations in the OTS model. This also yields an interactive proof system for all of QMA, which, furthermore, we show can be accomplished in statistical zero-knowledge. This provides the first relativistic (one-round), two-prover zero-knowledge proof systems for QMA.

Mathematically, bipartite quantum measurement systems can be modeled by the tensor product of free $*$-algebras. The third part of this thesis studies the complexity of determining positivity of noncommutative polynomials in these algebras. An element of a $*$-algebra is said to be positive if it is non-negative in all $*$-representations. In many situations, we'd like to be able to decide whether an element is positive, and if it is, find a certificate of positivity. For noncommutative algebras, it is well known that an element of the free $*$-algebra is positive if and only if it is a sum of squares. This provides an effective way to determine if a given noncommutative $*$-polynomial is positive, by searching through sums of squares decompositions. We show that no such procedure exists for the tensor product of two free $*$-algebras: determining whether a $*$-polynomial of such an algebra is positive is coRE-hard. We also show that it is coRE-hard to determine whether a noncommutative $*$-polynomial is trace-positive. Our results hold if free $*$-algebras are replaced by other algebras that model quantum measurements, such as group algebras of free groups or free products of cyclic groups.

Acknowledgments

I vividly recall my first year at Waterloo, when I always addressed my supervisor William as "Professor Slofstra". That was right after the COVID lockdown, during our first Zoom call, Professor Slofstra said, "Call me William. I am your supervisor only because I have ten more years of research experience than you. That doesn't mean I am superior. From now on, we are equal collaborators." So first and foremost, I would like to express my deepest gratitude to my supervisor/collaborator, William, for his invaluable guidance and support (including generous travel support) over the past five years. I also wish to thank my thesis committee members, Jurij Volčič, Michael Brannan, Matthew Kennedy, and Richard Cleve for their time and effort in reading my thesis and providing insightful feedback.

I would like to thank my amazing co-authors, Anne Broadbent, Norbert Lütkenhaus, Arthur Mehta, Shlok Nahar, Connor Paddock, Ernest Tan, Devashish Tupkary, and Yangchen Zhou. During my time at IQC, I benefited greatly from numerous enjoyable discussions with my colleagues. I thank Vahid Asadi, Adam Bene Watts, Archishna Bhattacharyya, Eric Culf, Alex Frei, Sarah Meng Li, Randy Lin, Kieran Mastel, Arsalan Motamedi, Shlok Nahar, Connor Paddock, Devashish Tupkary, Erickson Tjoa, Ernest Tan, and Matthijs Vernooij. I thank my real office mate, Sara Zafar Jafarzadeh, my rarely-seen office mate, Paul Oh, and our honored office mate, Vlad Gheorghiu, for making the working environment full of peace and love. My journey has also been enriched by academic visits. I am grateful to Jop Briët, Yinan Li, Zhengfeng Ji, Arthur Mehta, Junde Wu, Penghui Yao, and Lihong Zhi for their hospitality and stimulating discussions during my visit.

I would like to thank my friend Futian Zhang, a musician, HCI researcher, and street photographer. The photo I used for my academic website is one of his beautiful works. I am deeply grateful to my wife, Yue Xu, for her love, support, impeccable taste in food, and endless happiness she brought. Lastly, I thank my parents for their unconditional love and support. Their unwavering belief in me has been my greatest source of strength.

Dedication

To my parents, Mr. Jiansheng Zhao and Mrs. Chengmei Qiu.

Table of Contents

Examining Committee Membership ii

Author's Declaration iii

Statement of Contributions iv

Abstract v

Acknowledgments vii

Dedication viii

List of Figures xiv

List of Tables xv

1 Introduction 1

1.1 Self-testing 4

1.2 Quantum delegation 10

1.3 Hardness results 13

2 General Preliminaries **17**

2.1 Algebras . . . 17

2.1.1 Groups, $*$-algebras, and presentations . . . 17

2.1.2 Representations, states, and GNS theorem . . . 19

2.1.3 More on C^*-algebras . . . 21

2.2 Quantum . . . 23

2.2.1 Quantum states and measurements . . . 23

2.2.2 Nonlocal games and correlations . . . 24

2.2.3 Quantum circuits . . . 27

2.3 Complexity . . . 28

2.3.1 Notation . . . 28

2.3.2 Computability . . . 28

2.3.3 Quantum complexity classes . . . 30

3 Self-testing **33**

3.1 An operator-algebraic formulation of self-testing . . . 33

3.1.1 Abstract state self-tests . . . 34

3.1.2 Self-tests are abstract state self-tests . . . 39

3.1.3 Abstract state self-tests are self-tests . . . 47

3.2 POVM models versus PVM models . . . 52

3.2.1 The class of all quantum models and projective quantum models . . . 52

3.2.2 Self-testing for synchronous correlations and binary correlations . . . 56

3.3 Self-testing in other frameworks . . . 59

3.3.1 Self-testing for infinite-dimensional tensor product models . . . 59

3.3.2 Self-testing for commuting operator models . . . 65

4 Robust self-testing **75**

4.1 An operator-algebraic formulation of robust self-testing 75

4.1.1 Robust self-tests are abstract state self-tests 79

4.2 From correlations to nonlocal games 81

4.2.1 Robust self-testing for nonlocal games 86

4.3 A tracial-state characterization of self-testing 90

4.3.1 Tracial states 90

4.3.2 General results 98

4.3.3 Self-testing for synchronous and XOR games 108

4.4 Robust self-testing for nonlocal games with stable game algebras 113

4.4.1 Near-optimal strategies and approximate representations 113

4.4.2 A lifting theorem for game algebras 119

4.4.3 General results 123

4.4.4 Robust self-testing for synchronous and XOR games 125

5 Robustness and group stability **127**

5.1 An enhanced Gowers-Hatami theorem 127

5.2 Example: CHSH 133

6 Quantum delegation and quantum proofs **139**

6.1 Context and overview 139

6.1.1 Summary of results 143

6.1.2 Proof approach 146

6.1.3 Open problems 150

6.1.4 Notation and preliminaries . . . 152
6.2 Low-weight Pauli braiding test and its robustness . . . 154
6.2.1 The test . . . 154
6.2.2 Proof of robustness . . . 161
6.3 Energy test and Hamiltonian game . . . 166
6.4 Zero-knowledge proof system . . . 171
6.4.1 Simulation of history states for XZ-Hamiltonians . . . 171
6.4.2 A two prover zero-knowledge proof system for QMA . . . 173
6.5 Off-the-shelf model . . . 177
6.5.1 Formal description of the model . . . 177
6.5.2 Applications to ZK and delegated computation . . . 178

7 Decision problems in operator algebras **181**
7.1 Motivation and overview . . . 181
7.2 Preliminaries . . . 186
7.3 Approximate states . . . 189
7.3.1 Dealing with infinite operator norm . . . 194
7.4 Construction of a suitable family of algebras . . . 197
7.4.1 Group stage of construction . . . 199
7.4.2 Construction of $\mathcal{A}_{\mathcal{S}}(m)$ . . . 210
7.5 Proof of Theorem 7.1.3 . . . 216
7.6 Proof of Theorem 7.1.1 . . . 219

References **229**

APPENDICES **244**

A The closure of finite-dimensional states **245**

List of Figures

1.1 Screenshot of Tsirelson's original proof of his bound in [Tsi87] 2
1.2 Off-the-shelf model 12

6.1 Off-the-shelf proof system 144
6.2 Low-weight linearity test. 155
6.3 Low-weight anti-commutation test. 159
6.4 Transformation from QMA instances to nonlocal games 174
6.5 Statistical zero-knowledge delegation protocol using off-the-shelf devices . . 180

List of Tables

6.1 Operator solution for magic square game 158

Chapter 1

Introduction

Consider a physical system consisting of two separate labs, each capable of performing several different measurements. If the two labs are entangled, then their measurement statistics can be correlated in surprising ways that can not be explained by any classical theory. How unexpected can quantum correlations be? In his 1980s paper [Tsi87], Tsirelson initiated the study of the limitations of correlations allowed by quantum mechanics.

The story begins with a fundamental yet profound question, posed by Einstein, Podolsky, and Rosen in 1935 [EPR35]: *Can quantum-mechanical description of physical reality be considered complete?*. This question led to the famous EPR paradox which states that if the theory of quantum mechanics were complete, it would allow for "spooky action at a distance": measuring one particle could instantaneously affect another particle regardless of the distance between them. To explain the strange correlations predicted by quantum mechanics, Einstein, Podolsky, and Rosen suggested the existence of local hidden variables — undetected locally influential factors (e.g., shared randomness) that could impact the behavior of spatially isolated particles.

In 1964, Bell made a significant breakthrough with his formulation of Bell's inequalities [Bel64]. These inequalities offered a way to test whether the correlations observed in entangled particles could be explained by local hidden variable theories. The simplest form of Bell's inequality, known as the CHSH inequality [CHSH69] (named after Clauser,

Horne, Shimony, and Holt) involves two observers, Alice and Bob, each with a choice between two binary observables: A_1, A_2 for Alice and B_1, B_2 for Bob. These binary observables are unitary operators having eigenvalues ± 1 and they satisfy the compatibility condition $A_i B_j = B_j A_i$. The state of this joint system is described by a unit vector $|\psi\rangle$. CHSH inequality asserts that the expectation

$$\langle\psi| A_1 B_1 + A_1 B_2 + A_2 B_1 - A_2 B_2 |\psi\rangle \tag{1.0.1}$$

is bounded above by 2 if the measurement results are governed by any local hidden variable theory. This inequality allows for a practical test of quantum entanglement. Numerous experiments have demonstrated violations of the CHSH inequality. These experiments provide strong evidence against local hidden variable theories and support the nonlocal nature of quantum mechanics.

Building on these foundational works, Tsirelson proved that the quantum mechanical value of Equation (1.0.1) can reach up to $2\sqrt{2}$. This maximal violation of the CHSH inequality is now known as Tsirelson's bound. Tsirelson described his original proof (see Figure 1.1) as "a simple but lengthy calculation". Interestingly, this bound has a simple

$$\begin{aligned}
A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2 = {} & \frac{1}{\sqrt{2}}\,(A_1^2 + A_2^2 + B_1^2 + B_2^2) - \\
& - \frac{\sqrt{2}-1}{8}\,((\sqrt{2}+1)\,(A_1 - B_1) + A_2 - B_2)^2 - \\
& - \frac{\sqrt{2}-1}{8}\,((\sqrt{2}+1)\,(A_1 - B_2) - A_2 - B_1)^2 - \\
& - \frac{\sqrt{2}-1}{8}\,((\sqrt{2}+1)\,(A_2 - B_1) + A_1 + B_2)^2 - \\
& - \frac{\sqrt{2}-1}{8}\,((\sqrt{2}+1)\,(A_2 + B_2) - A_1 - B_1)^2 \\
& \leq \frac{1}{\sqrt{2}}\,(A_1^2 + A_2^2 + B_1^2 + B_2^2) \leq 2\sqrt{2} \cdot \mathbb{I}\,.
\end{aligned}$$

Figure 1.1: Screenshot of Tsirelson's original proof of his bound in [Tsi87]

yet short proof following the sum of squares (SOS) decomposition

$$2\sqrt{2}\mathbb{1} - (A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2) \\ = \frac{1}{\sqrt{2}}\left(\left(A_1 - \frac{B_1+B_2}{\sqrt{2}}\right)^2 + \left(A_2 - \frac{B_1-B_2}{\sqrt{2}}\right)^2\right). \quad (1.0.2)$$

The implications of Tsirelson's bound extend far beyond theoretical curiosity, inspiring several emerging areas of research in quantum information. This thesis is motivated by these implications and focuses on three main topics.

Self-testing for quantum systems. Equation (1.0.2) illustrates that Tsirelson's bound is achieved if and only if

$$\left(A_1 - \frac{B_1+B_2}{\sqrt{2}}\right)|\psi\rangle = \left(A_2 - \frac{B_1-B_2}{\sqrt{2}}\right)|\psi\rangle = 0. \quad (1.0.3)$$

Equation (1.0.3) can be thought of as a system of equations involving matrices and vectors. Remarkable, this system has a unique solution, where $|\psi\rangle$ is the maximally entangled two-qubit state, and A_i, B_j's are Pauli observables. This means some measurement statistics can uniquely determine the underlying state of the entangled systems and all the observables involved. This phenomenon is known as self-testing for quantum systems. In Chapters 3 to 5, we study the mathematics of self-testing via operator-algebraic and group-theoretical approaches.

Verifying quantum computation. In essence, self-testing allows us to infer the exact quantum state and measurements solely from the observed correlations, providing a powerful tool for verifying quantum computations. In a delegated quantum computation scenario, a client with access only to a daily-use laptop wants to delegate a quantum computation to a company equipped with advanced quantum computers. Both the client and the quantum server have their concerns: the client wants to verify that the server performed the desired quantum computation correctly (rather than using a classical supercomputer), while the server aims to conceal the inner workings of their quantum devices during the

interaction. In Chapter 6, we introduce a delegation protocol that leverages self-testing to address these concerns. Our protocol allows the client to verify the server's quantum computation while maintaining the secrecy of the server's internal operations.

Complexity of noncommutative optimization. Finding the maximal violation of a Bell-type inequality can be formulated as an optimization problem over noncommuting variables. Equation (1.0.2) represents a sum-of-squares certificate for the positivity of the noncommutative polynomial $2\sqrt{2} - (A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2)$. Does every positivity noncommutative polynomial have a sum-of-squares certificate? What is the computational complexity of determining the positivity of noncommutative polynomials? We study these questions in Chapter 7.

In the remainder of the introduction, we provide more context about these topics and summarize the results presented in this thesis.

1.1 Self-testing

In a bipartite Bell scenario, two spatially-separated parties (Alice and Bob) are given measurement settings x and y drawn from some finite sets X and Y respectively, and return measurement outcomes a and b drawn from finite sets A and B. In quantum mechanics, Alice and Bob's actions in such a scenario can be modeled by measurements $\{M_a^x : a \in A\}, x \in X$ and $\{N_b^y : b \in B\}, y \in Y$ on respective local Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. If the joint system is in state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, then the probability that Alice and Bob measure outcomes a, b on inputs x, y is

$$p(a, b|x, y) = \langle \psi | M_a^x \otimes N_b^y | \psi \rangle .$$

The collection of probabilities $p = \{p(a, b|x, y) : a \in A, b \in B, x \in X, y \in Y\}$ is called a *quantum correlation*, and the collection

$$S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\right)$$

is a *quantum model* for p. While the correlation p can be directly observed from Alice and Bob's actions, the model S cannot, and in fact there are typically many different models for a given correlation p. It is remarkable that some correlations have a unique quantum model, in the sense that there is an ideal model $\widetilde{S} = \left(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\widetilde{\psi}\rangle\right)$ for p, such that for any other model $S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\right)$, there are Hilbert spaces $\mathcal{H}_A^{aux}$, $\mathcal{H}_B^{aux}$, isometries $I_A : \mathcal{H}_A \to \widetilde{\mathcal{H}}_A \otimes \mathcal{H}_A^{aux}$ and $I_B : \mathcal{H}_B \to \widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}$, and a state $|aux\rangle \in \mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}$ such that

$$(I_A \otimes I_B) \cdot (M_a^x \otimes N_b^y) |\psi\rangle = \left(\widetilde{M}_a^x \otimes \widetilde{N}_b^y |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \tag{1.1.1}$$

for all $(x, y, a, b) \in X \times Y \times A \times B$. A correlation satisfying this condition is called a *self-test*. The isometries I_A and I_B are necessary, because tensoring a model with an auxiliary register and state does not change any observable consequences of the model, including the correlation p.

The definition of a self-test given above is somewhat ad-hoc: it's clear that some type of equivalence between models is required for the definition, but why exactly this equivalence, over this set of models? Indeed, many definitions of self-testing have appeared since the inception of self-testing in [MY04], with a rough consensus seeming to form around the above definition only recently. Despite this ad-hoc nature, the definition above and its variants have been very successful. Among other achievements, self-tests have been used in proofs of device-independent cryptography [BŠCA18a, BŠCA18b]; it is possible to self-test any pure bipartite state [CGS17]; and self-testing is one of the keys to the recent proof of MIP* = RE, which has resolved the Connes' embedding problem, one of the biggest problems in operator algebras [JNV+20].

Nonetheless, the ad-hoc nature of the above definition does ask for more explanation. Christandl, Houghton-Larsen, and Mančinska [CHLM22] have made substantial progress on this front by giving an operational definition[1] of self-testing which, while complicated, is equivalent to the above definition. In this thesis, we take a different approach: we propose a succinct, mathematically motivated definition of self-testing. Specifically, we say that a

[1] In this case, an operational definition is one which can be phrased entirely in terms of physically measurable properties.

correlation p is an *abstract state self-test* if for every $k, \ell \geqslant 1$, $x_1, \ldots, x_k \in X$, $a_1, \ldots, a_k \in A$, $y_1, \ldots, y_\ell \in Y$, $b_1, \ldots, b_\ell \in B$, the value

$$\langle \psi | M_{a_1}^{x_1} \cdots M_{a_k}^{x_k} \otimes N_{b_1}^{y_1} \cdots N_{b_\ell}^{y_\ell} | \psi \rangle$$

is the same across all quantum models for p. The name comes from a convenient way of rephrasing this definition using abstract states on the tensor product $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$, where $\mathcal{A}_{POVM}^{X,A}$ is the universal C^*-algebra generated by positive elements e_a^x, $a \in A$, $x \in X$, subject to the relations $\sum_{a \in A} e_a^x = 1$. Specifically, a correlation p belongs to the set C_q of (finite-dimensional) quantum correlations if and only if there is a finite-dimensional abstract state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$, such that $p(a, b|x, y) = f(e_a^x \otimes e_b^y)$ for all x, y, a, b. Here an *(abstract) state* (as opposed to a vector state) refers to a linear functional f from the algebra to $\mathbb{C}$, such that $f(a) \geqslant 0$ for all positive operators a, and $f(1) = 1$. An abstract state is said to be *finite-dimensional* if its GNS representation is finite-dimensional. With this terminology, a $p \in C_q$ is an abstract state self-test for finite-dimensional states if and only if there is a unique finite-dimensional state f realizing p.

In Chapter 3 we show that if p is an extreme point of the set C_q, then p is a self-test for quantum models if and only if it is an abstract state self-test for finite-dimensional states (see Theorem 3.1.5). Although this theorem is stated for general quantum models, the definition of self-testing is often restricted to models with projective (PVM) measurements, or other subclasses of all quantum models. This type of restriction on the class of models can also be made for abstract states. For instance, projective models correspond to states on the tensor product $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$, where $\mathcal{A}_{PVM}^{X,A}$ is the quotient of $\mathcal{A}_{POVM}^{X,A}$ by the relations $(e_a^x)^2 = e_a^x$ for $x \in X$, $a \in A$, and so we can say that a correlation p is an abstract state self-test for projective models if there is a unique finite-dimensional state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ realizing p (see Corollary 3.1.6 part (b)). In the full version of Theorem 3.1.5, we show that the abstract state definition and the standard definition of self-testing are equivalent for any sufficiently nice class $\mathcal{C}$ of models, provided that p has a full-rank model in $\mathcal{C}$. Interestingly, a result of Baptista, Chen, Kaniewski, Lolck, Mančinska, Gabelgaard Nielsen, and Schmidt [BCK+23] constructs a correlation $\widetilde{p}$ that does not have a full-rank projective model (the existence of such models had been assumed

in some prior work on self-testing). Formulating our results in this generality raises some interesting questions, such as

Question 1.1.1. *Whether there are self-tests for the class of projective models that are not self-tests for the class of all models?*

In Section 3.2, we prove that if p is an extreme binary correlation (in the sense that $|A| = |B| = 2$), or a synchronous correlation (in the sense of [PSS+16]), then p is a self-test for projective quantum models if and only if p is a self-test for all quantum models (see Theorem 3.2.6). This shows that many common examples of self-tests for projective models, such as the CHSH game and the Mermin-Peres magic square, are self-tests for all quantum models. Note that Question 1.1.1 was an open problem when our paper [PSZZ23] came out. This problem has since been resolved in [BCK+23]: the correlation $\widetilde{p}$ mentioned in the previous paragraph is a self-test for projective quantum models but not a self-test for all quantum models.

One of the advantages of the abstract state definition of self-testing is that it generalizes easily to other sets of correlations. For instance, the set of quantum correlations C_q is not closed [Slo19], and there are now several elementary proofs of this fact using self-testing techniques [Col20, Bei21]. The closure of C_q is denoted by C_{qa}, and a correlation p belongs to C_{qa} if and only if there is a (not necessarily finite-dimensional) state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ such that $f(e_a^x \otimes e_b^y) = p(a,b|x,y)$ for all a, b, x, y. Correlations $p \in C_{qa}$ do not necessarily have tensor product structures, and thus it is not clear how to generalize the standard notion of self-testing with local isometries to this setting. With the abstract state definition, we can say that a correlation $p \in C_{qa}$ is a self-test if there is a unique abstract state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ realizing p.

While not all correlations in C_{qa} have tensor product models, correlations in C_{qa} can be modeled using another framework for bipartite systems, commuting operator models. In a commuting operator model, Alice and Bob make measurements on a joint Hilbert space (with no tensor product structure), and their measurement operators are required to commute (in place of factoring as tensor products). The set of correlations with a commuting operator model is denoted by C_{qc}. If p has a finite-dimensional commuting

operator model, then p also has a finite-dimensional tensor product model. However, the MIP* = RE result of Ji, Natarajan, Vidick, Wright, and Yuen shows that there are correlations $p \in C_{qc}$ which are not contained in C_{qa} [JNV+20]. There is another tensor product for C^*-algebras which is associated with the commuting operator framework, the max-tensor product, and a correlation p belongs to C_{qc} if and only if there is a state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{X,A}$ with $f(e_a^x \otimes e_b^y) = p(a,b|x,y)$ for all a, b, x, y. The definition of an abstract state self-test immediately generalizes to commuting operator models. Having a definition of a self-test for commuting operator models raises the prospect of being able to construct self-tests in C_{qc} which have no finite-dimensional models, perhaps from group algebras which are known to have a unique tracial state (see, e.g., [DM14]). In Section 3.3, we show that there are already several examples of commuting operator self-tests with finite-dimensional models. In particular, using results from [Tsi87] we show that there are many XOR correlations that are commuting operator self-tests. Notably, this implies that the CHSH game is a commuting operator self-test. This has independently been observed by Frei [Fre22] as well.

Although one of the goals of this thesis is to address the many variations of self-testing definitions, it is still helpful to make some simplifications, and for this reason we look only at self-testing with pure states. A recent result of Baptista, Chen, Kaniewski, Lolck, Mančinska, Gabelgaard Nielsen, and Schmidt [BCK+23] shows that for extremal correlations, self-testing with pure states is equivalent to self-testing with mixed states (using the definition from [ŠB20]).

For the practical use of self-testing, it is important to consider the robustness of a self-test — what happens for models that achieve a correlation close to p. We say a correlation p is a robust self-test if there is an ideal model $\widetilde{S}$ for p, such that for any other model S that achieves a correlation close to p (in some suitable norm), there are isometries I_A and I_B such that Equation (1.1.1) holds up to some small additive error.

Given a correlation $p \in C_q$ which is a self-test, Theorem 3.1.5 states that there is a unique finite-dimensional state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ realizing p. Two questions naturally arise from this characterization:

Question 1.1.2. *Do we have a similar characterization of* ***robust self-testing*** *in terms of abstract states on C^*-algebras?*

Question 1.1.3. *What happens to* ***infinite-dimensional states*** *on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ that can realize p?*

The purpose of Chapter 4 is to show that these two questions are indeed the same: if in addition, p is a robust self-test, then there are no infinite-dimensional states on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ that can realize p (see Theorem 4.1.4). In other words, with the abstract state self-test definition, p is a robust self-test only if p is an abstract state self-test for *all* states. In Section 4.4 we show that the "if" direction of this statement also holds provided that p is the unique optimal correlation for some nonlocal game $\mathcal{G}$ whose strategies can be characterized by *tracial states* on the associated game algebra $C^*(\mathcal{G})$ (see Theorems 4.4.9 and 4.4.10). This last technical condition applies to many nonlocal games of interest, including all synchronous, XOR, and Boolean constraint system (BCS) games. Notably, this "if" direction also illustrates a tracial-state characterization of robust self-testing and provides one-line proofs for many well-known robust self-tests. For instance, the fact that the Clifford algebra of rank 2 has a unique tracial state directly implies that the CHSH game is a robust self-test.

Chapter 4 gives an operator-algebraic formulation of robust self-testing, but it does not explicitly address how to compute the robustness functions. Suppose a correlation p is a robust self-test with an ideal model $\widetilde{S}$. The robustness of this self-test is a function $\eta : \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ with $\lim_{\epsilon \to 0} \eta(\epsilon) = 0$ such that for any model S that achieves a correlation ϵ-close to p, there are isometries I_A, I_B such that Equation (1.1.1) holds within an $\eta(\epsilon)$-additive error. In Chapter 5 we discuss a group-theoretical approach to compute the robustness functions. Some nonlocal games have an associated group G such that optimal (resp. near-optimal) strategies correspond to representations (resp. approximate representations) of G, so the theory of group stability comes into play. Gowers and Hatami's celebrated result [GH17] establishes that all finite groups G are stable[2]: for any approxi-

[2]In more technical terms, they demonstrate that finite groups are dilation-stable, which means that f is close to $I^*\phi I$ for some isometry I.

mate representation f of G, there is always an exact representation ϕ nearby.

Gowers and Hatami focus on the normalized Hilbert-Schmidt norm. A version for state-dependent norms was developed by Vidick in [Vid18]. However, earlier approaches to proving robust self-testing results via the Gowers-Hatami theorem are sometimes insufficient: the exact representation ϕ given by the theorem not only carries the ideal model $\widetilde{S}$ but also contains some "junk models" that need to be disregarded. We tackle this problem in Chapter 5 by stating and proving an enhanced Gowers-Hatami theorem. We show that if the approximate representation f defined by a near-optimal model satisfies some additional symmetries, then one can find an exact representation ϕ nearby that contains the ideal model $\widetilde{S}$ exclusively (see Theorem 5.1.4).

1.2 Quantum delegation

In an interactive proof system, a computationally-bounded verifier interacts with a powerful prover in order to verify the truthfulness of an agreed-upon problem instance. Starting with QMA, and followed by QIP and QMIP (among others), *quantum* interactive proof system, (in which the verifier is *quantum* polynomial-time) were defined and studied [Wat00, Wat03, KM03].

Yet, these quantizations depend crucially on the tacit assumption that the verifier has access to *trusted* quantum polynomial-time verification. Given the current state-of-the-art in quantum computation development, the inherent difficulty at characterizing quantum systems, and the fact that there is no way to reliably verify the trace of a quantum computation, there is ample evidence that this assumption may be questionable. Indeed, despite impressive technological improvements, we may ultimately have to contend with a reality where quantum computers are never as trustworthy or reliable as classical devices. This prospect has motivated consideration of models where the verifier has access to very limited but trusted quantum functionality [ABOEM17, Bro18, FK17], or where the verifier is entirely classical and the prover is computationally bounded [Mah18], while another class called MIP* models an efficient classical verifier interacting with several isolated, un-

bounded quantum provers [CHTW10]. Each approach provides advantages and encounters challenges: early quantum servers will be expensive and thus all else equal, requiring a single prover is preferable; on the other hand, existing single-prover protocols either require a trusted device or make computational assumptions. Multi-prover protocols utilize powerful device-independence techniques which avoid these assumptions but at the high cost of requiring several powerful provers and requiring isolation.

The current zeitgeist in this field allows for imaginative considerations of how we describe and model tasks in a quantum world. These approaches have in common that instead of considering the straightforward quantum analog of classical protocols, we strive to make considerations that are naturally motivated in the quantum setting[3]. In this thesis, we continue on this momentum and introduce a novel approach to proof verification, where the set-up itself can only be motivated in the quantum setting. To this end, we consider the following question:

Question 1.2.1. *What is the expressive power of the class of* ***relativistic****, interactive proof systems with a single quantum prover, and a classical verifier having access to an* ***off-the-shelf untrusted quantum device****?*

We call the above model the *off-the-shelf (OTS)* model since it models the fact that the verifier, in addition to interacting with a standard prover, has access to a device that is (1) generic (it does not depend on the instance of the problem to be solved, only on the instance size), (2) efficient (for completeness, polynomial resources are sufficed), and (3) completely untrusted (for soundness, there are no assumptions on its computational power or inner-workings). Importantly, *relativistic* refers to a one-round protocol; this is desirable for its relative ease in enforcing isolation[4].

Operationally, we imagine the OTS model as the prover providing the verifier with such a generic, off-the-shelf device ahead of the proof verification (see Figure 1.2). In particular, the preparation of such a device in terms of its capabilities is independent of the particular

[3]See, for instance, the recent work on the complexity of preparing quantum states and unitaries [RY22].

[4]A relativistic protocol is highly desirable in the multi-prover scenario since isolation can be enforced using relative position and response times [CL17, Gri19].

problem instance, although we do allow dependence on its size. Once in possession of this device, the verifier may query the prover and simultaneously use a single measurement from the off-the-shelf device, which leads the verifier to *accept* or *reject*. The figures of merit for the interactive proof system are the usual *completeness* and *soundness*.

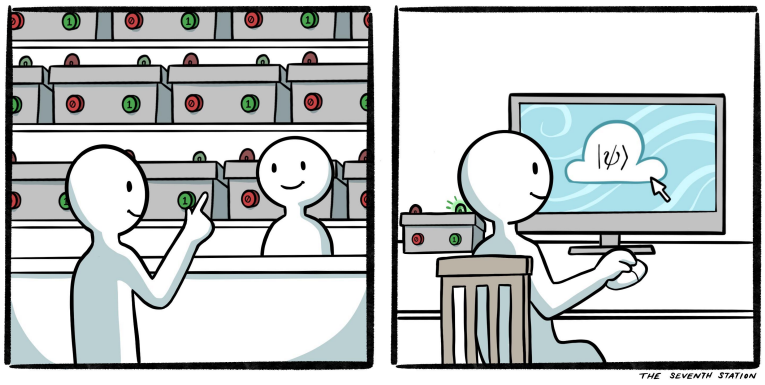


Figure 1.2: During the set-up the verifier selects an off-the-shelf device based on the required size of the problem instance. Afterward, the verifier is free to select any language and instance and interacts in a single round with both the prover and the off-the-shelf device, leading to the *accept/reject* output of the verifier.

Since the OTS scenario models aspects of near-term proof verification using untrusted quantum devices, we naturally wish to understand how it relates to some of the most relevant and studied properties of interactive proof systems:

Question 1.2.2. *Can the OTS model provide novel approaches to* ***zero-knowledge proof systems*** *and to* ***delegated quantum computation****?*

Zero-knowledge (ZK) proof systems capture the counter-intuitive notion that an interactive proof can be simultaneously convincing, while also completely concealing the inner-workings of the prover; such proof systems play an influential role in many areas of complexity and cryptography as well as in cybersecurity since they prevent reverse-engineering. We are interested here in *statistical* ZK, meaning that the concealing property holds against an unbounded verifier. Given our new OTS model, one of the first questions we thus ask is whether proof systems in the OTS model can be made ZK.

In *delegated quantum computation*, a computationally-weak client outsources a quantum computation to a more powerful (but computationally-bounded) device in a way that the result is verifiable. Starting with the OTS model, we can scale it down (such that the prover is no longer unbounded, but merely quantum polynomial-time; the verifier and off-the-shelf device remain unchanged). The question then becomes: via a relativistic interaction, can a classical polynomial-time client, together with an OTS device, verifiably outsource a quantum computation of their choosing to an isolated quantum polynomial-time device, assuming that the size of the quantum computation is compatible with the parameters of the OTS device?

In Chapter 6, we make important steps towards answering the above questions:

- We show that any language in QMA has a statistical ZK proof system in the OTS model (see Theorem 6.5.2).

- We show that the above OTS proof system can be adapted for delegated quantum computation for any problem in BQP, while remaining ZK and in the OTS model (see Theorem 6.5.3).

1.3 Hardness results

Recall that a self-adjoint bounded operator T on a Hilbert space $\mathcal{H}$ is positive if $\langle v, Tv\rangle \geqslant 0$ for all $v \in \mathcal{H}$. A self-adjoint element α of a complex $*$-algebra $\mathcal{A}$ is said to be *positive* if $\pi(\alpha)$ is positive for all $*$-representations $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$. Suppose that $\mathcal{A}$ is the complexification of a finitely-generated $*$-algebra $\mathcal{A}_{\mathbb{Q}}$ over $\mathbb{Q}$. Elements of $\mathcal{A}_{\mathbb{Q}}$ can be represented as noncommutative $*$-polynomials with rational coefficients, and hence we can work with them concretely, for instance on a computer.

In many situations, we'd like to be able to decide whether an element $a \in \mathcal{A}_{\mathbb{Q}}$ is positive in $\mathcal{A}$, and if it is, find a certificate of positivity.

A prototypical example is $\mathcal{A} = \mathbb{C}\mathcal{F}_n$, the group algebra of the free group $\mathcal{F}_n$, with

$\mathcal{A}_{\mathbb{Q}} = \mathbb{Q}\mathcal{F}_n$. In this case, the following two properties hold:

(a) Every positive element $\alpha \in \mathcal{A}$ is a *sum of (hermitian) squares (SOS)*, meaning that there are $b_1, \ldots, b_k \in \mathcal{A}$ such that $\alpha = \sum_{i=1}^{k} b_i^* b_i$.

(b) A self-adjoint element $\alpha \in \mathcal{A}$ is positive if and only if $\pi(\alpha)$ is positive in all finite-dimensional representations $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$.

Property (a) is called the *SOS property*; for archimedean algebras (see Section 2.1.2 for a definition) such as $\mathbb{C}\mathcal{F}_n$, this property is also called *archimedean closed*. Since a sum of squares is always positive, a sum of squares decomposition for an element a can be used as a certificate of positivity. The SOS property states that every positive element has such a certificate. For archimedean algebras, property (b) states that the enveloping C^*-algebra of $\mathcal{A}$ is *residually finite-dimensional (RFD)*, or equivalently that the quadratic module generated by hermitian squares in $\mathcal{A}$ is RFD [ANT19]. For convenience, we'll shorten this and just say that $\mathcal{A}$ is RFD.[5] If $\mathcal{A}$ is RFD, then for every non-positive self-adjoint element $\alpha \in \mathcal{A}$, there is a finite-dimensional representation ϕ such that $\phi(\alpha)$ is not positive. Thus if $\mathcal{A}_{\mathbb{Q}}$ is finitely-presented, then this representation can be used as a certificate of non-positivity. If $\mathcal{A}$ has the SOS property and is RFD, and $\mathcal{A}_{\mathbb{Q}}$ is finitely-presented, it is possible to decide whether a self-adjoint element $\alpha \in \mathcal{A}_{\mathbb{Q}}$ is positive by simultaneously searching for a sum of squares decomposition for α, and for a finite-dimensional representation showing that α is not positive.

For the free group algebra, property (a) is sometimes attributed to an unpublished result of Schmüdgen from the 1980s (see [NT13, Oza13]), with other proofs given in [McC01, HMP04, BT07, NT13, Oza13]. Property (b) is a result of Choi [Cho80]. Both properties also hold for the algebra of noncommutative $*$-polynomials $\mathbb{C}^*\langle x_1, \ldots, x_n \rangle$ by theorems of Helton [Hel02] and McCullough [McC01], for the $*$-algebra of n contractions by theorems of Helton-McCullough-Putinar [HMP04] or Helton-Klep-McCullough [HKM12], and for the group algebra $\mathbb{C}\mathbb{Z}_m^{*n}$ of a free product of cyclic groups again by [HMP04] or [HKM12].

[5] But note that this is not equivalent to the standard definition of RFD for $*$-algebras, which says that all non-zero elements are non-zero in some finite-dimensional representation.

That all these algebras are RFD also follows from [GM90] or [EL92]. Thus it is possible to decide positivity for all these algebras using the algorithm above, although actually we can do better: the proofs of the SOS property above are effective, meaning that they provide bounds on the degree of polynomials in the sum of squares needed to show that an element is positive. Hence we can decide positivity by searching just through SOS decompositions and stopping when the bound is reached.

In comparison, the commutative polynomial rings $\mathbb{C}[x_1, \ldots, x_n]$ famously do not have the SOS property for $n \geqslant 2$. However, Artin's solution of Hilbert's 17th problem states that every positive polynomial is a sum of squares of rational functions [Art27]. More generally, a result of Scheiderer [Sch00] states that finitely generated connected commutative $*$-algebras of dimension $\geqslant 3$, such as the group algebra $\mathbb{C}\mathbb{Z}^n$ for $n \geqslant 3$, do not have the SOS property (provided they have a state). Certificates of positivity are provided for all finitely-generated commutative algebras by the Krivine-Stengle positivstellensatz [Kri64, Ste74]. Effective versions of Artin's theorem and the Krivine-Stengle positivstellensatz are proven in [LPR20], and although the degree bounds are too large to yield practical algorithms, this gives a way to decide positivity in principle. For finitely-generated commutative algebras, positivity can also be decided with Tarski quantifier elimination or other algorithms for the first-order theory of the reals. In fact, since non-positivity lies in the existential theory of the reals, positivity can be decided in PSPACE [Can88].

If $\mathcal{A}$ is a finitely-generated commutative archimedean $*$-algebra, then Putinar's positivstellensatz states that every element which is strictly positive on the state space of $\mathcal{A}$ is a sum of squares [Put93]. For all archimedean $*$-algebras $\mathcal{A}$, Helton and McCullough's positivstellensatz [HM04] says that $\alpha \in \mathcal{A}$ is positive if and only if $\alpha + \epsilon$ is a sum of squares for all $\epsilon > 0$ (this exact formulation seems to appear first in [Cim09], see also [Sch09, Oza13]). This does not give a method for deciding positivity, but does show that deciding positivity is in the class Π_2^0 for archimedean algebras.

While positivity is decidable for the free group algebras and other prototypical non-commutative $*$-algebras $\mathcal{A}$ listed above, the point of Chapter 7 is to show that positivity becomes undecidable for tensor products $\mathcal{A} \otimes \mathcal{A}$ of such algebras: it is coRE-hard to de-

termine whether a given self-adjoint element $\alpha \in \mathcal{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{A}_{\mathbb{Q}}$ is positive in $\mathcal{A} \otimes \mathcal{A}$ (see Theorem 7.4.1). The coRE-hardness of determining positivity for $\mathcal{A} \otimes \mathcal{A}$ immediately implies that there exists no certificate of positivity in $\mathcal{A} \otimes \mathcal{A}$. In particular, unlike elements in $\mathcal{A}$, the tensor product algebra $\mathcal{A} \otimes \mathcal{A}$ does not have the SOS property (Corollary 7.1.2). In Chapter 7, we also discuss other related decision problems that arise from operator algebras and quantum information.

Chapter 2

General Preliminaries

2.1 Algebras

2.1.1 Groups, $*$-algebras, and presentations

We work with both groups and $*$-algebras. If $\mathbb{K}$ is a field with an involution $\lambda \mapsto \overline{\lambda}$, then a $*$-algebra over $\mathbb{K}$ is a unital associative $\mathbb{K}$-algebra $\mathcal{A}$ with an antilinear involution

$$\mathcal{A} \to \mathcal{A} : a \mapsto a^*$$

such that $(ab)^* = b^*a^*$ for all $a, b \in \mathcal{A}$. A *$*$-homomorphism* $\pi : \mathcal{A} \to \mathcal{B}$ between $*$-algebras $\mathcal{A}$ and $\mathcal{B}$ is an algebra homomorphism such that $\pi(a^*) = \pi(a)^*$. In this thesis, $\mathbb{K} = \mathbb{C}$ will be the default choice. We also work with $\mathbb{K} = \mathbb{Q}$ (with trivial involution) in Chapter 7. When $\mathcal{A}$ is a $*$-algebra over $\mathbb{Q}$, we use $\mathcal{A}_{\mathbb{C}}$ to denote $\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{C}$. In this thesis, we only deal with unital $*$-algebras. We use 1 for the identity in both groups and $*$-algebras.

If G is a group, then we let $\mathbb{K}G$ be the group algebra of G over the field $\mathbb{K}$. This is a $*$-algebra with $g^* = g^{-1}$. If S is a set, then $\mathcal{F}_S$ will denote the free group with generating set S, and $\mathcal{F}_n := \mathcal{F}_{\{x_1,\ldots,x_n\}}$. We use the standard notation for group presentations, in which if S is a set, and $R \subseteq \mathcal{F}_S$, then $\langle S : R \rangle$ denotes the quotient of $\mathcal{F}_S$ by the normal subgroup

generated by R. We often want to add generators and relations to a given presentation $G = \langle S : R \rangle$, so if S_1 is another set disjoint from S, and $R_1 \subseteq \mathcal{F}_{S \cup S_1}$, then we define $\langle G, S_1 : R_1 \rangle := \langle S \cup S_1 : R \cup R_1 \rangle$. If G is a group, then G^{*n} denotes the free product of n copies of G. The cyclic group of order k will be denoted by $\mathbb{Z}_k$. If S is a set, then $\mathbb{Z}_k^{*S}$ denotes the free product of $|S|$ copies of $\mathbb{Z}_k$, where the generators of the factors are denoted by the elements of S. In other words, $\mathbb{Z}_k^{*S} = \langle S : s^k = 1 \text{ for all } s \in S \rangle$.

We also define $*$-algebras by means of presentations. If S is a set, we let $\mathbb{K}^*\langle S \rangle$ denote the free noncommutative $*$-algebra with generating set S over a field $\mathbb{K}$. If $R \subseteq \mathbb{K}^*\langle S \rangle$, then $\mathbb{K}^*\langle S : R \rangle$ denotes the quotient of $\mathbb{K}^*\langle S \rangle$ by the two-sided $*$-ideal generated by R. As with groups, if $\mathcal{A} = \mathbb{K}^*\langle S : R \rangle$ is a $*$-algebra presentation, S_1 is a set disjoint from S, and $R_1 \subseteq \mathbb{K}^*\langle S \cup S_1 \rangle$, then

$$\mathbb{K}^*\langle \mathcal{A}, S : R_1 \rangle := \mathbb{K}^*\langle S \cup S_1 : R \cup R_1 \rangle.$$

If $G = \langle S : R \rangle$ is a group presentation, then

$$\mathbb{K}G = \mathbb{K}^*\langle S : 1 - r, r \in R, 1 - ss^*, 1 - s^*s, s \in S \rangle.$$

For both group and $*$-algebra presentations, we'll follow the standard practice of writing $a = b$ for the relation $b^{-1}a$ (in the case of groups) or $a - b$ (in the case of $*$-algebras). Also, a presented group (resp. algebra) is a group (resp. algebra) with a fixed presentation, and a finitely presented group (resp. algebra) is a presented group (resp. algebra) where the presentation has a finite number of generators and relations.

As mentioned above, unless specified otherwise a $*$-algebra will mean a $*$-algebra over $\mathbb{C}$. If a $*$-algebra $\mathcal{A}$ has a submultiplicative Banach norm $\|\cdot\|$ such that the *C^*-identity* $\|a^*a\| = \|a\|^2$ holds for all $a \in \mathcal{A}$ and $\mathcal{A}$ is closed with respect to $\|\cdot\|$, then $\mathcal{A}$ is said to be a C^*-algebra. For any Hilbert space $\mathcal{H}$, we use $\mathcal{B}(\mathcal{H})$ to denote the C^*-algebra of bounded operators on $\mathcal{H}$. We denote by $\mathbb{1}_{\mathcal{H}}$ the identity operator in $\mathcal{B}(\mathcal{H})$ and simply write $\mathbb{1}$ if $\mathcal{H}$ is clear from the context. The *commutant* of a subset $X \subseteq \mathcal{B}(\mathcal{H})$ is $X' := \{T \in \mathcal{B}(\mathcal{H}) : TS = ST \text{ for all } S \in X\}$.

The set of $d \times d$ matrices $M_d(\mathbb{C})$ equipped with the normalized Hilbert-Schmidt norm $\|T\|_{hs} := \frac{1}{d}\mathrm{Tr}(T^*T)$ is a C^*-algebra called *full matrix algebra* and denoted M_d.

2.1.2 Representations, states, and GNS theorem

Unless stated otherwise, all Hilbert spaces in this thesis are assumed to be separable. A *representation* π of a $*$-algebra $\mathcal{A}$ is a $*$-homomorphism from $\mathcal{A} \to \mathcal{B}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$. If $\mathcal{H}$ is finite-dimensional then we say π is *finite-dimensional*. A *subrepresentation* of π is a closed subspace $\mathcal{K} \subseteq \mathcal{H}$ such that

$$\pi(\mathcal{A})\mathcal{K} := \operatorname{span}\{\pi(a)v : a \in \mathcal{A}, v \in \mathcal{K}\} = \mathcal{K}.$$

A representation is *irreducible* if it contains no proper non-zero subrepresentations. A vector $v \in \mathcal{H}$ is *cyclic* for a representation $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ if $\pi(\mathcal{A})v$ is dense in $\mathcal{H}$. A *cyclic representation* of $\mathcal{A}$ is a tuple (H, π, v), where π is a representation of $\mathcal{A}$ on $\mathcal{H}$, and $v \in \mathcal{H}$ is cyclic for π. Two representations $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ and $\varphi : \mathcal{A} \to \mathcal{B}(\mathcal{K})$ of $\mathcal{A}$ are *(unitarily) equivalent*, denoted $\pi \cong \varphi$, if there is a unitary $U : \mathcal{H} \to \mathcal{K}$ such that $U\pi(a)U^* = \varphi(a)$ for all $a \in \mathcal{A}$. Two cyclic representations $(\mathcal{H}, \pi, v)$ and $(\mathcal{K}, \varphi, w)$ are (unitarily) equivalent if there is such a unitary with $Uv = w$.

A (bounded) state on a $*$-algebra $\mathcal{A}$ is a linear function $f : \mathcal{A} \to \mathbb{C}$ with $f(1) = 1$ such that $f(a^*) = \overline{f(a)}$, $f(a^*a) \geqslant 0$, and

$$\sup\left\{\frac{f(b^*a^*ab)}{f(b^*b)} : b \in \mathcal{A}, f(b^*b) \neq 0\right\} < \infty \tag{2.1.1}$$

for all $a \in \mathcal{A}$. The *GNS theorem* for $*$-algebras states that $f : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ is a state if and only if there is a $*$-representation $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ and a unit vector $v \in \mathcal{H}$ such that $f(a) = \langle v, \pi(a)v\rangle$ for all $a \in \mathcal{A}$ [Sch20, Theorem 4.38]. Given a state f, there is always such a representation π and unit vector v such that v is cyclic for π. Such a cyclic representation $(\mathcal{H}, \pi, v)$ is called a *GNS representation* of f. Every state has a unique GNS representation up to unitary equivalence. A state f is said to be *tracial* if $f(ab) = f(ba)$ for all $a, b \in \mathcal{A}$. Every full matrix algebra M_d has a unique tracial state tr given by $\operatorname{tr}(T) := \frac{1}{d}\operatorname{Tr}(T)$.

A state ψ on a $*$-algebra $\mathcal{A}$ induces a semi-norm $\|a\|_\psi := \sqrt{\psi(a^*a)}$ on $\mathcal{A}$ satisfying $|\psi(ab)| \leqslant \|a\|_\psi \|b\|_\psi$ for all $a, b \in \mathcal{A}$. If ψ is tracial, then $\|\cdot\|_\psi$ is unitarily invariant, meaning that $\|uav\|_\psi = \|a\|_\psi$ for all unitaries $u, v \in \mathcal{A}$ and elements $a \in \mathcal{A}$. For an arbitrary state ψ, the seminorm $\|\cdot\|_\psi$ is left unitarily invariant, but not necessarily right unitarily invariant.

A self-adjoint operator $T \in \mathcal{B}(\mathcal{H})$ is *positive* if $\langle v, Tv \rangle \geqslant 0$ for all $v \in \mathcal{H}$. A self-adjoint element a in a $*$-algebra is said to be *(representation) positive* if $\pi(a)$ is a positive operator for all Hilbert spaces $\mathcal{H}$ and representations $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$. The GNS theorem implies that a self-adjoint element $a \in \mathcal{A}$ is positive if and only if $f(a) \geqslant 0$ for all states f on $\mathcal{A}$. If $\mathcal{A}$ is a C^*-algebra, then $a \in \mathcal{A}$ is positive if and only if $a = b^*b$ for some $b \in \mathcal{A}$.

An element a of a $*$-algebra $\mathcal{A}$ is a *hermitian square* if there is $b \in \mathcal{A}$ such that $a = b^*b$, and a sum of (hermitian) squares if there are $b_1, \ldots, b_k \in \mathcal{A}$ such that $a = \sum_{i=1}^k b_i^* b_i$. If a is a sum of squares, then $\psi(a) \geqslant 0$ for all states ψ. If a_1 and a_2 are sums of squares, then $\psi(a_1 a_2) \geqslant 0$ for all tracial states ψ, since $\psi(b_1^* b_1 b_2^* b_2) = \psi((b_2 b_1^*)^*(b_2 b_1^*))$ when ψ is tracial.

Every $*$-algebra $\mathcal{A}$ has an operator norm $\|\cdot\|_{\mathcal{A}} : \mathcal{A} \to \mathbb{R}_{\geqslant 0} \cup \{\infty\}$ defined by

$$\|a\|_{\mathcal{A}} := \sup\{\sqrt{\psi(a^*a)} : \psi \text{ a state on } \mathcal{A}\}.$$

For any Hilbert space $\mathcal{H}$, we denote by $\|\cdot\|_{op}$ the operator norm on $\mathcal{B}(\mathcal{H})$. Using the GNS theorem, it can be shown that

$$\|a\|_{\mathcal{A}} = \sup\{\|\pi(a)\|_{op} : \pi \text{ a representation on a Hilbert space } \mathcal{H}\}$$

and $\psi(b^*a^*ab) \leqslant \|a\|_{\mathcal{A}}^2 \psi(b^*b)$ for all $a, b \in \mathcal{A}$ and states ψ on $\mathcal{A}$.

A $*$-algebra $\mathcal{A}$ is said to be *archimedean* if for all $a \in \mathcal{A}$ (or equivalently, all a in a generating set for $\mathcal{A}$), there is a scalar $\lambda > 0$ such that $\lambda - a^*a$ is a sum of squares. If $\mathcal{A}$ is archimedean, then a linear functional $f : \mathcal{A} \to \mathbb{C}$ satisfying $f(1) = 1$ and $f(a^*) = \overline{f(a)}$, $f(a^*a) \geqslant 0$ for all $a \in \mathcal{A}$ automatically satisfies the boundedness condition in Equation (2.1.1). Also, the operator norm $\|\cdot\|_{\mathcal{A}}$ takes only finite values, and the well-known Helton-McCullough positivstellensatz states that $a \in \mathcal{A}$ is positive if and only if $a + \epsilon$ is a sum of squares for all $\epsilon > 0$. Group algebras $\mathbb{C}G$ are archimedean, but free $*$-algebras $\mathbb{C}^*\langle S \rangle$ are not when S is non-empty. More background can be found in [Sch09] and [Oza13].

In this thesis, we will often work with finite-dimensional systems. A state f on a $*$-algebra is *finite-dimensional* if the Hilbert space $\mathcal{H}$ in the GNS representation (H, π, v) of f is finite-dimensional. If $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ is a finite-dimensional representation, then the

double-commutant theorem states that there is an isomorphism $H \cong \bigoplus_{i=1}^{\ell} \mathbb{C}^{n_i} \otimes \mathbb{C}^{m_i}$ for some integers n_i, m_i, $i = 1, \ldots, \ell$, such that

$$\pi(A) \cong \bigoplus_{i=1}^{\ell} M_{n_i}(\mathbb{C}) \otimes \mathbb{1}_{m_i}\,, \text{ and } \quad \pi(A)' \cong \bigoplus_{i=1}^{\ell} \mathbb{1}_{n_i} \otimes M_{m_i}(\mathbb{C}). \tag{2.1.2}$$

In particular, $\pi(A)$ and $\pi(A)'$ are direct sums of matrix algebras.

2.1.3 More on C^*-algebras

Let $\mathcal{A}$ be a C^*-algebra. The Gelfand–Naimark theorem states that $\mathcal{A}$ can be represented as a C^*-subalgebra of some $\mathcal{B}(\mathcal{H})$. In other words, there is a faithful representation $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$. For every $a \in \mathcal{A}$, $\|a\|^2 - a^*a$ is positive in $\mathcal{A}$ and hence a hermitian square. So $\mathcal{A}$ is archimedean. This implies a linear functional $f : \mathcal{A} \to \mathbb{C}$ is a state on $\mathcal{A}$ if and only if $f(1) = 1$ and $f(a^*a) \geqslant 0$. The set of all states on $\mathcal{A}$, denoted $\mathcal{S}(\mathcal{A})$, is called the state space of $\mathcal{A}$. $\mathcal{S}(\mathcal{A})$ is convex and weak*-compact. The extreme points of $\mathcal{S}(\mathcal{A})$ are called *pure states*. Let $f \in \mathcal{S}(\mathcal{A})$ and let $(\mathcal{H}, \pi, v)$ be a GNS representation of f. Then f is a pure state if and only if π is an irreducible representation.

Given two C^*-algebras $\mathcal{A}$ and $\mathcal{B}$, a linear mapping $\varphi : \mathcal{A} \to \mathcal{B}$ is said to be *positive* if $\varphi(x)$ is positive in $\mathcal{B}$ for any positive element $x \in \mathcal{A}$. A linear mapping $\Phi : \mathcal{A} \to \mathcal{B}$ is said to be *unital completely positive (ucp)* if

(i) $\Phi(1_{\mathcal{A}}) = 1_{\mathcal{B}}$, and

(ii) for any $x \in \mathbb{N}$, the mapping

$$\begin{gathered} \Phi_n : M_n(\mathcal{A}) \to M_n(\mathcal{B}) \\ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \mapsto \begin{pmatrix} \Phi(a_{11}) & \cdots & \Phi(a_{1n}) \\ \vdots & \ddots & \vdots \\ \Phi(a_{n1}) & \cdots & \Phi(a_{nn}) \end{pmatrix} \end{gathered}$$

is positive.

The Stinespring dilation theorem states that for any ucp map $\Phi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$, there exists a Hilbert space $\mathcal{K}$, a representation $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{K})$, and an isometry $V : \mathcal{H} \to \mathcal{K}$ such that

$$\Phi(a) = V^*\pi(a)V$$

for all $a \in \mathcal{A}$. Moreover, if $\mathcal{H}$ is finite-dimensional, then $\mathcal{K}$ can be taken as finite-dimensional.

Given two C^*-algebras $\mathcal{A}$ and $\mathcal{B}$, their algebraic tensor product $\mathcal{A} \otimes \mathcal{B}$ is a $*$-algebra. There is more than one way to make $\mathcal{A} \otimes \mathcal{B}$ into a C^*-algebra. The first is to define the max-norm $\|\cdot\|_{max}$ on $\mathcal{A} \otimes \mathcal{B}$ by

$$\|a\|_{max} := \sup\{\|\pi(a)\|_{op} : \pi \text{ a representation of } \mathcal{A} \otimes \mathcal{B} \text{ on a Hilbert space } \mathcal{H}\} \tag{2.1.3}$$

The *max tensor product* of $\mathcal{A}$ and $\mathcal{B}$, denoted $\mathcal{A} \otimes_{max} \mathcal{B}$, is the closure of $\mathcal{A} \otimes \mathcal{B}$ with respect to $\|\cdot\|_{max}$. Representations π of $\mathcal{A} \otimes_{max} \mathcal{B}$ on a Hilbert space $\mathcal{H}$ correspond to pairs of representations $\pi_A : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ and $\pi_B : \mathcal{B} \to \mathcal{B}(\mathcal{H})$, such that $\pi(a \otimes b) = \pi_A(a)\pi_B(b) = \pi_B(b)\pi_A(a)$ for all $a \in \mathcal{A}, b \in \mathcal{B}$. This gives us another way to understand $\otimes_{max}$. If instead of looking for all representations on $\mathcal{A} \otimes \mathcal{B}$ in Equation (2.1.3), we look at representations of the form $\pi_A \otimes \pi_B$ where π_A and π_B are representations of $\mathcal{A}$ and $\mathcal{B}$ respectively, then we get a C^*-algebra $\mathcal{A} \otimes_{min} \mathcal{B}$ called the *min tensor product*. More precisely, we can fix faithful representations $\mathcal{A} \subset \mathcal{B}(\mathcal{H})$ and $\mathcal{B} \subset \mathcal{B}(\mathcal{K})$. Then $\mathcal{A} \otimes \mathcal{B} \subset \mathcal{B}(\mathcal{H} \otimes \mathcal{K})$ as a $*$-subalgebra. Restricting the operator norm on $\mathcal{B}(\mathcal{H} \otimes \mathcal{K})$ to $\mathcal{A} \otimes \mathcal{B}$ defines the min-norm $\|\cdot\|_{min}$. The C^*-algebra $\mathcal{A} \otimes_{min} \mathcal{B}$ is the closure of $\mathcal{A} \otimes \mathcal{B}$ with respect to $\|\cdot\|_{min}$. Note that $\mathcal{A} \otimes_{min} \mathcal{B}$ is independent of the choice of faithful representations $\mathcal{A} \subset \mathcal{B}(\mathcal{H})$ and $\mathcal{B} \subset \mathcal{B}(\mathcal{K})$.

We say a state $f : \mathcal{A} \otimes \mathcal{B} \to \mathbb{C}$ is *max-continuous* (resp. *min-continuous*) if it is continuous with respective to $\|\cdot\|_{max}$ (resp. $\|\cdot\|_{min}$). Equivalent, f is max-continuous (resp. min-continuous) if it extends to a state on $\mathcal{A} \otimes_{max} \mathcal{B}$ (resp. $\mathcal{A} \otimes_{min} \mathcal{B}$). By our definition of states, every state on $\mathcal{A} \otimes \mathcal{B}$ is max-continuous.

2.2 Quantum

2.2.1 Quantum states and measurements

Through Chapters 3 to 6, we use bra-ket notation for vectors in Hilbert spaces. A *vector state* is a unit vector in some Hilbert space. Given two vector states $|\alpha\rangle \in \mathcal{H}$ and $|\beta\rangle \in \mathcal{K}$, we often use $|\alpha, \beta\rangle$ to denote the product state $|\alpha\rangle \otimes |\beta\rangle \in \mathcal{H} \otimes \mathcal{K}$. We use $\{|i\rangle\}_{i=1}^{d}$ to denote the standard basis for the Euclidean space $\mathbb{C}^d$. Given two Hilbert space $\mathcal{H}_A$ and $\mathcal{H}_B$, every bipartite vector state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ has a *Schmidt decomposition*

$$|\psi\rangle = \sum_{i \in \mathcal{I}} \lambda_i |\alpha_i\rangle \otimes |\beta_i\rangle ,$$

where the index set $\mathcal{I}$ is either finite or countable, the *Schmidt coefficients* λ_i are strictly positive, and $\{|\alpha_i\rangle\}_{i \in \mathcal{I}}$ and $\{|\beta_i\rangle\}_{i \in \mathcal{I}}$ are orthonormal subsets of $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. The cardinality of $\mathcal{I}$ is called the *Schmidt rank* of $|\psi\rangle$. For a derivation of the Schmidt decomposition in infinite-dimensional spaces, see e.g. [CLP17, Theorem A.5].

Given a Hilbert space space $\mathcal{H}$, we call

$$C_1(\mathcal{H}) := \{T \in \mathcal{B}(\mathcal{H}) : \sum_{n=1}^{\infty} s_n(T) < \infty\}$$

the *trace class operators*, where $s_1(T) \geqslant s_2(T) \geqslant \cdots \geqslant 0$ are the *singular values* of T. For any $T \in C_1(\mathcal{H})$ and any orthonormal basis $\{|\alpha_i\rangle\}_{i \in \mathcal{I}}$ for $\mathcal{H}$,

$$\sum_{i \in \mathcal{I}} \langle \alpha_i | T | \alpha_i \rangle \tag{2.2.1}$$

converges and the value is independent of the choice of the orthonormal basis. We denote by $\mathrm{Tr}(T)$ the value of Equation (2.2.1) and call it the *trace of* T. An operator $\rho \in C_1(\mathcal{H})$ is called a *density operator* (or a quantum state) on $\mathcal{H}$ if ρ is a positive operator with $\mathrm{Tr}(\rho) = 1$. We say that a density operator ρ on $\mathcal{H}$ is a *pure quantum state* if $\rho = |\psi\rangle\langle\psi|$ for some vector state $|\psi\rangle \in \mathcal{H}$, and we say that ρ is a *mixed quantum state* if it is not a pure quantum state. Every density operator ρ on $\mathcal{H}$ induces a semi-norm $\|X\|_\rho := \sqrt{\mathrm{Tr}\big(X^* X \rho\big)}$ on $\mathcal{B}(\mathcal{H})$ which is called the ρ-norm.

A *positive operator-valued measure* (or POVM) on a Hilbert space $\mathcal{H}$ with finite index set $\mathcal{I}$ is a collection of positive operators $\{M_i : i \in \mathcal{I}\}$ on $\mathcal{H}$ such that $\sum_{i\in I} M_i = \mathbb{1}$. We say that a POVM $\{M_i\}_{i\in\mathcal{I}}$ is a *projection-valued measure* (or PVM) if in addition, the operators M_i are self-adjoint projections for all $i \in \mathcal{I}$. Naimark's dilation theorem states that for any POVM $\{M_i\}_{i\in\mathcal{I}}$ on a Hilbert space $\mathcal{H}$, there is a Hilbert space K, an isometry $V : \mathcal{H} \to \mathcal{K}$, and a PVM $\{P_i\}_{i\in\mathcal{I}}$ such that $M_i = V^* P_i V$. One common proof of the theorem is to take $\mathcal{K} = \mathcal{H} \otimes \mathbb{C}^{\mathcal{I}}$, $P_i = \mathbb{1}_{\mathcal{H}} \otimes |i\rangle\langle i|$, and $V : \mathcal{H} \to \mathcal{K}$ sending $|h\rangle \mapsto \sum_{i\in\mathcal{I}} M_i^{1/2} |h\rangle \otimes |i\rangle$, where $\{|i\rangle\}_{i\in\mathcal{I}}$ is the standard orthonormal basis for $\mathbb{C}^{\mathcal{I}}$.

Given a PVM $\{M_1, \ldots, M_m\} \subset \mathcal{B}(\mathcal{H})$, the corresponding *observable* is the unitary operator $A \in \mathcal{B}(\mathcal{H})$ of order m defined by

$$A := \sum_{k=1}^{m} \exp\left(\frac{2\pi\sqrt{-1}}{m} k\right) M_k.$$

If $m = 2$, then $A = M_1 - M_2$ is hermitian and we call it a *binary observable*.

2.2.2 Nonlocal games and correlations

Let X, Y, A, and B be finite sets. A *bipartite correlation* (or *behaviour*) is a function $p \in \mathbb{R}_{\geqslant 0}^{A\times B\times X\times Y}$ such that

$$\sum_{(a,b)\in A\times B} p(a, b|x, y) = 1$$

for all $x \in X$, $y \in Y$. A correlation can be thought of as specifying the probability of getting outputs $(a, b) \in A \times B$ from inputs $(x, y) \in X \times Y$. A *quantum model* for a correlation p is a tuple

$$S = (\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle),$$

where

(i) $\mathcal{H}_A$ and $\mathcal{H}_B$ are *finite-dimensional* Hilbert spaces,

(ii) $\{M_a^x : a \in A\}, x \in X$ and $\{N_b^y : b \in B\}, y \in Y$ are POVMs on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, and

(iii) $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a vector state,

such that

$$p(a,b|x,y) = \langle \psi | M_a^x \otimes N_b^y | \psi \rangle$$

for all $(a,b,x,y) \in A \times B \times X \times Y$.

Any tuple satisfying (i)-(iii) determines a correlation p via this last equation, and we refer to this as the correlation of the quantum model. A quantum model S for a correlation p is *projective* if the measurement operators $\{M_a^x : a \in A\}, x \in X$ and $\{N_b^y, b \in B\}, y \in Y$ are PVMs. A quantum model is *full-rank* if $\dim \mathcal{H}_A = \dim \mathcal{H}_B$, and the Schmidt rank of $|\psi\rangle$ is $\dim \mathcal{H}_A$.

The set of correlations in $\mathbb{R}_{\geqslant 0}^{A \times B \times X \times Y}$ which have a quantum model is convex, and is usually denoted by $C_q(X,Y,A,B)$. We use C_q to denote the union of $C_q(X,Y,A,B)$ over all finite sets X, Y, A, B. By the Naimark dilation theorem, every element of C_q has a projective quantum model, and by restricting to the support projection, every element of C_q also has a full-rank (but not necessarily projective) quantum model (see Section 3.1.2 for the definition of support projection). The sets C_q are not closed in general [Slo19], and the closure of C_q is denoted by C_{qa}. It also makes sense to talk about models in which the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are infinite-dimensional, and this leads to another set of correlations C_{qs} in between C_q and C_{qa}.

Aside from the above models that exhibit a tensor product structure, Algebraic Quantum Field Theory suggests a commuting-operator framework for correlations. A *commuting operator model* for a correlation p is a tuple

$$(\mathcal{H}, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle),$$

where

(i) $\mathcal{H}$ is a Hilbert space,

(ii) $\{M_a^x : a \in A\}$, $x \in X$ and $\{N_b^y : b \in B\}$, $y \in Y$ are POVMs on $\mathcal{H}$ such that

$$M_a^x N_b^y = N_b^y M_a^x$$

for all $(a, b, x, y) \in A \times B \times X \times Y$, and

(iii) $|\psi\rangle \in \mathcal{H}$ is a vector state

such that

$$p(a, b|x, y) = \langle \psi | M_a^x \cdot N_b^y | \psi \rangle$$

for all $(a, b, x, y) \in A \times B \times X \times Y$. We let C_{qc} be the set of correlations with a commuting operator model. It is well-known that C_{qc} is closed and convex, and the set of correlations with finite-dimensional commuting operator models is equal to C_q.

We refer to the correlations in C_q, C_{qs}, C_{qa}, and C_{qc} as quantum correlations, quantum spatial correlations, quantum approximable correlations, and quantum commuting correlations respectively.

Operationally, one can think that correlations arise from an interactive game: a referee samples a question pair (x, y) according to a distribution μ on $X \times Y$, sends x to the player Alice, and sends y to the player Bob; Alice and Bob then return $a \in A$ and $b \in B$ respectively. Their behavior is captured by a correlation $p \in \mathbb{R}_{\geqslant 0}^{A \times B \times X \times Y}$ where $p(a, b|x, y)$ indicates the probability that Alice and Bob return a and b upon receiving x and y. Based on a predicate $V : A \times B \times X \times Y \to \{0, 1\}$, the referee then determines whether the players win ($V(a, b|x, y) = 1$) or lose ($V(a, b|x, y) = 0$). We call the tuple $\mathcal{G} := (X, Y, A, B, \mu, V)$ a *nonlocal game*. Alice and Bob know the rules of $\mathcal{G}$ and can strategize together, but they are not allowed to communicate once the game begins.

Given a nonlocal game $\mathcal{G} = (X, Y, A, B, \mu, V)$ and a correlation $p \in \mathbb{R}_{\geqslant 0}^{A \times B \times X \times Y}$, the winning probability of p for $\mathcal{G}$ is

$$w(\mathcal{G}; p) := \sum_{a,b,x,y} \mu(x, y) V(a, b|x, y) p(a, b|x, y).$$

We refer to models for p as *strategies* for $\mathcal{G}$. Given a strategy S, we denote by $w(\mathcal{G}; S)$ (or simply $w(S)$ if $\mathcal{G}$ is clear from the context) the winning probability of S for $\mathcal{G}$. That is, $w(\mathcal{G}; S) = w(\mathcal{G}; p)$ where p is the correlation achieved by S. The *quantum value* $w_q(\mathcal{G})$ of

$\mathcal{G}$ is defined to be the supremum of $w(\mathcal{G}; S)$ over all quantum strategies S for $\mathcal{G}$. Since C_{qa} is the closure of C_q and C_{qs} is in between C_q and C_{qa},

$$w_q(\mathcal{G}) = \sup\{w(\mathcal{G}; p) : p \in C_q\} = \sup\{w(\mathcal{G}; p) : p \in C_{qs}\} = \sup\{w(\mathcal{G}; p) : p \in C_{qa}\}.$$

In this thesis, a correlation p (resp. a strategy S) is said to be *optimal*[1] for $\mathcal{G}$ if $w(\mathcal{G}; p) = w_q(\mathcal{G})$[2] (resp. $w(\mathcal{G}; S) = w_q(\mathcal{G})$).

2.2.3 Quantum circuits

In this thesis, we take σ_I, σ_X, and σ_Z to denote the following Pauli operators:

$$\sigma_I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and } \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

A *unitary quantum circuit* is simply a unitary which can be written as a product of gates from some universal gate set $\mathcal{U}$. Unless otherwise specified we will assume the universal gate set is the following universal gate set $\{H, \Lambda(X), \Lambda^2(X)\}$, where H is the Hadamard gate, $\Lambda(X)$ is the controlled σ_X gate, and $\Lambda^2(X)$ is the Toffoli gate. A *general quantum circuit* or simply a *quantum circuit* is a unitary quantum circuit that can additionally apply non-unitary gates which, introduce qubits initialized in the 0 state, trace out qubits, or measure qubits in the standard basis.

We say a family of quantum circuits $\{Q_n\}_{n\in\mathbb{N}}$ is a *polynomial-size family of quantum circuits* if there exists polynomial r such that Q_n has size at most $r(n)$. A family of quantum circuits $\{Q_n\}$ is called *polynomial-time uniform* family if there exists a polynomial time Turing machine that on input 1^n outputs a description of Q_n. In this case, the family will also be a polynomial-size family of quantum circuits.

[1] If $w_q(\mathcal{G}) = 1$, we often replace "optimal" with "perfect".

[2] One can also define the commuting-operator value $w_{co}(\mathcal{G}) := \sup\{w(\mathcal{G}; p) : p \in C_{qc}\}$. In this thesis, being optimal always means achieving the quantum value $w_q(\mathcal{G})$, even when we are working with $p \in C_{qc}$ or infinite-dimensional commuting-operator strategies.

Given a quantum circuit Q, we denote its size (number of gates plus number of wires) by $|Q|$. The task of delegating the computation of Q is captured by the following promise problem:

Definition 2.2.1 (Q-CIRCUIT)**.** *The input is a quantum circuit Q on n qubits. The problem is to decide between the following two cases:*

- *Yes:* $\|((|1\rangle\langle 1| \otimes I_{n-1})Q|0^n\rangle\|^2 \geqslant 1-\gamma$
- *No:* $\|((|1\rangle\langle 1| \otimes I_{n-1})Q|0^n\rangle\|^2 \leqslant \gamma$

where we are promised that one of the two cases holds.

Problem in Definition 2.2.1 is known to be BQP-complete for $1-2\gamma > \frac{1}{\text{poly}(n)}$.

2.3 Complexity

2.3.1 Notation

We take $[n]$ to denote the set $\{1, \ldots n\}$. Given two real valued functions $f, g : \mathbb{R} \to \mathbb{R}$, we write $f = O(g)$ (resp. $f = \Omega(g)$) if there exists a positive real number M and an $x_0 \in \mathbb{R}$ such that $|f(x)| \leqslant Mg(x)$ (resp. $|f(x)| \geqslant Mg(x)$) for all $x \geqslant x_0$. We call a function f negligible, and write $f = \text{negl}(n)$, if for all constants $c > 0$ we have $f = O(n^{-c})$. For two distributions P and Q on a finite set $\mathcal{X}$ the statistical differences of P and Q is given by $\sum_{x\in\mathcal{X}} |P(x) - Q(x)|$.

2.3.2 Computability

Given a set Σ, a word of length n over Σ is a finite sequence $a_1 a_2 \cdots a_n$, where $a_i \in \Sigma$ for all $1 \leqslant i \leqslant n$. We use the standard terminology from the theory of computation (see, e.g. [Sip12]). In particular, a subset $\mathcal{L}$ of words over Σ is in RE if there is a Turing machine M

with input alphabet Σ which recognizes $\mathcal{L}$, meaning that there is a computation path where M halts on input x if and only if $x \in \mathcal{L}$. In this definition M can be non-deterministic, but every language in RE can be recognized by a deterministic Turing machine. A language $\mathcal{L}$ is in coRE if its complement $\overline{\mathcal{L}}$ is in RE, and is decidable if it is in both RE and coRE. Equivalently, $\mathcal{L}$ is decidable if there is a deterministic Turing machine that halts on every input x, returning "accept" if $x \in \mathcal{L}$ and "reject" otherwise. Since many types of objects can be encoded as strings, we often talk about sets of other objects being RE or coRE. For instance, the set

$$\text{HALT} = \{(M, x) \text{ a Turing machine}, x \text{ an input to } M \mid M \text{ halts on input } x\}$$

is the prototypical example of an undecidable RE set, although formalizing it as a language requires choosing some encoding of pairs (M, x) as strings. The complement coHALT of pairs (M, x) such that M does not halt on input x is the prototypical example of an undecidable coRE set. A function f from strings on Σ to strings on Σ' is computable if there is a deterministic Turing machine with input alphabet Σ and output alphabet Σ' which takes input x to $f(x)$. A language $\mathcal{L}$ of strings over Σ is RE-hard (resp. coRE-hard) if there is a computable function f from pairs of Turing machines (M, x) to strings over Σ, such that $f(M, x) \in \mathcal{L}$ if and only if M halts on input x (sometimes this is called RE-hard under many-one reductions). Because natural numbers can be encoded as binary strings, we can also talk about RE, coRE, RE-hard, and coRE-hard subsets of $\mathbb{N}$.

We also care about how many steps it takes a Turing machine to accept an input. The time function of a non-deterministic Turing machine M is the function $T : \mathbb{N} \to \mathbb{N}$, where $T(n)$ is the smallest possible integer such that, given an input string x of length $\leqslant n$, if M halts on x, then some computation path of M halts in $\leqslant T(n)$ steps. We use the convention that every Turing machine takes at least one step to halt, so $T(n) \geqslant 1$ for all n. We say that $\mathcal{L}$ can be recognized in time $T' : \mathbb{N} \to \mathbb{N}$ if there is a Turing machine M recognizing $\mathcal{L}$ with time function $T(n) \leqslant T'(n)$ for all n. In particular, $\mathcal{L}$ can be recognized in polynomial time if it can be recognized in time Cn^k for some $C, k \in \mathbb{N}$. Similarly, we say that $\mathcal{L}$ can be recognized in deterministic time $T' : \mathbb{N} \to \mathbb{N}$ if there is a deterministic Turing machine M recognizing $\mathcal{L}$ with time function $T(n) \leqslant T'(n)$ for all n. A function f

is computable in time $T(n)$ if there is a deterministic Turing machine computing f which halts in $\leqslant T(n)$ steps on all input strings of length $\leqslant n$.

2.3.3 Quantum complexity classes

Definition 2.3.1 (QMA). *A promise problem $L = (L_{yes}, L_{no})$ is in* QMA *if there exist polynomials p and q, and a polynomial-time uniform family of quantum circuits $\{Q_n\}$ where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a $p(n)$-qubit quantum state $|\psi\rangle$, and $q(n)$ auxiliary qubits in state $|0\rangle^{\otimes q(n)}$, such that:*

- *(Completeness) if $x \in L_{yes}$, then there exists some $|\psi\rangle$ such that Q_n accepts $(x, |\psi\rangle)$ with probability at least $1 - \mathrm{negl}(n)$, and*
- *(Soundness) if $x \in L_{no}$, then for any state $|\psi\rangle$, Q_n accepts $(x, |\psi\rangle)$ with probability at most $\mathrm{negl}(n)$.*

The Hamiltonian of a quantum system is a Hermitian operator that encodes the energy of that system. The following *local Hamiltonian problem* plays a central role in quantum proofs. It was shown to be QMA complete for parameters $k = 5$ and $\beta - \alpha = \frac{1}{\mathrm{poly}(n)}$ [KSV02].

Definition 2.3.2. *Let $k \in \mathbb{N}$, $\alpha, \beta \in \mathbb{R}$ with $\alpha < \beta$, the k-*Local Hamiltonian *problem with parameters α and β is the following promise problem. Let n be the number of qubits of a quantum system. The input is a set of $m(n)$ Hamiltonians $H_1, \ldots, H_{m(n)}$ where m is a polynomial in n and each H_i acts on k qubits out of the n qubit system with $\|H_i\| \leqslant 1$. For $H = \sum_{j=1}^{m(n)} H_j$ the promise problem is to decide between the following.*

- ***Yes.*** *There exists an n-qubit state $|\varphi\rangle$ such that $\langle\varphi| H |\varphi\rangle \leqslant \alpha \cdot m(n)$.*
- ***No.*** *For every n-qubit state $|\varphi\rangle$ it holds that $\langle\varphi| H |\varphi\rangle \geqslant \beta \cdot m(n)$.*

We sometimes refer to the family of circuits $\{Q_n\}$ in Definition 2.3.1 simply as a family of *verification circuits*. Definition 2.3.1 can be understood as an interactive proof system.

In general, we consider multiple-prover interactive proof (MIP) systems in the quantum setting. This leads to the study of the class MIP^*. Informally, a language is in MIP^* if it can be decided by a polynomial-time classical verifier that interacts with *multiple* isolated, all-powerful and entangled provers. In this thesis, we only deal with MIP^* proof systems involving two provers and one round; which are defined as the following.

Definition 2.3.3. *A promise language $L = (L_{yes}, L_{no})$ is in $\mathsf{MIP}^*[2,1]_{c,s}$ if there exists a polynomial-time computable function that takes an instance $x \in L$ to a description of a non-local game $\mathcal{G}_x$ satisfying the following conditions.*

- *(Completeness) For every $x \in L_{yes}$ we have $\omega^*(\mathcal{G}_x) \geqslant c$.*
- *(Soundness) For every $x \in L_{no}$ we have $\omega^*(\mathcal{G}_x) < s$.*

We refer to the mapping, $x \mapsto \mathcal{G}_x$, as a $\mathsf{MIP}^*[2,1]_{c,s}$ proof system, or in some places a $\mathsf{MIP}^*[2,1]_{c,s}$ protocol. When the parameters are clear from the context we simply call it an MIP^* proof system.

Next, we discuss *zero knowledge*, which is an additional property for proof systems. Intuitively, in a zero-knowledge proof system, no verifier (including a malicious one) can learn anything beyond the membership in the language of the instance under consideration. For our scenario of $\mathsf{MIP}^*[2,1]$, it is sufficient to quantify over verifiers that send at most one valid question to each prover (otherwise, we can impose that the provers abort the protocol). Hence, a malicious verifier can only deviate from the honest one by sampling an initial question according to an alternate distribution, and by sampling the second question adaptively.

More formally, a malicious verifier $\widehat{V}$ is a probabilistic polynomial-time Turing (PPT) machine which on input x and randomness θ samples question q_1 for either Alice or Bob. Given reply r_1, the malicious verifier samples question q_2 in a way that may depend on q_1 and r_1. For a given quantum strategy $\mathcal{S}$ and malicious verifier $\widehat{V}$, we take $View(\widehat{V}(x), \mathcal{S})$ to be the random variable corresponding to the transcript of questions and answers $(x, \theta, q_1, r_1, q_2, r_1)$. A protocol is zero-knowledge when for all "yes" instances a simulator can sample from the distribution above.

Definition 2.3.4. *An* $\mathrm{MIP}^*[2,1]_{c,s}$ *proof system is* statistical zero-knowledge *if for every* $x \in L_{yes}$ *there exists an honest prover strategy* $\mathcal{S}$ *satisfying the following:*

1. $\omega^*(\mathcal{S}) \geqslant c$.

2. *For any PPT malicious verifier* $\widehat{V}$ *there exists a PPT simulator* $Sim_{\widehat{V}}$ *with output distribution that is* ϵ*-close to* $View(\widehat{V}(x), S)$ *in statistical distance for some negligible function* $\epsilon(|x|)$.

Chapter 3

Self-testing

3.1 An operator-algebraic formulation of self-testing

The standard definition of self-testing centres around the following notion of local dilations of quantum models:

Definition 3.1.1. *A quantum model*

$$\widetilde{S} = \left(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x : a \in A, x \in X\}, \{\widetilde{N}_b^y : b \in B, y \in Y\}, |\widetilde{\psi}\rangle\right)$$

is a ***local dilation*** *of another model*

$$S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\right),$$

denoted $S \succeq \widetilde{S}$, if there are finite-dimensional Hilbert spaces $\mathcal{H}_A^{aux}$ and $\mathcal{H}_B^{aux}$, a vector state $|aux\rangle \in \mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}$, and isometries $I_A : \mathcal{H}_A \to \widetilde{\mathcal{H}}_A \otimes \mathcal{H}_A^{aux}$ and $I_B : \mathcal{H}_B \to \widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}$ such that

$$(I_A \otimes I_B) \cdot (M_a^x \otimes N_b^y) |\psi\rangle = \left(\widetilde{M}_a^x \otimes \widetilde{N}_b^y |\widetilde{\psi}\rangle\right) \otimes |aux\rangle$$

for all $(a, b, x, y) \in A \times B \times X \times Y$.

Note that if $S \succeq \widetilde{S}$, then S and $\widetilde{S}$ give the same correlation. The relation $\succeq$ is a preorder, in the sense that it is transitive and reflexive, but is not anti-symmetric. We now recall the standard definition of self-testing for quantum models.

Definition 3.1.2. *Let $\mathcal{C}$ be a class of quantum models. A correlation p is a **self-test for the class** $\mathcal{C}$ if there is a model $\widetilde{S}$ for p in $\mathcal{C}$, such that $S \succeq \widetilde{S}$ for all other models S for p in $\mathcal{C}$.*

In Definition 3.1.2, we are primarily interested in the classes of projective quantum models and all quantum models, although we discuss several other classes at the beginning of this section. Stating Definition 3.1.2 for an arbitrary class $\mathcal{C}$ of quantum models lets us handle all these cases with one definition. For convenience, we refer to the models $\widetilde{S}$ and S appearing in Definition 3.1.2 as the *ideal model* and *employed model* respectively. In this language, a correlation is a self-test if any employed model for the correlation is equivalent to the ideal model up to local dilation.

3.1.1 Abstract state self-tests

Quantum models for correlations can also be expressed as states on C^*-algebras. Given finite sets X and A, define the *POVM algebra* $\mathcal{A}_{POVM}^{X,A}$ to be the universal C^*-algebra generated by positive contractions e_a^x, $x \in X$, $a \in A$, subject to the relations $\sum_{a \in A} e_a^x = 1$ for all $x \in X$. If $\phi : \mathcal{A}_{POVM}^{X,A} \to \mathcal{B}(\mathcal{H})$ is a representation of $\mathcal{A}_{POVM}^{X,A}$ on a Hilbert space $\mathcal{H}$, then $\{\phi(e_a^x) : a \in A\}$ is a POVM on $\mathcal{H}$. Conversely, given any collection $\{M_a^x : a \in A\}$, $x \in X$ of POVMs on a Hilbert space $\mathcal{H}$, there is a unique representation $\phi : \mathcal{A}_{POVM}^{X,A} \to \mathcal{B}(\mathcal{H})$ with $\phi(e_a^x) = M_a^x$. To distinguish the generators of $\mathcal{A}_{POVM}^{X,A}$ from the generators of $\mathcal{A}_{POVM}^{Y,B}$ for a given tuple (X, Y, A, B), we let $m_a^x := e_a^x \in \mathcal{A}_{POVM}^{X,A}$ and $n_b^y := e_b^y \in \mathcal{A}_{POVM}^{Y,B}$. If

$$S = (\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle)$$

is a quantum model for $p \in C_q$, then there is a (unique) representation $\phi_A \otimes \phi_B$ of the C^*-algebra $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ with $\phi_A(m_a^x) = M_a^x$ and $\phi_B(n_b^y) = N_b^y$ for all $(a, b, x, y) \in A \times B \times X \times Y$. We call $\phi_A \otimes \phi_B$ the *associated representation of S*. The abstract state f_S

on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ defined by $f_S(x) := \langle\psi|(\phi_A \otimes \phi_B)(x)|\psi\rangle$ is finite-dimensional, and satisfies

$$f_S(m_a^x \otimes n_b^y) = \langle\psi|\phi_A(m_a^x) \otimes \phi_B(n_b^y)|\psi\rangle = p(a,b|x,y). \tag{3.1.1}$$

We refer to f_S as the *abstract state defined by* S. Conversely, if f is a finite-dimensional state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$, then applying the double commutant theorem to a GNS representation of f yields a quantum model S such that $f = f_S$ [SW08]. In particular, a correlation $p \in \mathbb{R}_{\geqslant 0}^{A\times B\times X\times Y}$ belongs to C_q if and only if there is a finite-dimensional state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ with $f(m_a^x \otimes n_b^y) = p(a,b|x,y)$ for all $(a,b,x,y) \in A \times B \times X \times Y$. Consequently, a correlation p belongs to C_{qa} if and only if there is a (not necessarily finite-dimensional) state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ with $f(m_a^x \otimes n_b^y) = p(a,b|x,y)$ for all $(a,b,x,y) \in A \times B \times X \times Y$ [Fri12, JNP+11].

Other classes of models can be identified with subsets of states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. For instance, let $\mathcal{A}_{PVM}^{X,A}$ be the quotient of $\mathcal{A}_{POVM}^{X,A}$ by the relations $(e_a^x)^2 = e_a^x$ for all $x \in X$, $a \in A$ (the resulting algebra $\mathcal{A}_{PVM}^{X,A}$ is isomorphic to the group C^*-algebra $C^*(\mathbb{Z}_m^{*n})$, where $m = |A|$ and $n = |X|$). If

$$q : \mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B} \to \mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$$

is the quotient homomorphism, and f is a state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$, then $f \circ q$ is a state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. The pullback map $q^* : f \mapsto f \circ q$ is an injection, and hence identifies states on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ with a subset of states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. We say that a state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ is *projective* if it belongs to the image of q^*. A finite-dimensional state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ is projective if and only if $f = f_S$ for some projective quantum model S.

The first main contribution of this thesis is a definition of self-testing in terms of states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$.

Definition 3.1.3. *Let $\mathcal{S}$ be a subset of states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. A correlation p is an **abstract state self-test for $\mathcal{S}$** if there exists a unique abstract state $f \in \mathcal{S}$ with correlation p.*

The first main theorem of this thesis is that, in many cases, Definition 3.1.3 is equivalent to the standard definition of self-testing in Definition 3.1.2. To state this theorem in as much generality as possible, we make the following definitions:

Definition 3.1.4. *Let*

$$S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\right) \text{ and}$$
$$\widetilde{S} = \left(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x : a \in A, x \in X\}, \{\widetilde{N}_b^y : b \in B, y \in Y\}, |\widetilde{\psi}\rangle\right)$$

be two quantum models.

1. *We say that S and $\widetilde{S}$ are **locally equivalent**, and write $S \cong \widetilde{S}$, if there are local unitaries $U_A : \mathcal{H}_A \to \widetilde{\mathcal{H}}_A$ and $U_B : \mathcal{H}_B \to \widetilde{\mathcal{H}}_B$ such that*

   (i) $U_A \otimes U_B |\psi\rangle = |\widetilde{\psi}\rangle$, and

   (ii) $U_A M_a^x U_A^* = \widetilde{M}_a^x$ and $U_B N_b^y U_B^* = \widetilde{N}_b^y$ for all $(a, b, x, y) \in A \times B \times X \times Y$.

2. *We say $\widetilde{S}$ is a **submodel** of S if there are projections $\Pi_A \in \mathcal{B}(\mathcal{H}_A)$ and $\Pi_B \in \mathcal{B}(\mathcal{H}_B)$ such that $\Pi_A \mathcal{H}_A = \widetilde{\mathcal{H}}_A, \Pi_B \mathcal{H}_B = \widetilde{\mathcal{H}}_B$, $\Pi_A \otimes \Pi_B |\psi\rangle = \lambda |\widetilde{\psi}\rangle$ for some $\lambda \neq 0$, $\Pi_A M_a^x \Pi_A = \widetilde{M}_a^x$, $\Pi_B N_b^y \Pi_B = \widetilde{N}_b^y$, and $[\Pi_A, M_a^x] = [\Pi_B, N_b^y] = 0$ for all $(a, b, x, y) \in A \times B \times X \times Y$.*

*A class of quantum models $\mathcal{C}$ is **closed** if for any $S \in \mathcal{C}$, every $\widetilde{S}$ that is locally equivalent to a submodel of S is in $\mathcal{C}$.*

We can now state our first main theorem:

Theorem 3.1.5. *Let p be an extreme point in C_q, let $\mathcal{C}$ be a closed class of quantum models that contains a full-rank model for p, and let $\mathcal{S} := \{f_S : S \in \mathcal{C}\}$ be the set of finite-dimensional states induced by $\mathcal{C}$. Then p is a self-test for $\mathcal{C}$ if and only if p is an abstract state self-test for $\mathcal{S}$.*

The proof of Theorem 3.1.5 follows from Theorem 3.1.20 and Theorem 3.1.22. The hypotheses of Theorem 3.1.5 can actually be weakened a bit further: the "if" direction holds as long as p is extreme and $\mathcal{C}$ is closed, even if $\mathcal{C}$ does not contain a full-rank model for p; while the "only if" direction only requires that $\mathcal{C}$ is closed and contains a full-rank model for p. However, the assumption that p is extreme is necessary for the "if" direction, as shown by Example 3.1.23; and the condition that p has a full-rank model is necessary for the "only if" direction, which was shown in [BCK+23, Section 6.3].

The class of all quantum models and the class of projective quantum models are both closed. As discussed above, if $\mathcal{C}$ is the class of all quantum models, then $\{f_S : S \in \mathcal{C}\}$ is the set of all finite-dimensional states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$, while if $\mathcal{C}$ is the class of projective quantum models then $\{f_S : S \in \mathcal{C}\}$ is the set of projective finite-dimensional states. Also, every correlation in C_q has a full-rank quantum model. Thus for these two classes, Theorem 3.1.5 implies:

Corollary 3.1.6. *Suppose $p \in C_q(X, Y, A, B)$ is an extreme point. Then:*

(a) The correlation p is a self-test for the class of quantum models if and only if p is an abstract state self-test for finite-dimensional states.

(b) If p has a full-rank projective quantum model, then p is a self-test for projective quantum models if and only if p is an abstract state self-test for projective finite-dimensional states.

The proof of Corollary 3.1.6 is given in Section 3.2.1. In part (b), if p is an abstract state self-test for projective finite-dimensional states, then p is a self-test for projective quantum models even if p does not have a full-rank projective quantum model. As shown in [BCK+23], the hypothesis that p has a full-rank projective quantum model is required for the other direction. The correlation $\widetilde{p}$ constructed in [BCK+23, Section 6.3] does not have a full-rank projective quantum model, and this correlation is a self-test for projective quantum models but is not an abstract state self-test for projective finite-dimensional states.

In Section 3.2.1, we'll show that if a correlation $p \in C_q$ is a self-test for all quantum models (or equivalently, an abstract state self-test for the set of all finite-dimensional states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$), then it has a projective ideal model, and hence is a self-test for projective quantum models. The converse implication does not hold in general: the correlation $\widetilde{p}$ mentioned above is a self-test for projective quantum models but is not a self-test for all quantum models. Nonetheless, our second main result is that for quantum correlations that have full-rank projective models, every self-test for projective quantum model is also a self-test for all quantum models.

Theorem 3.1.7. *For any quantum correlation $p \in C_q$, the following statements hold.*

(a) If p is a self-test for all quantum models, then p has a full-rank projective ideal model and is a self-test for projective quantum models.

(b) If p is a self-test for projective quantum models and has a full-rank projective model, then p is a self-test for all quantum models.

Theorem 3.1.7 implies that many prominent self-tests for projective models, such as the CHSH game, Mermin-Peres magic square game, and so on, are also self-tests for POVM quantum models. In our paper [PSZZ23], we only proved a weaker version of part (b): for synchronous quantum correlations and extremal binary quantum correlations, every self-test for projective quantum models is also a self-test for all quantum models. Indeed, we proved this by first showing that every correlation in these two classes has a full-rank projective model. The general conclusion stated here follows from a recent result by Baptista, Chen, Kaniewski, Lolck, Mančinska, Gabelgaard Nielsen, and Schmidt in [BCK+23] (see Theorem 4.1 and 4.3 in their paper). In Section 3.2.1, I'll review their approach as well as our original proof.

When combining Corollary 3.1.6 and Theorem 3.1.7, we immediately see that:

Corollary 3.1.8. *If p is an extreme point in C_q and has a full-rank projective quantum model, then the following statements are equivalent:*

(1) p is a self-test for all quantum models.

(2) p is a self-test for projective quantum models.

(3) p is an abstract state self-test for finite-dimensional states.

(4) p is an abstract state self-test for projective finite-dimensional states.

Before starting to prove the main theorems, we note that a major advantage of Definition 3.1.3 is that it naturally generalizes to definitions of self-testing for other models of nonlocal correlations, including commuting operator models. We discuss this in Section 3.3. We prove Theorem 3.1.5 in the remaining of this section and prove Corollary 3.1.6 and Theorem 3.1.7 in Section 3.2.1. Unless stated otherwise, all the Hilbert spaces in this section and the next section are assumed to be finite-dimensional.

3.1.2 Self-tests are abstract state self-tests

We start by proving the "only if" direction of Theorem 3.1.5, that a self-test (as in Definition 3.1.2) is an abstract state self-test. For the purposes of this proof, we use the following terminology. If

$$S = (\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle)$$

is a quantum model, the *support* of $|\psi\rangle$ in $\mathcal{H}_A$ (resp. $\mathcal{H}_B$) is the image of the reduced density matrix $\rho_A := \mathrm{tr}_{\mathcal{H}_B}(|\psi\rangle\langle\psi|)$ (resp. $\rho_B = \mathrm{tr}_{\mathcal{H}_A}(|\psi\rangle\langle\psi|)$. The *support projections* Π_A and Π_B of $|\psi\rangle$ are the self-adjoint projections onto the support of $|\psi\rangle$ in $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Restricting to the support of $|\psi\rangle$ gives another quantum model

$$S' := (\Pi_A\mathcal{H}_A, \Pi_B\mathcal{H}_B, \{\Pi_A M_a^x \Pi_A\}, \{\Pi_B N_b^y \Pi_B\}, |\psi\rangle),$$

which we call the *support model* of S. The support model S' is a full-rank model, but is not necessarily a submodel of S if Π_A and Π_B do not commute with all the measurement operators M_a^x and N_b^y. We say that S is *centrally supported* if

$$[\Pi_A, M_a^x] = [\Pi_B, N_b^y] = 0$$

for all $(a, b, x, y) \in A \times B \times X \times Y$. The support model S' of a quantum model S is a submodel of S if and only if S is centrally supported. Any full-rank model is centrally supported, since the support projections are the identity operators. Conversely, if S is centrally supported, then its support model is a full-rank submodel of S. Hence we have:

Lemma 3.1.9. *Let $\mathcal{C}$ be a closed class of quantum models, and let $p \in C_q$. Then $\mathcal{C}$ contains a centrally supported model for p if and only if $\mathcal{C}$ contains a full-rank model for p.*

For later use, we note the following two lemmas:

Lemma 3.1.10. *If S is a centrally supported model with support model S', then $S' \geq S$ and $S \geq S'$.*

Proof. Suppose $S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\right)$ is a centrally supported quantum model. Let Π_A and Π_B be the support projections of $|\psi\rangle$, and let $S' = (\mathcal{H}'_A, \mathcal{H}'_B, \{\widehat{M}_a^x\}, \{\widehat{N}_b^y\}, |\psi\rangle)$ be the support model for S, so $\mathcal{H}'_A = \Pi_A \mathcal{H}_A$, $\mathcal{H}'_B = \Pi_B \mathcal{H}_B$, $\widehat{M}_a^x = \Pi_A M_a^x \Pi_A$, and $\widehat{N}_b^y = \Pi_B N_b^y \Pi_B$. Since

$$\widehat{M}_a^x \otimes \widehat{N}_b^y |\psi\rangle = M_a^x \otimes N_b^y |\psi\rangle \text{ for all } a \in A, b \in B, x \in X, y \in Y,$$

it follows that $S' \geq S$.

To see $S \geq S'$, pick an arbitrary unit vector $|w_A\rangle \in \mathcal{H}'_A$, and define an isometry $I_A : \mathcal{H}_A \to \mathcal{H}'_A \otimes \mathcal{H}_A$ by $I_A(v) = v \otimes |w_A\rangle$ if $v \in \mathcal{H}'_A$, and $I_A(v) = |w_A\rangle \otimes v$ if $v \in (\mathcal{H}'_A)^\perp$. Similarly, define an isometry $I_B : \mathcal{H}_B \to \mathcal{H}'_B \otimes \mathcal{H}_B$ using a vector $|w_B\rangle \in \mathcal{H}'_B$. Using the fact that S is centrally supported,

$$\begin{aligned}(I_A \otimes I_B) M_a^x \otimes N_b^y |\psi\rangle &= (I_A \otimes I_B) \Pi_A M_a^x \Pi_A \otimes \Pi_B N_b^y \Pi_B |\psi\rangle \\ &= (\widehat{M}_a^x \otimes \widehat{N}_b^y |\psi\rangle) \otimes |w_A\rangle \otimes |w_B\rangle\end{aligned}$$

for all $x \in X$, $a \in A$, $y \in Y$, $b \in B$, so $S \geq S'$. □

Lemma 3.1.11. *Two projections $P, Q \in \mathcal{B}(\mathcal{H})$ commute if and only if PQP is a projection.*

Proof. The "only if" direction is obvious. For the "if" direction, suppose PQP is a projection, i.e., $PQPQP = PQP$. Let $S := PQ(\mathbb{1} - P)$. Then $SS^* = PQ(\mathbb{1} - P)QP = PQP - PQPQP = 0$, which implies $S = 0$. Hence $PQ = PQP$. Then $QP = (PQ)^* = (PQP)^* = PQP = PQ$. □

Although we won't use it, Lemma 3.1.11 immediately implies that the support model of a centrally supported projective model remains projective:

Proposition 3.1.12. *Suppose S is a projective quantum model and is centrally supported, then its support model S' is projective.*

We will now provide a useful characterization of centrally supported quantum models. To do this, we first need to establish the following lemmas.

Lemma 3.1.13. *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite vector state, and let Π_A and Π_B be the support projections of $|\psi\rangle$. For any self-adjoint operator $E \in \mathcal{B}(\mathcal{H}_A)$, if there exists an operator $\widehat{E} \in \mathcal{B}(\mathcal{H}_B)$ such that $E \otimes \mathbb{1} |\psi\rangle = \mathbb{1} \otimes \widehat{E} |\psi\rangle$, then the support projection Π_A commutes with E.*

Proof. Let $|\psi\rangle = \sum_{i=1}^{k} \lambda_i |\alpha_i\rangle \otimes |\beta_i\rangle$ be a Schmidt decomposition of $|\psi\rangle$, so the support projection of $|\psi\rangle$ on $\mathcal{H}_A$ is $\Pi_A = \sum_{i=1}^{k} |\alpha_i\rangle\langle\alpha_i|$. Suppose there exists an operator $\widehat{E} \in \mathcal{B}(\mathcal{H}_B)$ such that $E \otimes \mathbb{1} |\psi\rangle = \mathbb{1} \otimes \widehat{E} |\psi\rangle$. Then

$$\Pi_A E \otimes \mathbb{1} |\psi\rangle = \Pi_A \otimes \widehat{E} |\psi\rangle = \mathbb{1} \otimes \widehat{E} |\psi\rangle = E \otimes \mathbb{1} |\psi\rangle,$$

or in other words $(\mathbb{1} - \Pi_A)E \otimes \mathbb{1} |\psi\rangle = 0$. This implies

$$\sum_{i=1}^{k} \lambda_i \big((\mathbb{1} - \Pi_A)E |\alpha_i\rangle\big) \otimes |\beta_i\rangle = 0,$$

and since $\lambda_i > 0$ for all $1 \leqslant i \leqslant k$ and $\{|\beta_i\rangle : 1 \leqslant i \leqslant k\}$ is an orthonormal subset, it follows that $(\mathbb{1} - \Pi_A)E |\alpha_i\rangle = 0$ for all $1 \leqslant i \leqslant k$. Hence,

$$(\mathbb{1} - \Pi_A)E\Pi_A = \sum_{i=1}^{k} (\mathbb{1} - \Pi_A)E |\alpha_i\rangle\langle\alpha_i| = 0,$$

and $E\Pi_A = \Pi_A E\Pi_A$. Since E is self-adjoint, $\Pi_A E = (E\Pi_A)^* = \Pi_A E\Pi_A = E\Pi_A$. □

Lemma 3.1.14. *If $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a full-rank vector state, then for any $E \in \mathcal{B}(\mathcal{H}_A)$ (resp. $F \in \mathcal{B}(\mathcal{H}_B)$) there is an operator $\widehat{E} \in \mathcal{B}(\mathcal{H}_B)$ (resp. $\widehat{F} \in \mathcal{B}(\mathcal{H}_A)$) such that $E \otimes \mathbb{1} |\psi\rangle = \mathbb{1} \otimes \widehat{E} |\psi\rangle$ (resp. $\mathbb{1} \otimes F |\psi\rangle = \widehat{F} \otimes \mathbb{1} |\psi\rangle$).*

Proof. Since the vector state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is full-rank, we can assume without loss of generality that $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^k$ and $|\psi\rangle$ has Schmidt decomposition

$$|\psi\rangle = \sum_{i=1}^{k} \lambda_i |i\rangle \otimes |i\rangle .$$

Let $\lambda := \sum_{i=1}^k \lambda_i |i\rangle\langle i|$ and $|\tau\rangle := \sum_{i=1}^k |i\rangle \otimes |i\rangle$. Then λ is invertible and $|\psi\rangle = \mathbb{1} \otimes \lambda |\tau\rangle = \lambda \otimes \mathbb{1} |\tau\rangle$. Given $E \in \mathcal{B}(\mathcal{H}_A)$, let $\widehat{E} := \lambda E^T \lambda^{-1}$, where E^T is the transpose of E in the standard basis. Since $\mathbb{1} \otimes M^T |\tau\rangle = M \otimes \mathbb{1} |\tau\rangle$ for any operator M,

$$\mathbb{1} \otimes \widehat{E} |\psi\rangle = (\mathbb{1} \otimes \lambda E^T \lambda^{-1})(\mathbb{1} \otimes \lambda) |\tau\rangle = \mathbb{1} \otimes \lambda E^T |\tau\rangle = E \otimes \lambda |\tau\rangle = E \otimes \mathbb{1} |\psi\rangle .$$

The existence of $\widehat{F}$ for F follows similarly. □

Proposition 3.1.15. *A quantum model*

$$S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\big)$$

is centrally supported if and only if for every $a \in A$, $x \in X$ (resp. $b \in B$, $y \in Y$) there exists an operator $\widehat{M}_a^x \in \mathcal{B}(\mathcal{H}_B)$ (resp. $\widehat{N}_b^y \in \mathcal{B}(\mathcal{H}_A)$) such that $M_a^x \otimes \mathbb{1}|\psi\rangle = \mathbb{1} \otimes \widehat{M}_a^x |\psi\rangle$ (resp. $\mathbb{1} \otimes N_b^y |\psi\rangle = \widehat{N}_b^y \otimes \mathbb{1} |\psi\rangle$) .

Proof. The "if" part follows directly from Lemma 3.1.13. For the "only if" part, let Π_A and Π_B be the support projections of $|\psi\rangle$, and suppose $[\Pi_A, M_a^x] = [\Pi_B, N_b^y] = 0$ for all $(a, b, x, y) \in A \times B \times X \times Y$. Since $\Pi_A \otimes \Pi_B |\psi\rangle$ is full-rank in $(\Pi_A \mathcal{H}_A) \otimes (\Pi_B \mathcal{H}_B)$, by Lemma 3.1.14 there is an operator $\widehat{M}_a^x$ in $\mathcal{B}(\Pi_B \mathcal{H}_B)$ (which is also an operator in $\mathcal{B}(\mathcal{H}_B)$ acting trivially on $(\mathbb{1} - \Pi_B)\mathcal{H}_B$) such that $\Pi_A M_a^x \Pi_A \otimes \Pi_B |\psi\rangle = \Pi_A \otimes \widehat{M}_a^x \Pi_B |\psi\rangle$ for any $a \in A, x \in X$. Therefore

$$M_a^x \otimes \mathbb{1} |\psi\rangle = M_a^x \Pi_A \otimes \Pi_B |\psi\rangle = \Pi_A M_a^x \Pi_A \otimes \Pi_B |\psi\rangle = \Pi_A \otimes \widehat{M}_a^x \Pi_B |\psi\rangle = \mathbb{1} \otimes \widehat{M}_a^x |\psi\rangle .$$

Similarly, for any $b \in B, y \in Y$ there is $\widehat{N}_b^y \in \mathcal{B}(\mathcal{H}_A)$ such that $\mathbb{1} \otimes N_b^y |\psi\rangle = \widehat{N}_b^y \otimes \mathbb{1} |\psi\rangle$. □

This characterization allows us to show that centrally supported models can only locally dilate to centrally supported models:

Proposition 3.1.16. *Suppose S and $\widetilde{S}$ are two quantum models such that $S \succeq \widetilde{S}$. Then S is centrally supported if and only if $\widetilde{S}$ is centrally supported.*

Proof. Suppose

$$S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\right) \text{ and}$$
$$\widetilde{S} = \left(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\widetilde{\psi}\rangle\right)$$

are two quantum models for a quantum correlation p such that $S \succeq \widetilde{S}$ with local isometries I_A, I_B and vector state $|aux\rangle \in \mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}$. Let Π_A, Π_B and $\widetilde{\Pi}_A, \widetilde{\Pi}_B$ be the support projections of S and $\widetilde{S}$ respectively.

For the "if" direction, suppose $\widetilde{S}$ is centrally supported. Then for any $x \in X$, $a \in A$, by Proposition 3.1.15, there is an operator $F_a^x \in \mathcal{B}(\widetilde{\mathcal{H}}_B)$ such that $\widetilde{M}_a^x \otimes \mathbb{1} |\widetilde{\psi}\rangle = \mathbb{1} \otimes F_a^x |\widetilde{\psi}\rangle$. This implies $\widehat{M}_a^x := I_B^*(F_a^x \otimes \mathbb{1}_{\mathcal{H}_B^{aux}})I_B$ is an operator in $\mathcal{B}(\mathcal{H}_B)$ such that

$$\begin{aligned}
\mathbb{1} \otimes \widehat{M}_a^x |\psi\rangle &= I_A^* I_A \otimes I_B^*(F_a^x \otimes \mathbb{1}_{\mathcal{H}_B^{aux}})I_B |\psi\rangle \\
&= I_A^* \otimes I_B^* \left(\mathbb{1}_{\widetilde{\mathcal{H}}_A} \otimes F_a^x \otimes \mathbb{1}_{\mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}} (I_A \otimes I_B |\psi\rangle)\right) \\
&= I_A^* \otimes I_B^* \left((\mathbb{1}_{\widetilde{\mathcal{H}}_A} \otimes F_a^x |\psi\rangle) \otimes |aux\rangle\right) \\
&= I_A^* \otimes I_B^* \left((\widetilde{M}_a^x \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B^{aux}} |\psi\rangle) \otimes |aux\rangle\right) = M_a^x \otimes \mathbb{1} |\psi\rangle .
\end{aligned}$$

Similarly, for any $b \in B$, $y \in Y$, there is a $\widehat{N}_b^y \in \mathcal{B}(\mathcal{H}_A)$ such that $\mathbb{1} \otimes N_b^y |\psi\rangle = \widehat{N}_b^y \otimes \mathbb{1} |\psi\rangle$. By Proposition 3.1.15 again, this means S is centrally supported.

For the "only if" direction, suppose S is centrally supported. Then

$$S' := \left(\widetilde{\mathcal{H}}_A \otimes \mathcal{H}_A^{aux}, \widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}, \{\widetilde{M}_a^x \otimes \mathbb{1}_{\mathcal{H}_A^{aux}}\}, \{\widetilde{N}_b^y \otimes \mathbb{1}_{\mathcal{H}_B^{aux}}\}, |\widetilde{\psi}, aux\rangle\right)$$

is a quantum model for p with support projections $\widetilde{\Pi}_A \otimes \Pi_A^{aux}$ and $\widetilde{\Pi}_B \otimes \Pi_B^{aux}$ where $\Pi_A^{aux} \in \mathcal{B}(\mathcal{H}_A^{aux})$ and $\Pi_B^{aux} \in \mathcal{B}(\mathcal{H}_B^{aux})$ are the support projections of $|aux\rangle$. Since S is

centrally supported, for any $x \in X, a \in A$, by Proposition 3.1.15, there is an operator $\widehat{M}_a^x \in \mathcal{B}(\mathcal{H}_B)$ such that $M_a^x \otimes \mathbb{1} |\psi\rangle = \mathbb{1} \otimes \widehat{M}_a^x |\psi\rangle$. Since $I_A I_A^* \otimes I_B I_B^* |\widetilde{\psi}, aux\rangle = |\widetilde{\psi}, aux\rangle$ and $I_A I_A^* \otimes \mathbb{1} \geqslant I_A I_A^* \otimes I_B I_B^*$, we see that $I_A I_A^* \otimes \mathbb{1} |\widetilde{\psi}, aux\rangle = |\widetilde{\psi}, aux\rangle$. Then $I_B \widehat{M}_a^x I_B^*$ is an operator in $\mathcal{B}(\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux})$ such that

$$\begin{aligned}
\mathbb{1} \otimes I_B \widehat{M}_a^x I_B^* |\widetilde{\psi}, aux\rangle &= I_A I_A^* \otimes I_B \widehat{M}_a^x I_B^* |\widetilde{\psi}, aux\rangle \\
&= (I_A \otimes I_B)(\mathbb{1} \otimes \widehat{M}_a^x |\psi\rangle) \\
&= (I_A \otimes I_B)(M_a^x \otimes \mathbb{1} |\psi\rangle) \\
&= (\widetilde{M}_a^x \otimes \mathbb{1}_{\mathcal{H}_A^{aux}}) \otimes \mathbb{1} |\widetilde{\psi}, aux\rangle .
\end{aligned}$$

By Lemma 3.1.13 we see that $\widetilde{\Pi}_A \otimes \Pi_A^{aux}$ commutes with $\widetilde{M}_a^x \otimes \mathbb{1}_{\mathcal{H}_A^{aux}}$, and hence $[\widetilde{\Pi}_A, \widetilde{M}_a^x] = 0$ for all $x \in X, a \in A$. Similarly, $[\widetilde{\Pi}_B, \widetilde{N}_b^y] = 0$ for all $y \in Y, b \in B$. We conclude that $\widetilde{S}$ is centrally supported. □

As an immediate consequence, we have:

Corollary 3.1.17. *Suppose p is a self-test for a class of quantum models $\mathcal{C}$ and $\mathcal{C}$ contains a centrally supported model for p, then every model in $\mathcal{C}$ for p is centrally supported. If in addition, $\mathcal{C}$ is closed, then p has a full-rank ideal model in $\mathcal{C}$.*

Proof. Let S be a centrally supported model in $\mathcal{C}$ for p, and let $\widetilde{S}$ be an ideal model in $\mathcal{C}$ for p. Since $S \succeq \widetilde{S}$, by Proposition 3.1.16, $\widetilde{S}$ must be centrally supported and hence all models in $\mathcal{C}$ for p are centrally supported. If $\mathcal{C}$ is closed, then by Lemmas 3.1.9 and 3.1.10, the support model S' of $\widetilde{S}$ is in $\mathcal{C}$ and is a full-rank ideal model for p. □

In particular, Corollary 3.1.17 applies to the class of all quantum models $\mathcal{C}_{POVM}$. In fact, we can say more about the ideal model in this case. We prove stronger versions of Corollary 3.1.17 for $\mathcal{C}_{POVM}$ in Propositions 3.2.1 and 3.2.3.

The following proposition shows that two quantum models S and $\widetilde{S}$ with $S \succeq \widetilde{S}$ induce the same abstract state if one of them (hence both of them) is centrally supported.

Proposition 3.1.18. *Let*

$$S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\right) \text{ and}$$
$$\widetilde{S} = \left(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\widetilde{\psi}\rangle\right)$$

be two quantum models for a correlation $p \in C_q(X, Y, A, B)$, with associated representations $\pi_A \otimes \pi_B$ and $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$ respectively. Suppose $S \succeq \widetilde{S}$ via local isometries I_A and I_B and vector state $|aux\rangle \in \mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}$. If either S or $\widetilde{S}$ is centrally supported, then

$$(\widetilde{\pi}_A(\alpha) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle) \otimes |aux\rangle = I_A \pi(\alpha) I_A^* \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \text{ for all } \alpha \in \mathcal{A}_{POVM}^{X,A}, \quad (3.1.2)$$

$$(\mathbb{1}_{\widetilde{\mathcal{H}}_A} \otimes \widetilde{\pi}_B(\beta) |\widetilde{\psi}\rangle) \otimes |aux\rangle = \mathbb{1}_{\widetilde{\mathcal{H}}_A \otimes \mathcal{H}_A^{aux}} \otimes I_B \pi(\beta) I_B^* |\widetilde{\psi}, aux\rangle \text{ for all } \beta \in \mathcal{A}_{POVM}^{Y,B}, \quad (3.1.3)$$

and $f_S = f_{\widetilde{S}}$.

Proof. By Proposition 3.1.16, both S and $\widetilde{S}$ are centrally supported. To prove Equation (3.1.2), we first show that this equation holds for all monomials $\alpha = \alpha_1 \cdots \alpha_k \in \mathcal{A}_{POVM}^{X,A}$, $\alpha_i \in \{e_a^x : x \in X, a \in A\}$ by induction on the monomial degree $k \in \mathbb{N}$. Indeed, the cases $k = 0, 1$ follow straight from Definition 3.1.1. Suppose that Equation (3.1.2) holds for all monomials in $\mathcal{A}_{POVM}^{X,A}$ of degree k. For any monomial $\alpha = \alpha_1 \cdots \alpha_k \alpha_{k+1}$ in $\mathcal{A}_{POVM}^{X,A}$ of degree $k+1$, let $\alpha' := \alpha_1 \cdots \alpha_k$. Since $\widetilde{S}$ is centrally supported, by Proposition 3.1.15 there is an $\widetilde{F} \in \mathcal{B}(\widetilde{\mathcal{H}}_B)$ such that $\widetilde{\pi}_A(\alpha_{k+1}) \otimes \mathbb{1} |\widetilde{\psi}\rangle = \mathbb{1} \otimes \widetilde{F} |\widetilde{\psi}\rangle$. Thus by the inductive hypothesis,

$$\begin{aligned}
\left(\widetilde{\pi}_A(\alpha) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle\right) \otimes |aux\rangle &= \left(\widetilde{\pi}_A(\alpha')\widetilde{\pi}_A(\alpha_{k+1}) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \\
&= \left(\widetilde{\pi}_A(\alpha') \otimes \widetilde{F} |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \\
&= I_A \pi_A(\alpha') I_A^* \otimes \widetilde{F} \otimes \mathbb{1}_{\mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \\
&= \left(I_A \pi_A(\alpha') I_A^* (\widetilde{\pi}(\alpha_{k+1}) \otimes \mathbb{1}_{\mathcal{H}_A^{aux}})\right) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \\
&= \left(I_A \pi_A(\alpha') I_A^* I_A \pi_A(\alpha_{k+1}) I_A^*\right) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \\
&= I_A \pi_A(\alpha) I_A^* \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle .
\end{aligned}$$

We conclude that Equation (3.1.2) holds for all α. The proof of Equation (3.1.3) is similar. Hence, for any $\alpha \in \mathcal{A}_{POVM}^{X,A}$ and $\beta \in \mathcal{A}_{POVM}^{Y,B}$,

$$f_{\widetilde{S}}(\alpha \otimes \beta) = \langle \widetilde{\psi}| \widetilde{\pi}_A(\alpha) \otimes \widetilde{\pi}_B(\beta) |\widetilde{\psi}\rangle$$

$$
\begin{aligned}
&= \langle \widetilde{\psi}, aux | \, \widetilde{\pi}_A(\alpha) \otimes \widetilde{\pi}_B(\beta) \otimes \mathbb{1}_{\mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}} \, | \widetilde{\psi}, aux \rangle \\
&= \langle \widetilde{\psi}, aux | \, I_A \pi_A(\alpha) I_A^* \otimes I_B \pi_B(\beta) I_B^* \, | \widetilde{\psi}, aux \rangle \\
&= \langle \psi | \, \pi_A(\alpha) \otimes \pi_B(\beta) \, | \psi \rangle \\
&= f_S(\alpha \otimes \beta),
\end{aligned}
$$

which implies $f_S = f_{\widetilde{S}}$. □

For later use, we note that when combining Lemma 3.1.10 and Proposition 3.1.18 we have

Corollary 3.1.19. *Suppose S is a centrally supported model, and let S' its support model. Then $f_S = f_{S'}$.*

We can now prove the "only if" direction of Theorem 3.1.5 (with the weaker hypotheses mentioned after the theorem statement).

Theorem 3.1.20. *Let $p \in C_q(X, Y, A, B)$. Let $\mathcal{C}$ be a class of quantum models that is closed and contains a full-rank model for p, and let $\mathcal{S} = \{f_S : S \in \mathcal{C}\}$. If p is a self-test for $\mathcal{C}$ then p is an abstract state self-test for $\mathcal{S}$.*

Proof. Let S be a full-rank model in $\mathcal{C}$ for p. Suppose p is a self-test for $\mathcal{C}$, and let $\widetilde{S} \in \mathcal{C}$ be an ideal model for p, so $S \succeq \widetilde{S}$. Full-rank models are centrally supported, so $\widetilde{S}$ is centrally supported by Proposition 3.1.16. Then Proposition 3.1.18 implies that $f_{\widetilde{S}}$ is the unique state in $\mathcal{S}$ achieving p. □

As mentioned in Section 3.1, the assumption that $\mathcal{C}$ contains a full-rank model for p is crucial for Theorem 3.1.20. In [BCK+23], Baptista, Chen, Kaniewski, Lolck, Mančinska, Gabelgaard Nielsen, and Schmidt construct a quantum correlation $\widetilde{p}$ where the class of projective quantum models contains no full-rank models for $\widetilde{p}$. They further show that $\widetilde{p}$ is a self-test for projective quantum models but not an abstract state self-test for finite-dimensional projective states.

3.1.3 Abstract state self-tests are self-tests

Before we can establish the "if" direction of Theorem 3.1.5 we need to review some basic facts about the representation theory of C^*-algebras. For more details we refer the reader to [Bla06].

Lemma 3.1.21. *Let $\pi_A : \mathcal{A} \to \mathcal{B}(\mathcal{H}_A)$ and $\widetilde{\pi}_A : \mathcal{A} \to \mathcal{B}(\widetilde{\mathcal{H}}_A)$ be two representations of a C^*-algebra $\mathcal{A}$, and let $\pi_B : \mathcal{B} \to \mathcal{B}(\mathcal{H}_B)$ and $\widetilde{\pi}_B : \mathcal{B} \to \mathcal{B}(\widetilde{\mathcal{H}}_B)$ be two representations of a C^*-algebra $\mathcal{B}$.*

(1) $\pi_A \otimes \pi_B$ is irreducible if and only if π_A and π_B are irreducible.

(2) Suppose π_A and π_B are irreducible. Let $|\psi\rangle$ and $|\psi'\rangle$ be two vector states in $\mathcal{H}_A \otimes \mathcal{H}_B$. If $(\pi_A \otimes \pi_B, \mathcal{H}_A \otimes \mathcal{H}_B, |\psi\rangle)$ and $(\pi_A \otimes \pi_B, \mathcal{H}_A \otimes \mathcal{H}_B, |\psi'\rangle)$ are GNS representations for the same state, then $|\psi\rangle\langle\psi| = |\psi'\rangle\langle\psi'|$ (in other words, the states $|\psi\rangle$ and $|\psi'\rangle$ only differ by a complex phase).

(3) Suppose $\pi_A, \widetilde{\pi}_A, \pi_B$ and $\widetilde{\pi}_B$ are irreducible. Then $\pi_A \otimes \pi_B \cong \widetilde{\pi}_A \otimes \widetilde{\pi}_B$ if and only if $\pi_A \cong \widetilde{\pi}_A$ and $\pi_B \cong \widetilde{\pi}_B$.

Proof. Part (1) is an immediate consequence of Schur's lemma, along with the fact that $\big(\pi_A(\mathcal{A}) \otimes \pi_B(\mathcal{B})\big)' = \big(\pi_A(\mathcal{A})\big)' \otimes \big(\pi_B(\mathcal{B})\big)'$ [Bla06, III.4.5.8].

For part (2), since GNS representations of a state are unitarily equivalent, there exists a unitary operator U acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ such that

$$U|\psi\rangle = |\psi'\rangle, \text{ and} \tag{3.1.4}$$

$$U\pi_A(\alpha) \otimes \pi_B(\beta)U^* = \pi_A(\alpha) \otimes \pi_B(\beta) \text{ for all } \alpha \in \mathcal{A}, \beta \in \mathcal{B}. \tag{3.1.5}$$

Since π_A and π_B are irreducible, part (1) and Equation (3.1.5) implies that $U \in \big(\pi_A(\mathcal{A}) \otimes \pi_B(\mathcal{B})\big)' = \mathbb{C}\mathbb{1}$. Then part (2) follows from Equation (3.1.4).

For part (3), if $\pi_A \otimes \pi_B \cong \widetilde{\pi}_A \otimes \widetilde{\pi}_B$ as an $\mathcal{A} \otimes \mathcal{B}$-module, then $\pi_A \otimes \mathbb{1}_{\mathcal{H}_B} \cong \widetilde{\pi}_A \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B}$ as an $\mathcal{A}$-module. But this requires $\pi_A \cong \widetilde{\pi}_A$ by Schur's lemma. □

We note that Lemma 3.1.21 and its proof hold for representations of C^*-algebras on infinite-dimensional Hilbert spaces.

Now we are ready to prove the "if" direction of Theorem 3.1.5 (with, again, the weaker hypotheses mentioned after the theorem statement).

Theorem 3.1.22. *Let $p \in C_q(X, Y, A, B)$ be an extreme point in C_q, let $\mathcal{C}$ be a class of quantum models that is closed, and let $\mathcal{S} = \{f_S : S \in \mathcal{C}\}$. If p is an abstract state self-test for $\mathcal{S}$, then p is a self-test for $\mathcal{C}$, and furthermore p has an ideal model $\widetilde{S}$ such that the associated representation $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$ is irreducible.*

Proof. Let f be the unique state in $\mathcal{S}$ achieving p. Given a quantum model

$$S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\right)$$

in $\mathcal{C}$ for p with the associated representation $\pi_A \otimes \pi_B$, we can decompose the local Hilbert spaces and associated representations with the double-commutant theorem to get

$$\begin{aligned}
\mathcal{H}_A &= \bigoplus_i \mathcal{H}_i^A \otimes K_i^A, \quad \pi_A(\mathcal{A}_{POVM}^{X,A}) = \bigoplus_i \mathcal{B}(\mathcal{H}_i^A) \otimes \mathbb{1}_{K_i^A}, \text{ and} \\
\mathcal{H}_B &= \bigoplus_j \mathcal{H}_j^B \otimes K_j^B, \quad \pi_B(\mathcal{A}_{POVM}^{Y,B}) = \bigoplus_j \mathcal{B}(\mathcal{H}_j^B) \otimes \mathbb{1}_{K_j^B}
\end{aligned}$$

for some Hilbert spaces $\mathcal{H}_i^A, K_i^A, \mathcal{H}_j^B, K_j^B$. Choose orthonormal bases $\{|\alpha_i^k\rangle\}_k$ and $\{|\beta_j^\ell\rangle\}_\ell$ for K_i^A and K_j^B respectively. Then

$$|\psi\rangle = \bigoplus_{i,j} \left(\sum_{k,\ell} |\psi_{ij}^{kl}\rangle \otimes \lambda_{ij}^{k\ell} \, |\alpha_i^k, \beta_j^\ell\rangle \right) \in \bigoplus_{i,j} \mathcal{H}_i^A \otimes \mathcal{H}_j^B \otimes K_i^A \otimes K_j^B,$$

where $\sum_{i,j} \sum_{k,\ell} |\lambda_{ij}^{k\ell}|^2 = 1$ and every $|\psi_{ij}^{k\ell}\rangle$ is a vector state in $\mathcal{H}_i^A \otimes \mathcal{H}_j^B$. Moreover, π_A and π_B decompose as

$$\pi_A(\alpha) = \bigoplus_{i,k} \pi_i^A(\alpha) \otimes |\alpha_i^k\rangle\langle\alpha_i^k| \text{ and } \pi_B(\beta) = \bigoplus_{j,\ell} \pi_j^B(\beta) \otimes |\beta_j^\ell\rangle\langle\beta_j^\ell|,$$

where π_i^A and π_j^B are irreducible representations.

For convenience, let $\Lambda := \{(i,j,k,\ell) : \lambda_{ij}^{k\ell} \neq 0\}$ be the set of indices for which the coefficient $\lambda_{ij}^{k\ell}$ is non-zero. It is clear that Λ is non-empty. Now, for every $(i,j,k,\ell) \in \Lambda$, $S_{ij}^{kl} := (\mathcal{H}_i^A, \mathcal{H}_j^B, \{\pi_i^A(m_a^x)\}, \{\pi_j^B(n_b^y)\}, |\psi_{ij}^{k\ell}\rangle)$ is a submodel of S. Since $\mathcal{C}$ is closed, we see that $S_{ij}^{k\ell} \in \mathcal{C}$. And if $p_{ij}^{k\ell} \in C_q$ is the correlation of $S_{ij}^{k\ell}$, then $\sum_{(i,j,k,\ell)\in\Lambda} |\lambda_{ij}^{k\ell}|^2 p_{ij}^{k\ell} = p$. But since p is an extreme point in C_q and f is the unique abstract state in $\mathcal{S}$ achieving p, we must have $p_{ij}^{k\ell} = p$ and ultimately $f_{S_{ij}^{k\ell}} = f$ for all $(i,j,k,\ell) \in \Lambda$.

In particular, it follows from the above argument that there are models

$$\widetilde{S} = \left(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x : a \in A, x \in X\}, \{\widetilde{N}_b^y : b \in B, y \in Y\}, |\widetilde{\psi}\rangle\right) \in \mathcal{C}$$

for p such that the associated representation $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$ is irreducible. Let's suppose that we have fixed such a model $\widetilde{S}$ (not necessarily arising from S), and continue working with the model S. Since π_i^A and π_j^B are irreducible, if $(i,j,k,\ell) \in \Lambda$ then $(\pi_i^A \otimes \pi_j^B, \mathcal{H}_i^A \otimes \mathcal{H}_j^B, |\psi_{ij}^{k\ell}\rangle)$ is a GNS representation of f. Hence by Lemma 3.1.21, part (2), for any i,j the vector states $|\psi_{ij}^{k\ell}\rangle, (i,j,k,\ell) \in \Lambda$ differ at most by a complex phase. By absorbing this phase into the coefficients $\lambda_{ij}^{k\ell}$, we can rewrite

$$|\psi\rangle = \bigoplus_{ij} |\psi_{ij}\rangle \otimes \lambda_{ij} |\kappa_{ij}\rangle,$$

where $|\psi_{ij}\rangle \in \mathcal{H}_i^A \otimes \mathcal{H}_j^B$ and $|\kappa_{ij}\rangle \in K_i^A \otimes K_j^B$ are vector states, and $\sum_{i,j} |\lambda_{ij}|^2 = 1$.

Since $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$ is irreducible, $(\widetilde{\pi}_A \otimes \widetilde{\pi}_B, \widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B, |\widetilde{\psi}\rangle)$ is a GNS representation of f. Similarly, $(\pi_i^A \otimes \pi_j^B, \mathcal{H}_i^A \otimes \mathcal{H}_j^B, |\psi_{ij}\rangle)$ is a GNS representation of f for $(i,j) \in \Lambda' := \{(i,j) : \lambda_{ij} \neq 0\}$. Hence the representations $\pi_i^A \otimes \pi_j^B, (i,j) \in \Lambda'$ are all unitarily equivalent to $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$. By Lemma 3.1.21, part (3), if $i \in \Lambda_A := \{i : \lambda_{ij} \neq 0 \text{ for some } j\}$, then π_i^A is unitarily equivalent to $\widetilde{\pi}_A$ via some unitary $U_i^A : \mathcal{H}_i^A \to \widetilde{\mathcal{H}}_A$. Similarly if $j \in \Lambda_B := \{j : \lambda_{ij} \neq 0 \text{ for some } i\}$, then π_j^B is unitarily equivalent to $\widetilde{\pi}_B$ via some unitary $U_j^B : \mathcal{H}_j^B \to \widetilde{\mathcal{H}}_B$. If $(i,j) \in \Lambda'$, then $(\widetilde{\pi}_A \otimes \widetilde{\pi}_B, \widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B, U_i^A \otimes U_j^B |\psi_{ij}\rangle)$ is a GNS representation of f, so $U_i^A \otimes U_j^B |\psi_{ij}\rangle$ and $|\widetilde{\psi}\rangle$ differ by a complex phase. By absorbing this phase into λ_{ij}, we can assume that $U_i^A \otimes U_j^B |\psi_{ij}\rangle = |\widetilde{\psi}\rangle$ for all $(i,j) \in \Lambda'$.

For every $i \in \Lambda_A$, we can define an isometry $I_i^A : \mathcal{H}_i^A \otimes K_i^A \to \widetilde{\mathcal{H}}_A \otimes K_i^A$ via $I_i^A := U_i^A \otimes \mathbb{1}_{K_i^A}$. For every $i \notin \Lambda_A$, let $I_i^A : \mathcal{H}_i^A \otimes K_i^A \to \widetilde{\mathcal{H}}_A \otimes (\mathcal{H}_i^A \otimes K_i^A)$ be the isometry

$|v\rangle \mapsto |w\rangle \otimes |v\rangle$, where $|w\rangle \in \widetilde{\mathcal{H}}_A$ is some arbitrarily chosen vector state. Define isometries I_j^B analogously. Let

$$\mathcal{H}_A^{aux} := \left(\bigoplus_{i\in\Lambda_A} K_i^A\right) \oplus \left(\bigoplus_{i\notin\Lambda_A} (\mathcal{H}_i^A \otimes K_i^A)\right) \text{ and } \mathcal{H}_B^{aux} := \left(\bigoplus_{j\in\Lambda_B} K_j^B\right) \oplus \left(\bigoplus_{j\notin\Lambda_B} (\mathcal{H}_j^B \otimes K_j^B)\right),$$

and define $|aux\rangle := \bigoplus_{(i,j)\in\Lambda'} \lambda_{ij} |\kappa_{ij}\rangle \in \mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}$. Finally, letting $I_A := \bigoplus_i I_i^A$ and $I_B := \bigoplus_j I_j^B$, we see that

$$(I_A \otimes I_B)\pi_A(\alpha) \otimes \pi_B(\beta) |\psi\rangle = \left(\widetilde{\pi}_A(\alpha) \otimes \widetilde{\pi}_B(\beta) |\widetilde{\psi}\rangle\right) \otimes |aux\rangle$$

for all $\alpha \in \mathcal{A}_{POVM}^{X,A}$, $\beta \in \mathcal{A}_{POVM}^{Y,B}$. We conclude that $S \geq \widetilde{S}$, so p is a self-test for $\mathcal{C}$ with ideal model $\widetilde{S}$. □

The point in Theorem 3.1.22 of showing that there is an ideal strategy

$$\widetilde{S} = \left(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\widetilde{\psi}\rangle\right)$$

for which the associated representation $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$ is irreducible is that then $|\widetilde{\psi}\rangle$ is cyclic for $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$, so $\left(\widetilde{\pi}_A \otimes \widetilde{\pi}_B, \widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B, |\widetilde{\psi}\rangle\right)$ is the GNS representation of the unique abstract state $f = f_{\widetilde{S}}$ for p. In particular, the GNS representation of f will be irreducible, which means that f is an extreme point of the set of states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$.

As mentioned in Section 3.1, the assumption that the correlation p is an extreme point in C_q is necessary for Theorem 3.1.22. In the following example, we describe a non-extreme quantum correlation which is an abstract state self-test but not a self-test.

Example 3.1.23. *Let $X = Y = \{0\}$ and $A = B = \{0, 1\}$, and consider the correlations p, p_1, and p_2 defined by*

$$p(0,0|0,0) = p(1,1|0,0) = \frac{1}{2},\ p(0,1|0,0) = p(1,0|0,0) = 0,$$
$$p_1(0,0|0,0) = 1,\ p_1(0,1|0,0) = p_1(1,0|0,0) = p_1(1,1|0,0) = 0, \text{ and}$$
$$p_2(0,0|0,0) = p_2(0,1|0,0) = p_2(1,0|0,0) = 0,\ p_2(1,1|0,0) = 1.$$

With question sets of size 1*, all correlations are classical, so in particular* p*,* p_1*, and* p_2 *belong to* $C_q(X, Y, A, B)$*. Since* $p = \frac{1}{2}p_1 + \frac{1}{2}p_2$*,* p *is not an extreme point in* C_q*.*

Suppose f *is an abstract state on* $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ *achieving* p*. The correlation* p *is synchronous, so as we'll show in Theorem 3.2.6 part (b),* f *is projective. The algebra* $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ *is spanned by* $1 \otimes 1$*,* $m_0^0 \otimes 1$*,* $1 \otimes n_0^0$*, and* $m_0^0 \otimes n_0^0$*, so* f *is determined by its values on these monomials. From the correlation* p*, we see that*

$$f(1 \otimes 1) = 1, \quad f(m_0^0 \otimes 1) = p(0,0|0,0) + p(0,1|0,0) = \frac{1}{2},$$
$$f(1 \otimes n_0^0) = p(0,0|0,0) + p(1,0|0,0) = \frac{1}{2}, \quad f(m_0^0 \otimes n_0^0) = p(0,0|0,0) = \frac{1}{2}.$$

So p *is an abstract state self-test for the set of all states on* $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$*.*

We will now show that p *is not a self-test for the class of quantum models. Consider the following quantum models for* p*:*

$$\widehat{S} = \left(\mathbb{C}^2, \mathbb{C}^2, \{\widehat{M}_0 = \widehat{N}_0 = |0\rangle\langle 0|, \widehat{M}_1 = \widehat{N}_1 = |1\rangle\langle 1|\}, |\widehat{\psi}\rangle = \tfrac{|00\rangle+|11\rangle}{\sqrt{2}}\right), \text{ and}$$
$$S = \left(\mathbb{C}^3, \mathbb{C}^3, \{M_0 = N_0 = |0\rangle\langle 0|, M_1 = N_1 = |1\rangle\langle 1| + |2\rangle\langle 2|\}, |\psi\rangle = \tfrac{|00\rangle}{\sqrt{2}} + \tfrac{|11\rangle+|22\rangle}{2}\right).$$

Now, assume p *is a self-test for quantum models with ideal model*

$$\widetilde{S} = \left(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\widetilde{\psi}\rangle\right).$$

Then $S \succeq \widetilde{S}$ *via some isometries* I_A, I_B *and vector state* $|aux\rangle$*, and* $\widehat{S} \succeq \widetilde{S}$ *via some isometries* $\widehat{I}_A, \widehat{I}_B$ *and vector state* $|\widehat{aux}\rangle$*, so in particular*

$$I_A \otimes I_B\, |\psi\rangle = |\widetilde{\psi}\rangle \otimes |aux\rangle \text{ and } \widehat{I}_A \otimes \widehat{I}_B\, |\widehat{\psi}\rangle = |\widetilde{\psi}\rangle \otimes |\widehat{aux}\rangle\,.$$

The states $|\psi\rangle$ *and* $|\widehat{\psi}\rangle$ *have Schmidt rank* 2 *and* 3 *respectively. Since isometries preserve Schmidt rank, the Schmidt rank of* $|\widetilde{\psi}\rangle$ *must divide both* 3 *and* 2*. Therefore the Schmidt rank of* $|\widetilde{\psi}\rangle$ *is* 1*. It's well-known that* p *cannot be attained with a separable pure state, so* p *is not a self-test for quantum models. Indeed, suppose that*

$$S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\right)$$

is a model for p *with* $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle$*. Then* $p(a,b|0,0) = p_a q_b$*, where* $p_a = \langle\psi_1|M_a^0|\psi_1\rangle$ *and* $q_b = \langle\psi_2|N_a^0|\psi_2\rangle$*. But there are no probability distributions* $\{p_0, p_1\}$ *and* $\{q_0, q_1\}$ *with* $p_0 q_0 = p_1 q_1 = 1/2$ *and* $p_0 q_1 = p_1 q_0 = 0$*.*

3.2 POVM models versus PVM models

3.2.1 The class of all quantum models and projective quantum models

In this subsection, we look closer at the class $\mathcal{C}_{POVM}$ of all quantum models and the class $\mathcal{C}_{PVM}$ of projective quantum models. We start by proving Corollary 3.1.6.

Proof of Corollary 3.1.6. $\mathcal{C}_{POVM}$ and $\mathcal{C}_{PVM}$ are both closed. Recall from Section 3.1 that if f is a state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$, then $f = f_S$ for some $S \in \mathcal{C}_{POVM}$ (resp. $\mathcal{C}_{PVM}$) if and only if f is finite-dimensional (resp. projective and finite-dimensional). If S is a model for p, then the support model of S is a full-rank model for p. Hence every $p \in C_q$ has a full-rank model in $\mathcal{C}_{POVM}$, so part (a) of Corollary 3.1.6 follows immediately from Theorem 3.1.5 applied to $\mathcal{C}_{POVM}$. Part (b) is Theorem 3.1.5 applied to $\mathcal{C}_{PVM}$. □

As mentioned previously, every correlation $p \in C_q$ has a projective quantum model, and hence there is a projective finite-dimensional state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ with correlation p. If p is an abstract state self-test for finite-dimensional states, then the unique finite-dimensional state achieving p must be projective. It follows immediately that if p is an abstract state self-test for all finite-dimensional states, then p is an abstract state self-test for projective finite-dimensional states. This allows us to prove:

Proposition 3.2.1. *If $p \in C_q$ is a self-test for all quantum models, then*

(a) every quantum model for p is centrally supported,

(b) every full-rank model for p is projective,

(c) p has an ideal model which is full-rank and projective, and

(d) p is a self-test for projective quantum models.

Note that Proposition 3.2.1 does not require that p is an extreme point of C_q. The proof uses the following lemma:

Lemma 3.2.2. *If S is a full-rank model and f_S is projective, then S is projective.*

Proof. Let $S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\big)$. Since f_S is projective,

$$\langle\psi| \left(M_a^x - (M_a^x)^2\right) \otimes \mathbb{1} \, |\psi\rangle = f_S\big(m_a^x - (m_a^x)^2\big) = 0$$

for all $x \in X, a \in A$. Since $M_a^x - (M_a^x)^2$ is a positive operator and $|\psi\rangle$ is full-rank, we conclude that $M_a^x - (M_a^x)^2 = 0$ for all $a \in A$, $x \in X$. The same argument shows that N_b^y is a projection for all $b \in B$, $y \in Y$. □

Proof of Proposition 3.2.1. Part (a) follows from Corollary 3.1.17. By Theorem 3.1.20, p is an abstract state self-test for finite-dimensional states, and hence an abstract state self-test for finite-dimensional projective states. In particular, the unique abstract state f for p is projective, so part (b) follows directly from Lemma 3.2.2. Part (a) and Corollary 3.1.17 imply that p has a full-rank ideal model $\widetilde{S}$. Then by part (b), $\widetilde{S}$ is also projective. It follows that p is a self-test for projective quantum models. □

As mentioned in Section 3.1, Baptista, Chen, Kaniewski, Lolck, Mančinska, Gabelgaard Nielsen, and Schmidt [BCK+23] have constructed a correlation which is a self-test for full-rank quantum models, and a self-test for projective quantum models, but does not have a full-rank projective quantum model. By Proposition 3.2.1, this correlation is not a self-test for all quantum models.

When p is an extremal quantum correlation, Lemma 3.2.2 can also be used to prove a stronger version of Proposition 3.2.1, part (c):

Proposition 3.2.3. *Suppose $p \in C_q(X, Y, A, B)$ is an extreme point in C_q and is a self-test for all quantum models. Then p has a full-rank projective ideal model for which the associated representation is irreducible.*

Proof of Proposition 3.2.3. By Corollary 3.1.6, part (a), p is an abstract state self-test for finite-dimensional states. As mentioned above, the unique finite-dimensional state f corresponding to p must be projective. By Theorem 3.1.22, p has an ideal model

$$\widetilde{S} = \big(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\widetilde{\psi}\rangle\big)$$

for which the associated representation $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$ is irreducible, and in particular

$$\Big(\widetilde{\pi}_A \otimes \widetilde{\pi}_B, \widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B, |\widetilde{\psi}\rangle\Big)$$

is a GNS representation of the projective state $f_{\widetilde{S}} = f$. Since f is the pullback of a state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$, any GNS representation of f is a pullback of a representation of $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$, and hence $\widetilde{S}$ is projective.

Let S' be the support model of $\widetilde{S}$. By Lemma 3.2.2, S' is projective, so by Lemma 3.1.11 the support projection Π_A commutes with $\widetilde{M}_a^x$ for all $x \in X$, $a \in A$. Thus $\Pi_A \in \widetilde{\pi}_A(\mathcal{A}_{POVM}^{X,A})'$, and since $\widetilde{\pi}_A$ is irreducible, we must have $\Pi_A = \mathbb{1}_{\widetilde{\mathcal{H}}_A}$ is the identity. Similarly $\Pi_B = \mathbb{1}_{\widetilde{\mathcal{H}}_B}$, and we conclude that $\widetilde{S} = S'$ is full-rank. □

As we can see from the proof, the ideal model is given by the GNS representation of the unique abstract state for p, and this GNS representation exhibits a "bipartite" structure. We conclude that

Corollary 3.2.4. *Let p be an extreme point in C_q. If there is a unique finite-dimensional abstract state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ achieving p, then f has a GNS representation $(\mathcal{H}_A \otimes \mathcal{H}_B, \pi_A \otimes \pi_B, |\psi\rangle)$ where $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is full-rank, and π_A and π_B are irreducible representations of $\mathcal{A}_{POVM}^{X,A}$ and $\mathcal{A}_{POVM}^{Y,B}$ on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Moreover, p is a self-test for all quantum models with an ideal model*

$$S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\big)$$

where $M_a^x := \pi_A(m_a^x)$ and $N_b^y := \pi_B(n_b^y)$ for all $(x, y, a, b) \in X \times Y \times A \times B$. The same conclusion holds if $\mathcal{A}_{POVM}$ and "self-test for all quantum models" are replaced with $\mathcal{A}_{PVM}$ and "self-test for projective quantum models".

Now we are ready to prove Theorem 3.1.7. Note that part (a) is already proved in Proposition 3.2.1. For part (b), as mentioned in Section 3.1, we follow the approach in [BCK+23]. The following lemma is restated from part of Theorem 3.18 in [BCK+23].

Lemma 3.2.5. *Let S be a quantum model, and let S_{Nai} be any Naimark dilation of S. If S_{Nai} is centrally supported, then $S \succeq S_{Nai}$.*

Proof. Suppose $S_{Nai} = \left(\widehat{\mathcal{H}}_A, \widehat{\mathcal{H}}_B, \{P_a^x\}, \{Q_b^y\}, |\widehat{\psi}\rangle\right)$ is a Naimark dilation of a quantum model $S = (\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle)$ such that S_{Nai} is centrally supported. Let Π_A and Π_B be the support projections of S, and let $I_A : \mathcal{H}_A \to \widehat{\mathcal{H}}_A$ and $I_B : \mathcal{H}_B \to \widehat{\mathcal{H}}_B$ be the isometries such that $M_A^x = I_A^* P_a^x I_A$, $N_b^y = I_B^* Q_b^y I_B$, and $|\widehat{\psi}\rangle = I_A \otimes I_B |\psi\rangle$. Then $I_A \Pi_A I_A^*$ and $I_B \Pi_B I_B^*$ are the support projections of S_{Nai}. For every x and a, since $I_A \Pi_A I_A^*$ and P_a^x commute, we obtain

$$[\Pi_A, M_a^x] = \Pi_A I_A^* P_a^x I_A - I_A^* P_a^x I_A \Pi_A = I_A^* \left(I_A \Pi_A I_A^* P_a^x - P_a^x I_A \Pi_A I_A^*\right) I_A = 0.$$

This implies

$$\begin{aligned}
\langle\psi| (M_a^x)^2 \otimes \mathbb{1} |\psi\rangle &= \langle\psi| M_a^x \Pi_A M_a^x \otimes \mathbb{1} |\psi\rangle = \langle\psi| I_A^* P_a^x (I_A \Pi_A I_A^*) P_a^x I_A \otimes \mathbb{1} |\psi\rangle \\
&= \langle\psi| I_A^* P_a^x P_a^x (I_A \Pi_A I_A^*) I_A \otimes \mathbb{1} |\psi\rangle = \langle\psi| I_A^* P_a^x I_A \Pi_A \otimes \mathbb{1} |\psi\rangle \\
&= \langle\psi| M_a^x \otimes \mathbb{1} |\psi\rangle .
\end{aligned}$$

So the positive operator $M_a^x - (M_a^x)^2$ satisfies $\langle\psi| \left(M_a^x - (M_a^x)^2\right) \otimes \mathbb{1} |\psi\rangle = 0$, and hence $\left(M_a^x - (M_a^x)^2\right) \otimes \mathbb{1} |\psi\rangle = 0$ for all x and a. Similarly, we have $\mathbb{1} \otimes \left(N_b^y - (N_b^y)^2\right) |\psi\rangle = 0$ for all y and b. It follows that

$$\begin{aligned}
&\| I_A \otimes I_B \big(M_a^x \otimes N_b^y |\psi\rangle\big) - P_a^x \otimes Q_b^y \big(I_A \otimes I_B |\psi\rangle\big) \|^2 \\
=& \langle\psi| M_a^x \otimes N_b^y |\psi\rangle - \langle\psi| (M_a^x)^2 \otimes (N_b^y)^2 |\psi\rangle = 0.
\end{aligned}$$

We conclude $I_A \otimes I_B \big(M_a^x \otimes N_b^y |\psi\rangle\big) = P_a^x \otimes Q_b^y |\widehat{\psi}\rangle$ for all x, y, a, b, and hence $S \succeq S_{Nai}$. □

Proof of Theorem 3.1.7. Part (a) is just Proposition 3.2.1, part (d). For (b), let $\widetilde{S}$ be an ideal model. For any quantum model S, let S_{Nai} be a Naimark dilation of S. So S_{Nai} is projective and hence $S_{Nai} \succeq \widetilde{S}$. Since p has a full-rank projective model, by Corollary 3.1.17, S_{Nai} is centrally supported. It follows from Lemma 3.2.5 that $S \succeq S_{Nai}$. Hence $S \succeq \widetilde{S}$. We conclude that p is a self-test for all quantum models. □

3.2.2 Self-testing for synchronous correlations and binary correlations

The hypothesis in Theorem 3.1.7, part (b) that p has a full-rank projective quantum model does not hold for all quantum correlations, as shown in [BCK+23]. In this subsection, we show that it does hold for two large classes of quantum correlations, namely synchronous correlations and extremal binary correlations. So Theorem 3.1.7 part (b) applies to these cases. Recall that the set of synchronous quantum correlations $C_q^{syn}(X, A)$ is the convex subset of $C_q(X, X, A, A)$ such that $p(a, b|x, x) = 0$ for all $x \in X$ and $a \neq b \in A$. A correlation is said to be a binary correlation if the measurement scenario has only two outputs, usually taken to be $A = B = \{0, 1\}$.

Theorem 3.2.6. *Suppose $p \in C_q^{syn}(X, A)$, or p is an extreme point in $C_q(X, Y, A, B)$ with $A = B = \{0, 1\}$. Then the following statements hold.*

(a) p has a full-rank projective quantum model.

(b) Every finite-dimensional abstract state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ for p is projective.

(c) p is a self-test for all quantum models if and only if p is a self-test for projective quantum models.

Part (c) of this theorem follows directly from part (a) and Theorem 3.1.7. We prove parts (a) and (b) for synchronous correlations and extremal binary correlations in Proposition 3.2.8 and Proposition 3.2.10 respectively.

Self-testing for synchronous correlations

We first study synchronous correlations. The following result is well-known (see, e.g. [PSS+16, Theorem 5.5] and [CM14, Lemma 3]).

Lemma 3.2.7. *If* $S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\big)$ *is a projective quantum model for a synchronous quantum correlation* $p \in C_q^{syn}(X, A)$*, then*

$$M_a^x \otimes \mathbb{1} |\psi\rangle = \mathbb{1} \otimes N_a^x |\psi\rangle$$

for all $a \in A, x \in X$*.*

The proof in [PSS+16, Theorem 5.5] uses the fact that $\{M_a^x\}_{a\in A}$ and $\{N_b^y\}_{b\in B}$ are PVMs. Indeed, this lemma also holds for non-projective models. The following proposition proves Theorem 3.2.6 for synchronous correlations.

Proposition 3.2.8. *Suppose* $S = (\mathcal{H}_A \otimes \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in A, y \in X\}, |\psi\rangle)$ *is a quantum model for* $p \in C_q^{syn}(X, A)$*. Then*

$$M_a^x \otimes \mathbb{1} |\psi\rangle = \mathbb{1} \otimes N_a^x |\psi\rangle \tag{3.2.1}$$

for all $x \in X$*,* $a \in A$*. Furthermore,* f_S *is a projective finite-dimensional state, and the support model of* S *is projective.*

Proof. By Naimark's dilation theorem there are isometries V_A, V_B and self-adjoint projections P_a^x, Q_b^y, such that $M_a^x = V_A^* P_a^x V_A, Q_b^y = V_B^* N_b^y V_B$. If we define $|\psi'\rangle := V_A \otimes V_B |\psi\rangle$, then

$$S_{Nai} := (V_A \mathcal{H}_A, V_B \mathcal{H}_B, \{P_a^x : a \in A, x \in X\}, \{Q_b^y : b \in A, y \in X\}, |\psi'\rangle)$$

is a projective quantum model for p. By Lemma 3.2.7, it follows that for each $a \in A$ and $x \in X$ we have $P_a^x \otimes \mathbb{1} |\psi'\rangle = \mathbb{1} \otimes Q_a^x |\psi'\rangle$, and therefore $P_a^x V_A \otimes V_B |\psi\rangle = V_A \otimes Q_a^x V_B |\psi\rangle$. Applying the adjoint $V_A^* \otimes V_B^*$ to both sides, we obtain $M_a^x \otimes \mathbb{1} |\psi\rangle = \mathbb{1} \otimes N_a^x |\psi\rangle$ for all $a \in A$, $x \in X$. From this observation we deduce that

$$\langle\psi| (M_a^x)^2 \otimes \mathbb{1} |\psi\rangle = \langle\psi| M_a^x \otimes N_a^x |\psi\rangle = \sum_{b\in A} \langle\psi| M_a^x \otimes N_b^x |\psi\rangle = \langle\psi| M_a^x \otimes \mathbb{1} |\psi\rangle,$$

and therefore $f_S\big((m_a^x - (m_a^x)^2) \otimes \mathbb{1}\big) = \langle\psi| \big(M_a^x - (M_a^x)^2\big) \otimes \mathbb{1} |\psi\rangle = 0$ for all $a \in A$, $x \in X$. Similarly, $f_S\big(\mathbb{1} \otimes (n_b^y - (n_b^y)^2)\big) = 0$ for all $b \in B, y \in Y$. It follows that f_S is projective. By Proposition 3.1.15, Equation (3.2.1) also implies that S is centrally supported . Let S' be the support model of S. Then $f_{S'} = f_S$ by Corollary 3.1.19 and S' is projective by Lemma 3.2.2. □

Self-testing for binary correlations

We now study binary correlations. We adapt a proof technique from [CHTW10, Proposition 2]:

Lemma 3.2.9. *Suppose $p \in C_q(X, Y, \{0,1\}, \{0,1\})$ is an extreme point in C_q. Let*

$$S = (\mathcal{H}_A, \mathcal{H}_B, \{M_0^x, M_1^x : x \in X\}, \{N_0^y, N_1^y : y \in Y\}, |\psi\rangle)$$

be a quantum model of p. For each $x \in X$, let $\sum_{i=1}^{d} \lambda_i^x |\phi_i^x\rangle\langle\phi_i^x|$ be the spectral decomposition of M_0^x, where $d = dim(\mathcal{H}_A)$. Then one of the following conditions must hold for each $1 \leqslant i \leqslant d$ and $x \in X$:

(a) $\lambda_i^x = 0$,

(b) $\lambda_i^x = 1$, *or*

(c) $|\phi_i^x\rangle\langle\phi_i^x| \otimes \mathbb{1} |\psi\rangle = 0$.

Proof. Suppose $x_0 \in X$ and $i_0 \in \{1, \ldots, d\}$. Define new binary outcome measurements $\{E_0^{x_0}, E_1^{x_0}\}$ and $\{F_0^{x_0}, F_1^{x_0}\}$ by $E_0^{x_0} := \sum_{j \neq i_0} \lambda_j^{x_0} |\phi_j^{x_0}\rangle\langle\phi_j^{x_0}|$, $E_1^{x_0} := \mathbb{1} - E_0^{x_0}$, $F_0^{x_0} := E_0^{x_0} + |\phi_{i_0}^{x_0}\rangle\langle\phi_{i_0}^{x_0}|$, and $F_1^{x_0} := \mathbb{1} - F_0^{x_0}$. For the remaining $x \neq x_0 \in X$, set $E_a^x = F_a^x := M_a^x$, so that

$$M_a^x = \lambda_{i_0}^{x_0} F_a^x + (1 - \lambda_{i_0}^{x_0}) E_a^x \tag{3.2.2}$$

for all $x \in X$, $a \in \{0,1\}$. Let p_1 and p_2 be the correlations with quantum models $S_1 := (\mathcal{H}_A, \mathcal{H}_B, \{F_a^x : a \in \{0,1\}, x \in X\}, \{N_b^y : b \in \{0,1\}, y \in Y\}, |\psi\rangle)$ and $S_2 := (\mathcal{H}_A, \mathcal{H}_B, \{E_a^x : a \in \{0,1\}, x \in X\}, \{N_b^y : b \in \{0,1\}, y \in Y\}, |\psi\rangle)$ respectively. By Equation (3.2.2) we see that $p = \lambda_{i_0}^{x_0} p_1 + (1 - \lambda_{i_0}^{x_0}) p_2$. Since p is an extreme point in C_q, either $\lambda_{i_0}^{x_0} = 0$, $\lambda_{i_0}^{x_0} = 1$, or $p_1 = p_2 = p$. In the last case, we have that $0 = \langle\psi| (F_0^{x_0} - E_0^{x_0}) \otimes \mathbb{1} |\psi\rangle = \langle\psi| (|\phi_{i_0}^{x_0}\rangle\langle\phi_{i_0}^{x_0}|) \otimes \mathbb{1} |\psi\rangle$, and since $|\phi_{i_0}^{x_0}\rangle\langle\phi_{i_0}^{x_0}| \otimes \mathbb{1}$ is a positive operator, $(|\phi_{i_0}^{x_0}\rangle\langle\phi_{i_0}^{x_0}| \otimes \mathbb{1}) |\psi\rangle = 0$. □

The following proposition proves Theorem 3.2.6 for extremal binary quantum correlation.

Proposition 3.2.10. *Suppose $p \in C_q(X, Y, \{0,1\}, \{0,1\})$ is an extreme point in C_q. For any quantum model $S = (\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle)$ for p, there is a projective model $S' = (\mathcal{H}_A, \mathcal{H}_B, \{P_a^x\}, \{Q_b^y\}, |\psi\rangle)$ for p employing the same vector state $|\psi\rangle$ such that*

$$M_a^x \otimes \mathbb{1} |\psi\rangle = P_a^x \otimes \mathbb{1} |\psi\rangle \text{ and } \mathbb{1} \otimes N_b^y |\psi\rangle = \mathbb{1} \otimes Q_b^y |\psi\rangle$$

for all $x \in X, y \in Y$, and $a, b \in \{0,1\}$, and $f_S = f_{S'}$ is projective.

Proof. Let $\sum_i \lambda_i^x |\phi_i^x\rangle\langle\phi_i^x|$ be the spectral decomposition of M_0^x for each $x \in X$. For all x and i, let

$$\widetilde{\lambda}_i^x := \begin{cases} 1 & \lambda_i^x = 1, \\ 0 & \text{otherwise,} \end{cases}$$

and define $P_0^x := \sum_i \widetilde{\lambda}_i^x |\phi_i^x\rangle\langle\phi_i^x|$ and $P_1^x = \mathbb{1} - P_0^x$. By Lemma 3.2.9, $\{P_0^x, P_1^x\}$ is a binary outcome PVM such that

$$M_a^x \otimes \mathbb{1} |\psi\rangle = P_a^x \otimes \mathbb{1} |\psi\rangle$$

for $a \in \{0,1\}$. Similarly, there are binary outcome PVMs $\{Q_0^y, Q_1^y\}$ on $\mathcal{H}_B$ such that

$$\mathbb{1} \otimes N_b^y |\psi\rangle = \mathbb{1} \otimes Q_b^y |\psi\rangle$$

for all $y \in Y$, $b \in \{0,1\}$. Taking $S' = (\mathcal{H}_A, \mathcal{H}_B, \{P_a^x\}, \{Q_b^y\}, |\psi\rangle)$ completes the proof. □

3.3 Self-testing in other frameworks

3.3.1 Self-testing for infinite-dimensional tensor product models

Recall that a *tensor product (POVM) model* for a correlation p is a tuple

$$S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\big),$$

where the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are not restricted to be finite-dimensional. The set of correlations p with a tensor product model is denoted by $C_{qs} = C_{qs}(X, Y, A, B)$. Like

C_q, the set C_{qs} is convex but not closed [Slo19]; however, its closure is also the set C_{qa}. Like C_q, correlations $p \in C_{qs}$ can be expressed by abstract states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. We say a state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ is a *tensor product state* if there exists a tensor product model S such that $f = f_S$. Because of the tensor product structure, the standard definition of self-testing using local dilations in Definition 3.1.1 and Definition 3.1.2 extends straightforwardly to tensor product models and correlations in C_{qs}. Coladangelo and Stark have constructed examples of correlations which are in C_{qs} but not in C_q [CS18]. We do not know of any examples of self-tests in $C_{qs} \backslash C_q$. Since the double-commutant theorem does not hold for infinite-dimensional Hilbert spaces, we also do not know whether abstract state self-tests are self-tests when p is an extreme point. However, we can prove that self-tests for correlations in C_{qs} are abstract state self-tests:

Proposition 3.3.1. *If $p \in C_{qs}$ is a self-test for the class of tensor product models then p is an abstract state self-test for the subset of tensor product states.*

The proof of Proposition 3.3.1 is similar to the proof of Theorem 3.1.20. First, note that the definition of support projections, support models, and centrally supported models generalize straightforwardly to tensor product models. A tensor product model S is said to be full-rank if the support projections of the vector state in S are the identity operators, so in particular a full-rank tensor product model is centrally supported. Although Lemma 3.1.13 and Lemma 3.1.14 no longer hold for tensor product models, they can be replaced by "approximate" versions. To state these lemmas, we use the following notation: if $|v_1\rangle$ and $|v_2\rangle$ are vectors in a Hilbert space $\mathcal{H}$, we write $|v_1\rangle \approx_\epsilon |v_2\rangle$ if $\||v_1\rangle - |v_2\rangle\| \leqslant \epsilon$. By the triangle inequality, we see that $|v_1\rangle \approx_{\epsilon_1} |v_2\rangle \approx_{\epsilon_2} |v_3\rangle$ implies $|v_1\rangle \approx_{\epsilon_1+\epsilon_2} |v_3\rangle$. Also, if $|v_1\rangle \approx_\epsilon |v_2\rangle$ and $T \in \mathcal{B}(\mathcal{H})$, then $T|v_1\rangle \approx_{\|T\|\epsilon} T|v_2\rangle$.

Lemma 3.3.2. *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite vector state, let Π_A and Π_B be the support projections of $|\psi\rangle$, and let E be a self-adjoint operator in $\mathcal{B}(\mathcal{H}_A)$. If, for any $\epsilon > 0$, there exists an operator $\widehat{E} \in \mathcal{B}(\mathcal{H}_B)$ such that $E \otimes \mathbb{1} |\psi\rangle \approx_\epsilon \mathbb{1} \otimes \widehat{E} |\psi\rangle$, then the support projection Π_A commutes with E.*

Proof. Let $|\psi\rangle = \sum_{i \in \Lambda} \lambda_i |\alpha_i\rangle \otimes |\beta_i\rangle$ be a Schmidt decomposition of $|\psi\rangle$ where $\Lambda \subset \mathbb{N}$, so the support projection of $|\psi\rangle$ on $\mathcal{H}_A$ is $\Pi_A = \sum_{i \in \Lambda} |\alpha_i\rangle\langle\alpha_i|$. Now, fix an $\epsilon > 0$ and let $\widehat{E}$

be an operator in $\mathcal{B}(\mathcal{H}_B)$ such that $E \otimes \mathbb{1} |\psi\rangle \approx_{\epsilon/2} \mathbb{1} \otimes \widehat{E} |\psi\rangle$. Since $\Pi_A \leqslant \mathbb{1}$, we see that

$$\Pi_A E \otimes \mathbb{1} |\psi\rangle \approx_{\epsilon/2} \Pi_A \otimes \widehat{E} |\psi\rangle = \mathbb{1} \otimes \widehat{E} |\psi\rangle \approx_{\epsilon/2} E \otimes \mathbb{1} |\psi\rangle .$$

Hence $(\mathbb{1} - \Pi_A)E \otimes \mathbb{1} |\psi\rangle \approx_\epsilon 0$ for all $\epsilon > 0$, and we must have $(\mathbb{1} - \Pi_A)E \otimes \mathbb{1} |\psi\rangle = 0$. This implies

$$\sum_{i \in \Lambda} \lambda_i \big((\mathbb{1} - \Pi_A) E |\alpha_i\rangle \big) \otimes |\beta_i\rangle = 0.$$

Since $\lambda_i > 0$ for all $i \in \Lambda$ and $\{|\beta_i\rangle : i \in \Lambda\}$ is an orthonormal subset, it follows that $(\mathbb{1} - \Pi_A)E |\alpha_i\rangle = 0$ for all $i \in \Lambda$. Then

$$(\mathbb{1} - \Pi_A)E\Pi_A = \sum_{i \in \Lambda} (\mathbb{1} - \Pi_A) E |\alpha_i\rangle\langle\alpha_i| = 0,$$

and $E\Pi_A = \Pi_A E \Pi_A$. Since E is self-adjoint, $\Pi_A E = (E\Pi_A)^* = \Pi_A E \Pi_A = E\Pi_A$. □

Lemma 3.3.3. *If $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a full-rank vector state, then for any $\epsilon > 0$ and $E \in \mathcal{B}(\mathcal{H}_A)$ (resp. $F \in \mathcal{B}(\mathcal{H}_B)$), there is an operator $\widehat{E} \in \mathcal{B}(\mathcal{H}_B)$ (resp. $\widehat{F} \in \mathcal{B}(\mathcal{H}_A)$) such that $E \otimes \mathbb{1} |\psi\rangle \approx_\epsilon \mathbb{1} \otimes \widehat{E} |\psi\rangle$ (resp. $\mathbb{1} \otimes F |\psi\rangle \approx_\epsilon \widehat{F} \otimes \mathbb{1} |\psi\rangle$).*

Proof. If $\mathcal{H}_A$ or $\mathcal{H}_B$ is finite-dimensional, then both are finite-dimensional, and the lemma follows from Lemma 3.1.14. Suppose that $\mathcal{H}_A$ and $\mathcal{H}_B$ are infinite-dimensional Hilbert spaces. Since the vector state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is full rank, it has Schmidt decomposition

$$|\psi\rangle = \sum_{i=1}^{\infty} \lambda_i |\alpha_i\rangle \otimes |\beta_i\rangle ,$$

where $(\lambda_i)_{i=1}^\infty$ is a positive sequence in $\ell^2(\mathbb{N})$ such that $\sum_{i=1}^\infty |\lambda_i|^2 = 1$, and $\{|\alpha_i\rangle : i \in \mathbb{N}\}$ and $\{|\beta_i\rangle : i \in \mathbb{N}\}$ are orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. In particular, $\mathcal{H}_A$ and $\mathcal{H}_B$ are separable. Suppose $\epsilon > 0$ and E is an operator in $\mathcal{B}(\mathcal{H}_A)$. Let $E_{ij} := \langle\alpha_i| E |\alpha_j\rangle$ for every $i, j \in \mathbb{N}$. Since $E \otimes \mathbb{1} |\psi\rangle = \sum_{i,j=1}^\infty \lambda_j E_{ij} |\alpha_i\rangle \otimes |\beta_j\rangle$ and $\sum_{i,j=1}^\infty |\lambda_j E_{ij}|^2 = \| E \otimes \mathbb{1} |\psi\rangle \|^2 < \infty$, there exists an $N \in \mathbb{N}$ such that

$$\sum_{i,j=1}^{N} |\lambda_j E_{ij}|^2 \geqslant \| E \otimes \mathbb{1} |\psi\rangle \|^2 - \epsilon^2.$$

Let $\widetilde{\mathcal{H}}_A := \mathrm{span}\{|\alpha_i\rangle : 1 \leqslant i \leqslant N\}$, $\widetilde{\mathcal{H}}_B := \mathrm{span}\{|\beta_i\rangle : 1 \leqslant i \leqslant N\}$, and let $\widetilde{\Pi}_A := \sum_{i=1}^N |\alpha_i\rangle\langle\alpha_i| \in \mathcal{B}(\mathcal{H}_A)$ and $\widetilde{\Pi}_B := \sum_{i=1}^N |\beta_i\rangle\langle\beta_i| \in \mathcal{B}(\mathcal{H}_B)$ be the projections onto $\widetilde{\mathcal{H}}_A$ and $\widetilde{\mathcal{H}}_B$ respectively. Then $|\widetilde{\psi}\rangle := \widetilde{\Pi}_A \otimes \widetilde{\Pi}_B |\psi\rangle = \sum_{i=1}^N \lambda_i |\alpha_i\rangle \otimes |\beta_i\rangle$ is a full-rank vector in the finite-dimensional space $\widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B$, and

$$E \otimes \mathbb{1}_{\mathcal{H}_B} |\psi\rangle \approx_\epsilon \widetilde{\Pi}_A E \widetilde{\Pi}_A \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle .$$

By Lemma 3.1.14, there exists an operator $\widehat{E} \in \mathcal{B}(\widetilde{\mathcal{H}}_B)$ such that

$$\widetilde{\Pi}_A E \widetilde{\Pi}_A \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle = \mathbb{1}_{\widetilde{\mathcal{H}}_A} \otimes \widehat{E} |\widetilde{\psi}\rangle .$$

Extending $\widehat{E}$ to $\mathcal{H}_B$ by having it act trivially on $\{|\beta_i\rangle : i \geqslant N+1\}$, we see that $E \otimes \mathbb{1} |\psi\rangle \approx_\epsilon \mathbb{1} \otimes \widehat{E} |\psi\rangle$. The existence of $\widehat{F}$ for F and ϵ follows similarly. □

Lemma 3.3.2 and Lemma 3.3.3 allow us to establish the following characterization of centrally supported tensor product models.

Proposition 3.3.4. *A tensor product model*

$$S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\big)$$

is centrally supported if and only if for any $\epsilon > 0$ and every $a \in A$, $x \in X$ (resp. $b \in B$, $y \in Y$) there exists an operator $\widehat{M}_a^x \in \mathcal{B}(\mathcal{H}_B)$ (resp. $\widehat{N}_b^y \in \mathcal{B}(\mathcal{H}_A)$) such that $M_a^x \otimes \mathbb{1} |\psi\rangle \approx_\epsilon \mathbb{1} \otimes \widehat{M}_a^x |\psi\rangle$ (resp. $\mathbb{1} \otimes N_b^y |\psi\rangle \approx_\epsilon \widehat{N}_b^y \otimes \mathbb{1} |\psi\rangle$) .

Proof. The "if" part follows directly from Lemma 3.3.2. For the "only if" part, let Π_A and Π_B be the support projections of $|\psi\rangle$, and suppose $[\Pi_A, M_a^x] = [\Pi_B, N_b^y] = 0$ for all $(a, b, x, y) \in A \times B \times X \times Y$. Since $\Pi_A \otimes \Pi_B |\psi\rangle$ is full-rank in $\Pi_A \mathcal{H}_A \otimes \Pi_B \mathcal{H}_B$, by Lemma 3.3.3, for any $\epsilon > 0$ there is an operator $\widehat{M}_a^x$ in $\mathcal{B}(\Pi_B \mathcal{H}_B)$ (which can be regarded as an operator in $\mathcal{B}(\mathcal{H}_B)$ acting trivially on $(\mathbb{1} - \Pi_B)\mathcal{H}_B$) such that $\Pi_A M_a^x \Pi_A \otimes \Pi_B |\psi\rangle \approx_\epsilon \Pi_A \otimes \widehat{M}_a^x \Pi_B |\psi\rangle$ for any $a \in A, x \in X$. Therefore

$$M_a^x \otimes \mathbb{1} |\psi\rangle = \Pi_A M_a^x \Pi_A \otimes \Pi_B |\psi\rangle \approx_\epsilon \Pi_A \otimes \widehat{M}_a^x \Pi_B |\psi\rangle = \mathbb{1} \otimes \widehat{M}_a^x |\psi\rangle .$$

Similarly, for any $\epsilon > 0$ and every $b \in B, y \in Y$ there exists $\widehat{N}_b^y \in \mathcal{B}(\mathcal{H}_A)$ such that $\mathbb{1} \otimes N_b^y |\psi\rangle \approx_\epsilon \widehat{N}_b^y \otimes \mathbb{1} |\psi\rangle$. □

Proposition 3.3.5. *Let*

$$S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\right) \text{ and}$$
$$\widetilde{S} = \left(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x : a \in A, x \in X\}, \{\widetilde{N}_b^y : b \in B, y \in Y\}, |\widetilde{\psi}\rangle\right)$$

be two tensor product models for a correlation $p \in C_{qs}(X, Y, A, B)$, with associated representations $\pi_A \otimes \pi_B$ and $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$ respectively. Suppose $S \succeq \widetilde{S}$ via local isometries I_A, I_B and vector state $|aux\rangle \in \mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}$. If $\widetilde{S}$ is centrally supported, then

$$(\widetilde{\pi}_A(\alpha) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle) \otimes |aux\rangle = I_A \pi(\alpha) I_A^* \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \text{ for all } \alpha \in \mathcal{A}_{POVM}^{X,A}, \quad (3.3.1)$$
$$(\mathbb{1}_{\widetilde{\mathcal{H}}_A} \otimes \widetilde{\pi}_B(\beta) |\widetilde{\psi}\rangle) \otimes |aux\rangle = \mathbb{1}_{\widetilde{\mathcal{H}}_A \otimes \mathcal{H}_A^{aux}} \otimes I_B \pi(\beta) I_B^* |\widetilde{\psi}, aux\rangle \text{ for all } \beta \in \mathcal{A}_{POVM}^{Y,B}, \quad (3.3.2)$$

and $f_S = f_{\widetilde{S}}$.

Proof. As in the proof of Proposition 3.1.18, we can show that Equation (3.3.1) holds for all monomials $\alpha = \alpha_1 \cdots \alpha_k \in \mathcal{A}_{POVM}^{X,A}$, $\alpha_i \in \{e_a^x : x \in X, a \in A\}$ using induction on the monomial degree $k \in \mathbb{N}$. Indeed, the cases $k = 0, 1$ follow straight from the definition of local dilation of tensor product models. Suppose that Equation (3.1.2) holds for all monomials in $\mathcal{A}_{POVM}^{X,A}$ of degree k. For any monomial $\alpha = \alpha_1 \cdots \alpha_k \alpha_{k+1}$ in $\mathcal{A}_{POVM}^{X,A}$ of degree $k+1$, let $\alpha' := \alpha_1 \cdots \alpha_k$. Since $\widetilde{S}$ is centrally supported, Proposition 3.3.4 implies that for any $\epsilon > 0$, there is an $\widetilde{F} \in \mathcal{B}(\widetilde{\mathcal{H}}_B)$ such that $\widetilde{\pi}_A(\alpha_{k+1}) \otimes \mathbb{1} |\widetilde{\psi}\rangle \approx_{\epsilon/2} \mathbb{1} \otimes \widetilde{F} |\widetilde{\psi}\rangle$. Note that $\|\widetilde{\pi}_A(\alpha')\| \leqslant 1$ and $\|I_A \pi_A(\alpha') I_A^*\| \leqslant 1$. Thus by the inductive hypothesis,

$$\begin{aligned}
\left(\widetilde{\pi}_A(\alpha) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle\right) \otimes |aux\rangle &= \left(\widetilde{\pi}_A(\alpha')\widetilde{\pi}_A(\alpha_{k+1}) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \\
&\approx_{\epsilon/2} \left(\widetilde{\pi}_A(\alpha') \otimes \widetilde{F} |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \\
&= I_A \pi_A(\alpha') I_A^* \otimes \widetilde{F} \otimes \mathbb{1}_{\mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \\
&\approx_{\epsilon/2} \left(I_A \pi_A(\alpha') I_A^* (\widetilde{\pi}(\alpha_{k+1}) \otimes \mathbb{1}_{\mathcal{H}_A^{aux}})\right) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \\
&= \left(I_A \pi_A(\alpha') I_A^* I_A \pi_A(\alpha_{k+1}) I_A^*\right) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \\
&= I_A \pi_A(\alpha) I_A^* \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle .
\end{aligned}$$

Therefore $\left(\widetilde{\pi}_A(\alpha) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \approx_\epsilon I_A \pi_A(\alpha) I_A^* \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle$ for all $\epsilon > 0$, and we conclude that Equation (3.3.1) holds for all $\alpha \in \mathcal{A}_{POVM}^{X,A}$. The proof of Equation (3.3.2)

is similar. Hence, for any $\alpha \in \mathcal{A}_{POVM}^{X,A}$ and $\beta \in \mathcal{A}_{POVM}^{Y,B}$,

$$\begin{aligned} f_{\widetilde{S}}(\alpha \otimes \beta) &= \langle \widetilde{\psi} | \, \widetilde{\pi}_A(\alpha) \otimes \widetilde{\pi}_B(\beta) \, | \widetilde{\psi} \rangle \\ &= \langle \widetilde{\psi}, aux | \, \widetilde{\pi}_A(\alpha) \otimes \widetilde{\pi}_B(\beta) \otimes \mathbb{1}_{\mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}} \, | \widetilde{\psi}, aux \rangle \\ &= \langle \widetilde{\psi}, aux | \, I_A \pi_A(\alpha) I_A^* \otimes I_B \pi_B(\beta) I_B^* \, | \widetilde{\psi}, aux \rangle \\ &= \langle \psi | \, \pi_A(\alpha) \otimes \pi_B(\beta) \, | \psi \rangle \\ &= f_S(\alpha \otimes \beta), \end{aligned}$$

which implies $f_S = f_{\widetilde{S}}$. □

Proposition 3.3.6. *Let S and $\widetilde{S}$ be two tensor product models for $p \in C_{qs}$. If S is centrally supported and $S \succeq \widetilde{S}$, then $\widetilde{S}$ is centrally supported.*

Proof. Let

$$\begin{aligned} S &= \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\big) \text{ and} \\ \widetilde{S} &= \big(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x : a \in A, x \in X\}, \{\widetilde{N}_b^y : b \in B, y \in Y\}, |\widetilde{\psi}\rangle\big) \end{aligned}$$

be two tensor product models with support projections Π_A, Π_B and $\widetilde{\Pi}_A, \widetilde{\Pi}_B$ respectively. Suppose S is centrally supported and $S \succeq \widetilde{S}$ with local isometries I_A, I_B and vector state $|aux\rangle \in \mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}$. Then

$$S' := \big(\widetilde{\mathcal{H}}_A \otimes \mathcal{H}_A^{aux}, \widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}, \{\widetilde{M}_a^x \otimes \mathbb{1}_{\mathcal{H}_A^{aux}}\}, \{\widetilde{N}_b^y \otimes \mathbb{1}_{\mathcal{H}_B^{aux}}\}, |\widetilde{\psi}, aux\rangle\big)$$

is a tensor product model for p with support projections $\widetilde{\Pi}_A \otimes \Pi_A^{aux}$ and $\widetilde{\Pi}_B \otimes \Pi_B^{aux}$, where $\Pi_A^{aux} \in \mathcal{B}(\mathcal{H}_A^{aux})$ and $\Pi_B^{aux} \in \mathcal{B}(\mathcal{H}_B^{aux})$ are the support projections of $|aux\rangle$. Since S is centrally supported, by Proposition 3.3.4, for every $x \in X, a \in A$, and $\epsilon > 0$, there is an operator $\widehat{M}_a^x \in \mathcal{B}(\mathcal{H}_B)$ such that $M_a^x \otimes \mathbb{1} \, |\psi\rangle \approx_\epsilon \mathbb{1} \otimes \widehat{M}_a^x \, |\psi\rangle$. Since $I_A I_A^* \otimes I_B I_B^* \, |\widetilde{\psi}, aux\rangle = |\widetilde{\psi}, aux\rangle$ and $\mathbb{1} \otimes \mathbb{1} \geqslant I_A I_A^* \otimes \mathbb{1} \geqslant I_A I_A^* \otimes I_B I_B^*$, we see that $I_A I_A^* \otimes \mathbb{1} \, |\widetilde{\psi}, aux\rangle = |\widetilde{\psi}, aux\rangle$ and $\|I_A \otimes I_B\| \leqslant 1$. Then, $I_B \widehat{M}_a^x I_B^*$ is an operator in $\mathcal{B}(\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux})$ such that

$$\begin{aligned} \mathbb{1} \otimes I_B \widehat{M}_a^x I_B^* \, |\widetilde{\psi}, aux\rangle &= I_A I_A^* \otimes I_B \widehat{M}_a^x I_B^* \, |\widetilde{\psi}, aux\rangle \\ &= (I_A \otimes I_B)(\mathbb{1} \otimes \widehat{M}_a^x \, |\psi\rangle) \end{aligned}$$

$$\begin{aligned}
&\approx_\epsilon (I_A \otimes I_B)(M_a^x \otimes \mathbb{1} \left|\psi\right\rangle) \\
&= (\widetilde{M}_a^x \otimes \mathbb{1}_{\mathcal{H}_A^{aux}}) \otimes \mathbb{1} \left|\widetilde{\psi}, aux\right\rangle.
\end{aligned}$$

By Lemma 3.3.2 we see that $\widetilde{\Pi}_A \otimes \Pi_A^{aux}$ commutes with $\widetilde{M}_a^x \otimes \mathbb{1}_{\mathcal{H}_A^{aux}}$, and hence $[\widetilde{\Pi}_A, \widetilde{M}_a^x] = 0$ for all $x \in X, a \in A$. Similarly, $[\widetilde{\Pi}_B, \widetilde{N}_b^y] = 0$ for all $y \in Y, b \in B$. We conclude that $\widetilde{S}$ is centrally supported. □

Proof of Proposition 3.3.1. Suppose $p \in C_{qs}(X, Y, A, B)$ is a self-test for the class of tensor product models. Let S be a full-rank tensor product model for p with ideal model $\widetilde{S}$, so that $S \succeq \widetilde{S}$. Full-rank models are centrally supported, so Proposition 3.3.6 implies that $\widetilde{S}$ is centrally supported. It follows from Proposition 3.3.5 that $f_{\widetilde{S}}$ is the unique abstract state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ achieving p. □

Proposition 3.3.1 applies to the set of states which have a tensor product model. There are also states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ which do not arise from a tensor product model. Suppose p is a correlation in C_{qs}, and consider the set of states f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ such that $f(m_a^x \otimes n_b^y) = p(a, b|x, y)$ for all $(a, b, x, y) \in A \times B \times X \times Y$. We do not know whether every such state has a tensor product model, or whether being a self-test for tensor-product models implies that there is a unique such state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$.

3.3.2 Self-testing for commuting operator models

Recall that a *commuting operator POVM model* for a correlation p is a tuple

$$(\mathcal{H}, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, \left|\psi\right\rangle),$$

where

(i) $\mathcal{H}$ is a Hilbert space,

(ii) $\{M_a^x : a \in A\}$, $x \in X$ and $\{N_b^y : b \in B\}$, $y \in Y$ are POVMs on $\mathcal{H}$ such that

$$M_a^x N_b^y = N_b^y M_a^x$$

for all $(a, b, x, y) \in A \times B \times X \times Y$, and

(iii) $|\psi\rangle \in \mathcal{H}$ is a vector state

such that

$$p(a, b|x, y) = \langle\psi|M_a^x \cdot N_b^y|\psi\rangle$$

for all $(a, b, x, y) \in A \times B \times X \times Y$. As with tensor product models, a commuting operator model is *projective* if the measurements $\{M_a^x\}$ and $\{N_b^y\}$ are projective, and *finite-dimensional* if $\mathcal{H}$ is finite-dimensional. We let $C_{qc} = C_{qc}(X, Y, A, B)$ be the set of correlations with a commuting operator model. It is well-known that C_{qc} is closed, convex, and contains C_{qa}, that every correlation in C_{qc} has a projective commuting operator model, and that the set of correlations with finite-dimensional commuting operator models is equal to C_q.

Analogously to the finite-dimensional case, if

$$S = (\mathcal{H}, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle)$$

is a commuting operator model for a correlation $p \in C_{qc}$, then there is an *associated representation* ϕ of $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$ with $\phi(m_a^x \otimes n_b^y) = M_a^x \cdot N_b^y$, and the associated abstract state f_S on $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$ defined by $f_S(x) := \langle\psi|\phi(x)|\psi\rangle$ satisfies $p(a, b|x, y) = f_S(m_a^x \otimes n_b^y)$. The tuple $(\phi, \mathcal{H}, |\psi\rangle)$ is a GNS representation of f_S if and only if $|\psi\rangle$ is a cyclic vector for ϕ, in which case we say that S is a *cyclic model*. Conversely, taking the GNS representation of a state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$ gives a commuting operator model S with $f = f_S$. Hence a correlation $p \in \mathbb{R}_{\geqslant 0}^{A \times B \times X \times Y}$ belongs to $C_{qc}(X, Y, A, B)$ if and only if there is a state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$ with $p(a, b|x, y) = f(m_a^x \otimes n_b^y)$ for all $(a, b, x, y) \in A \times B \times X \times Y$ [Fri12, JNP+11].

The definition of an abstract state self-test on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ suggests a notion of self-testing for commuting operator models:

Definition 3.3.7. *Let $\mathcal{S}$ be a subset of states on $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$. A correlation p is an **abstract state self-test for $\mathcal{S}$** if there exists a unique abstract state $f \in \mathcal{S}$ with*

correlation p. We say that p is a ***commuting operator self-test*** *if it is an abstract state self-test for all states on $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$.*

There is a surjective homomorphism $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B} \to \mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$, and this means that states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ can be thought of as a subset of states on $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$. Hence Definition 3.3.7 subsumes Definition 3.1.3. While Definition 3.1.3 is for finite-dimensional states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$, Definition 3.3.7 also gives us a definition of self-testing for non-finite-dimensional states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ (or in other words, for correlations $p \in C_{qa}$ which do not have a finite-dimensional model). This is potentially useful in understanding how self-testing interacts with limiting behaviour of finite-dimensional models. For instance, Mančinska and Schmidt [MS23] give an example of a nonlocal game which is a non-robust self-test by combining a finite-dimensional self-test with a game with a perfect C_{qa} strategy, but no perfect C_q strategy. In our language, this nonlocal game is a an abstract state self-test for finite-dimensional states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$, but not a self-test for all states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. Another example is the open question at the end of Section 3.3.1, which in this language asks whether every self-test for tensor-product models is an abstract state self-test for states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$.

An immediate question about Definition 3.3.7 is whether there is an equivalent description of this type of self-test in terms of models. For this purpose, we make the following definitions.

Definition 3.3.8. *Let*

$$S = (\mathcal{H}, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle) \text{ and}$$
$$\widetilde{S} = \left(\widetilde{\mathcal{H}}, \{\widetilde{M}_a^x : a \in A, x \in X\}, \{\widetilde{N}_b^y : b \in B, y \in Y\}, |\widetilde{\psi}\rangle\right)$$

be two commuting operator models.

1. *We say S and $\widetilde{S}$ are* ***equivalent****, and write $S \cong \widetilde{S}$, if there exists a unitary $U : \mathcal{H} \to \widetilde{\mathcal{H}}$ such that*

(i) $U|\psi\rangle = |\widetilde{\psi}\rangle$, *and*

(ii) $UM_a^x U^* = \widetilde{M}_a^x$ *and* $UN_b^y U^* = \widetilde{N}_b^y$ *for all* $(a,b,x,y) \in A \times B \times X \times Y$.

2. $\widetilde{S}$ *is a* ***submodel*** *of* S *if there is a self-adjoint projection* $\Pi \in \mathcal{B}(\mathcal{H})$ *commuting with* M_a^x *and* N_b^y *for all* $(a,b,x,y) \in A \times B \times X \times Y$, *such that* $\widetilde{\mathcal{H}} = \Pi\mathcal{H}$, $|\widetilde{\psi}\rangle = |\psi\rangle$, *and* $\widetilde{M}_a^x = \Pi M_a^x \Pi$ *and* $\widetilde{N}_b^y = \Pi N_b^y \Pi$ *for all* $(a,b,x,y) \in A \times B \times X \times Y$.

3. S *is said to be* ***degenerate*** *if there exists a non-trivial self-adjoint projection* $\Pi \in \mathcal{B}(\mathcal{H})$ *such that* $\Pi|\psi\rangle = |\psi\rangle$ *and* $[\Pi, M_a^x] = [\Pi, N_b^y] = 0$ *for all* $(a,b,x,y) \in A \times B \times X \times Y$. *A commuting operator model is said to be* ***nondegenerate*** *if it is not degenerate.*

A class of commuting operator models $\mathcal{C}$ *is* ***closed under submodels*** *if*

(i) for any $S \in \mathcal{C}$, *if* $\widetilde{S}$ *is a commuting operator model such that* $\widetilde{S} \cong S$ *then* $\widetilde{S} \in \mathcal{C}$, *and*

(ii) for any $S \in \mathcal{C}$, *if* $\widetilde{S}$ *is a submodel of* S *then* $\widetilde{S} \in \mathcal{C}$.

Note that in the definition of submodel in Definition 3.3.8, the condition $|\widetilde{\psi}\rangle = |\psi\rangle$ is equivalent to the condition that $\Pi|\psi\rangle = |\widetilde{\psi}\rangle$, since both imply that $|\psi\rangle$ is in the support of Π. This makes this notion of submodel a bit different from the definition of submodel in Definition 3.1.4, which only requires $\Pi_A \otimes \Pi_B |\psi\rangle = \lambda|\widetilde{\psi}\rangle$ for some non-zero complex number λ. As a result:

Remark 3.3.9. *Suppose* S *and* $\widetilde{S}$ *are commuting operator models. If* $\widetilde{S}$ *is equivalent to or a submodel of* S, *then* $f_{\widetilde{S}} = f_S$.

The following proposition shows that any commuting operator model S has a nondegenerate submodel $\widetilde{S}$ which is the GNS representation for the abstract state f_S.

Proposition 3.3.10. *A commuting operator model is nondegenerate if and only if it is a cyclic model. Furthermore, every commuting operator model has a nondegenerate submodel.*

Proof. We use $\mathcal{A}$ to denote $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$. Let $p \in C_{qc}(X, Y, A, B)$, and let

$$S = (\mathcal{H}, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle)$$

be a commuting operator model for p with associated representation π.

For the "if" direction, suppose $|\psi\rangle$ is cyclic for π. If Π is a projection in the commutant $\pi(\mathcal{A})'$ such that $\Pi |\psi\rangle = |\psi\rangle$, then $\Pi\pi(\alpha) |\psi\rangle = \pi(\alpha)\Pi |\psi\rangle = \pi(\alpha) |\psi\rangle$, so $\pi(\alpha) |\psi\rangle$ is contained in the image of Π. We conclude that $\Pi = \mathbb{1}$, so S must be non-degenerate.

For the "only if" direction, suppose $|\psi\rangle$ is not cyclic for π. Let $\mathcal{H}_0 := \big(\pi(\mathcal{A}) |\psi\rangle\big)^-$, and let $\Pi \in \mathcal{B}(\mathcal{H})$ be the self-adjoint projection onto $\mathcal{H}_0$. Then $\Pi \in \pi(\mathcal{A})'$ is a non-trivial projection such that $\Pi |\psi\rangle = |\psi\rangle$, and hence S is degenerate. Furthermore, $(\mathcal{H}_0, \{\Pi M_a^x \Pi : a \in A, x \in X\}, \{\Pi N_b^y \Pi : b \in B, y \in Y\}, |\psi\rangle)$ is a non-degenerate submodel of S. □

We can now show that Definition 3.3.7 is equivalent to having a unique nondegenerate commuting-operator model (and this holds for any class of commuting operator models closed under submodels).

Theorem 3.3.11. *Let $\mathcal{C}$ be a class of commuting operator models that is closed under submodels, and let $\mathcal{S} := \{f_S : S \in \mathcal{C}\}$ be the set of states on $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$ induced by $\mathcal{C}$. Then $p \in C_{qc}$ is a self-test for $\mathcal{S}$ if and only if there is a commuting operator model*

$$\widetilde{S} = (\widetilde{\mathcal{H}}, \{\widetilde{M}_a^x : a \in A, x \in X\}, \{\widetilde{N}_b^y : b \in B, y \in Y\}, |\widetilde{\psi}\rangle)$$

for p in $\mathcal{C}$, such that for every other commuting operator model

$$S = (\mathcal{H}, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle),$$

for p in $\mathcal{C}$, there is a submodel of S which is equivalent to $\widetilde{S}$.

Proof. The "if" direction follows directly from Remark 3.3.9. For the "only if" direction, suppose p is an abstract state self-test for $\mathcal{S}$, with unique state $f \in \mathcal{S}$. By definition $f = f_{S'}$ for some $S' \in \mathcal{C}$. By Proposition 3.3.10, S' has a non-degenerate submodel $\widetilde{S}$. Suppose S is any other model in $\mathcal{C}$ for p, and let S'' be a non-degenerate submodel of S. Then S'' and $\widetilde{S}$ are both cyclic models with $f_{S''} = f_S = f_{S'} = f_{\widetilde{S}}$. Since GNS representations are unique up to unitary equivalence, S'' is equivalent to $\widetilde{S}$. □

Note that the above theorem does not require p to be an extreme point in C_{qc}.

The class of finite-dimensional commuting operator models is closed under submodels, and thus Theorem 3.3.11 applies to this class. Every finite-dimensional state (resp. projective finite-dimensional state) on $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$ comes from a finite-dimensional state (resp. projective finite-dimensional state) on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$, and thus p is an abstract state self-test for finite-dimensional states (resp. projective finite-dimensional states) on $\mathcal{A}_{POVM}^{X,A} \otimes_{max} \mathcal{A}_{POVM}^{Y,B}$ if and only if p is an abstract state self-test for finite-dimensional states (resp. projective finite-dimensional states) on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. As a result, if $p \in C_q$ is an extreme point, then p is a self-test for (POVM) quantum models if and only if p has a unique nondegenerate commuting operator model (up to unitary equivalence). If, in addition, there exists a projective full-rank quantum model for p, then p is a self-test for projective quantum models if and only if p has a unique nondegenerate commuting operator model. This gives a new criterion for $p \in C_q$ to be a self-test for (finite-dimensional) quantum models.

It follows that if $p \in C_q$ is a commuting operator self-test, then p is a self-test for (finite-dimensional) quantum models. Tsirelson showed that a wide family of correlations in C_q are in fact commuting operator self-tests [Tsi87]. To state this result, let $Cor(X, Y)$ be the set of matrices $c \in \mathbb{R}^{X \times Y}$ for which there is a Euclidean space V and vectors $\{|u_x\rangle\}_{x \in X}$, $\{|v_y\rangle\}_{y \in Y}$ in V of norm at most 1, such that $c_{x,y} = \langle u_x | v_y \rangle$ for all $x, y \in X \times Y$. If $p \in C_{qc}(X, Y, \mathbb{Z}_2, \mathbb{Z}_2)$ then the matrix c defined by

$$c_{x,y} = \sum_{a,b \in \mathbb{Z}_2} (-1)^{a+b} p(a, b|x, y)$$

is in $Cor(X, Y)$, since if $\big(\mathcal{H}, \{M_a^x : a \in \mathbb{Z}_2, x \in X\}, \{N_b^y : b \in \mathbb{Z}_2, y \in Y\}, |\psi\rangle\big)$ is a commuting operator model for p, then $c_{x,y} = \langle \psi | (M_0^x - M_1^x)(N_0^y - N_1^y) | \psi \rangle$, where $\|M_0^x - M_1^x\| \leqslant 1$ and $\|N_0^y - N_1^y\| \leqslant 1$. We refer to c as the *XOR correlation* associated with p. Tsirelson shows that the linear map

$$C_q(X, Y, \mathbb{Z}_2, \mathbb{Z}_2) \to Cor(X, Y) \ : \ p \mapsto c$$

restricts to an isomorphism $C_q^{unbiased}(X, Y, \mathbb{Z}_2, \mathbb{Z}_2) \to Cor(X, Y)$, where

$$C_q^{unbiased}(X, Y, \mathbb{Z}_2, \mathbb{Z}_2) = \Big\{ p \in C_q(X, Y, \mathbb{Z}_2, \mathbb{Z}_2) : \sum_{b \in \mathbb{Z}_2} p(0, b|x, y) = \sum_{b \in \mathbb{Z}_2} p(1, b|x, y) \text{ and}$$

$$\sum_{a\in\mathbb{Z}_2} p(a,0|x,y) = \sum_{a\in\mathbb{Z}_2} p(a,1|x,y),\ x\in X,\ y\in Y\Big\}.$$

Theorem 3.3.12 ([Tsi87]). *If p is an extreme point of $C_q^{unbiased}$ and the associated XOR correlation c has even rank, then p is a commuting operator self-test.*

Proof. Since the isomorphism $C_q^{unbiased} \to Cor(X,Y)$ is linear, it preserves extreme points. If p is an extreme point of $C_q^{unbiased}$, then the associated XOR correlation c is an extreme point in $Cor(X,Y)$. By [Tsi87, Theorem 3.2], if c has even rank then all nondegenerate commuting operator models for p are unitarily equivalent. Hence, there is a unique state on $\mathcal{A}_{POVM}^{X,\mathbb{Z}_2} \otimes_{max} \mathcal{A}_{POVM}^{Y,\mathbb{Z}_2}$ achieving p. □

Example 3.3.13. *It is well known that the unique optimal correlation for the CHSH game is an extreme point of $C_q^{unbiased}$ with associated XOR correlation matrix*

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}.$$

Since the associated XOR correlation has rank 2, the optimal CHSH correlation is a commuting operator self-test.

A modern proof that the CHSH correlation is a commuting operator self-test can be found in [Fre22], where it is also shown that the Mermin-Peres magic square and magic pentagram games are commuting operator self-tests.

For more examples of commuting operator self-tests, let CHSH_α, $\alpha \in [0,2)$ be the family of *tilted* CHSH games introduced in [AMP12]. It is well-known that there is a unique correlation $p_\alpha \in C_q(\mathbb{Z}_2,\mathbb{Z}_2,\mathbb{Z}_2,\mathbb{Z}_2)$ achieving the optimal winning probability of CHSH_α, and that p_α is a self-test for projective quantum models [BP15, CGS17]. This self-testing result is instrumental in the separations of the correlation sets $C_q \subsetneq C_{qs} \subsetneq C_{qa}$ in [CS18, Col20, Bei21]. Theorem 3.2.6 shows that p_α is a self-test for POVM quantum models as well.

Proposition 3.3.14. *If $p_\alpha \in C_q(\mathbb{Z}_2,\mathbb{Z}_2,\mathbb{Z}_2,\mathbb{Z}_2)$ is the unique optimal correlation for $CHSH_\alpha$, $\alpha \in [0,2)$, then p_α is a commuting operator self-test.*

Proof. Fix $\alpha \in [0,2)$. Let $a_0 := m_0^0 - m_1^0, a_1 := m_0^1 - m_1^1, b_0 := n_0^0 - n_1^0$, and $b_1 := n_0^1 - n_1^1$ in $\mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes_{max} \mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$, and let $\eta := \alpha a_0 + a_0 b_0 + a_0 b_1 + a_1 b_0 - a_1 b_1$. A state f on $\mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes_{max} \mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$ achieves p_α if and only if $f(\eta) = \sqrt{8+2\alpha^2} =: \lambda$. Bamps and Pironio [BP15] show that

$$2\lambda(\lambda - \eta) = r_1^2 + r_2^2 = r_3^2 + r_4^2$$

in $\mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes_{max} \mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$, where

$$\begin{aligned}
r_1 &:= \lambda - \eta, \\
r_2 &:= \alpha a_1 - a_0 b_0 + a_0 b_1 - a_1 b_0 - a_1 b_1, \\
r_3 &:= \big(2a_0 - \frac{\lambda}{2}(b_0 + b_1) + \frac{\alpha}{2}(a_0 b_0 + a_0 b_1 - a_1 b_0 + a_1 b_1)\big), \text{ and} \\
r_4 &:= \big(2a_1 - \frac{\lambda}{2}(b_0 - b_1) + \frac{\alpha}{2}(a_0 b_0 - a_0 b_1 - a_1 b_0 - a_1 b_1)\big).
\end{aligned}$$

Moving to $\mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes_{max} \mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$, we see that

$$\begin{aligned}
2\lambda(\lambda - \eta) &= r_1^2 + r_2^2 + \frac{1}{2}(s_1 + s_2 + s_3 + s_4) + 2(s_5 + s_6) \\
&= r_3^2 + r_4^2 + \frac{1}{2}(s_1 + s_2 + s_3 + s_4) + 2(2 - a_0^2 - a_1^2)(2 - b_0^2 - b_1^2) \\
&\quad + \frac{1}{2}\big(\lambda - \alpha(a_0 - a_1)\big)^2(1 - b_0^2) + \frac{1}{2}\big(\lambda - \alpha(a_0 + a_1)\big)^2(1 - b_1^2),
\end{aligned}$$

where

$$\begin{aligned}
s_1 &:= (\alpha + 2b_0)^2(1 - a_0^2), \;\; s_2 := (\alpha + 2b_1)^2(1 - a_0^2), \\
s_3 &:= (\alpha - 2b_0)^2(1 - a_1^2), \;\; s_4 := (\alpha - 2b_1)^2(1 - a_1^2), \\
s_5 &:= (2 + a_0 a_1 + a_1 a_0)(1 - b_0^2), \text{ and } s_6 := (2 - a_0 a_1 - a_1 a_0)(1 - b_1^2).
\end{aligned}$$

Suppose f is a state on $\mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes_{max} \mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$ that achieves the optimal correlation p_α. Then $f\left(2\lambda(\lambda - \eta)\right) = 0$. Since $s_1, \ldots, s_6, \lambda - \alpha(a_0 - a_1), \lambda - \alpha(a_0 + a_1), 1 - b_0^2, 1 - b_1^2$, and $(2 - a_0^2 - a_1^2)(2 - b_0^2 - b_1^2)$ are positive in $\mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes_{max} \mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$, and $\lambda - \alpha(a_0 - a_1), \lambda - \alpha(a_0 + a_1)$ commute with $1 - b_0^2, 1 - b_1^2$, we obtain that $f(r_i^2) = f(s_j) = 0$ for $1 \leqslant i \leqslant 4$ and $1 \leqslant j \leqslant 8$ where

$$s_7 := \big(\lambda - \alpha(a_0 - a_1)\big)(1 - b_0^2), \text{ and } s_8 := \big(\lambda - \alpha(a_0 + a_1)\big)(1 - b_1^2).$$

Let $(\pi, \mathcal{H}, |\psi\rangle)$ be the GNS representation of f, and let $\mathcal{L}$ be the left ideal generated by $r_1, \ldots, r_4$ and $s_1, \ldots, s_8$. It follows that $\pi(l)\,|\psi\rangle = 0$ for all $l \in \mathcal{L}$. Observe that

$$(4-\alpha^2)(a_0a_1 + a_1a_0) = \big(b_0(r_3+r_4) - s_7 + 2\lambda\big)\big(b_0(r_3+r_4) - s_7\big) + s_1 + s_3 + 4s_5,$$

so $a_0a_1 + a_1a_0 \in \mathcal{L}$. This also implies

$$1 - b_0^2 = \frac{1}{2}\big(s_5 - (1-b_0^2)(a_0a_1 + a_1a_0)\big) \in \mathcal{L}.$$

Likewise, one can verify that $1-a_0^2, 1-a_1^2$, and $1-b_1^2$ are in $\mathcal{L}$. Furthermore,

$$\lambda a_0 - 2(b_0+b_1) = a_0r_1 + a_1r_2 - (b_0+b_1)\big((1-a_0^2) + (1-a_1^2)\big) + (b_0-b_1)(a_0a_1 + a_1a_0)$$

is in $\mathcal{L}$. Similarly, $\delta a_1 - 2(b_0 - b_1) \in \mathcal{L}$ where $\delta := \sqrt{8-2\alpha^2}$. Let $A_0 := \pi(a_0), A_1 := \pi(a_1), B_0 := \pi(b_0)$, and $B_1 := \pi(b_1)$. Then

$$\begin{aligned}(A_0A_1 + A_1A_0)\,|\psi\rangle &= (\mathbb{1} - A_0^2)\,|\psi\rangle = (\mathbb{1} - A_1^2)\,|\psi\rangle = (\mathbb{1} - B_0^2)\,|\psi\rangle = (\mathbb{1} - B_1^2)\,|\psi\rangle \\ &= \big(\lambda A_0 - 2(B_0+B_1)\big)\,|\psi\rangle = \big(\delta A_1 - 2(B_0 - B_1)\big)\,|\psi\rangle = 0.\end{aligned}$$

For any monomial $a_{i_1}\cdots a_{i_k}b_{j_1}\cdots b_{j_l}$ in $\mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes_{max} \mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$ we have

$$A_{i_1}\cdots A_{i_k}B_{j_1}\cdots B_{j_l}\,|\psi\rangle = B_{j_1}\cdots B_{j_l}\frac{2(B_0 + (-1)^{i_k}B_1)}{\sqrt{8+2(-1)^{i_k}\alpha^2}}\cdots\frac{2(B_0+(-1)^{i_1}B_1)}{\sqrt{8+2(-1)^{i_1}\alpha^2}}\,|\psi\rangle \tag{3.3.3}$$

$$= A_{i_1}\cdots A_{i_k}\frac{\lambda A_0 + (-1)^{j_l}\delta A_1}{4}\cdots\frac{\lambda A_0 + (-1)^{j_1}\delta A_1}{4}\,|\psi\rangle\,. \tag{3.3.4}$$

Hence by Eq. (3.3.3), $(\mathbb{1} - A_0^2)A_{i_1}\cdots A_{i_k}B_{j_1}\cdots B_{j_l}\,|\psi\rangle = 0$, and since $|\psi\rangle$ is cyclic for π, we conclude that $A_0^2 = \mathbb{1}$. Similarly, we have $A_1^2 = B_0^2 = B_1^2 = \mathbb{1}$ and $A_0A_1 + A_1A_0 = 0$. Thus, the C^*-algebra $C^*\langle A_0, A_1\rangle$ generated by A_0 and A_1 is the Clifford algebra of rank 2 which has a unique tracial state. Given $w_1 := A_{i_1}\cdots A_{i_k}$ and $w_2 := A_{j_1}\cdots A_{j_l}$,

$$\begin{aligned}\langle\psi|\,w_1w_2\,|\psi\rangle &= \langle\psi|\,A_{i_1}\cdots A_{i_k}\frac{2(B_0+(-1)^{j_l}B_1)}{\sqrt{8+2(-1)^{j_l}\alpha^2}}\cdots\frac{2(B_0+(-1)^{j_1}B_1)}{\sqrt{8+2(-1)^{j_1}\alpha^2}}\,|\psi\rangle \\ &= \langle\psi|\,\frac{2(B_0+(-1)^{j_l}B_1)}{\sqrt{8+2(-1)^{j_l}\alpha^2}}\cdots\frac{2(B_0+(-1)^{j_1}B_1)}{\sqrt{8+2(-1)^{j_1}\alpha^2}}A_{i_1}\cdots A_{i_k}\,|\psi\rangle \\ &= \langle\psi|\,A_{j_1}\cdots A_{j_l}A_{i_1}\cdots A_{i_k}\,|\psi\rangle = \langle\psi|\,w_2w_1\,|\psi\rangle\,,\end{aligned}$$

so $w \mapsto \langle\psi| w |\psi\rangle$ must be the unique tracial state on $C^*\langle A_0, A_1\rangle$. By Eq. (3.3.4), there is a unique state on $\mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes_{max} \mathcal{A}_{POVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$ achieving p_α, so p_α is a commuting operator self-test. □

We leave it as an open problem to show that there are commuting operator self-tests which do not have finite-dimensional models.

Chapter 4

Robust self-testing

4.1 An operator-algebraic formulation of robust self-testing

We study robust self-testing in this chapter. To define a robust self-test, we need the following notion of approximate dilation.

Definition 4.1.1. *Given $\epsilon \geqslant 0$ and two quantum models*

$$S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\big) \text{ and}$$
$$\widetilde{S} = \big(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\widetilde{\psi}\rangle\big),$$

we say $\widetilde{S}$ is an local ϵ-dilation of S, denoted $S \succeq_\epsilon \widetilde{S}$, if there are isometries $I_A : \mathcal{H}_A \to \widetilde{\mathcal{H}}_A \otimes \mathcal{H}_A^{aux}$ and $I_B : \mathcal{H}_B \to \widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}$, and vector state $|aux\rangle \in \mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}$ such that

$$I_A \otimes I_B\big(M_a^x \otimes \mathbb{1} |\psi\rangle\big) \approx_\epsilon \big(\widetilde{M}_a^x \otimes \mathbb{1} |\widetilde{\psi}\rangle\big) \otimes |aux\rangle \tag{4.1.1}$$
$$I_A \otimes I_B\big(\mathbb{1} \otimes N_b^y |\psi\rangle\big) \approx_\epsilon \big(\mathbb{1} \otimes \widetilde{N}_b^y |\widetilde{\psi}\rangle\big) \otimes |aux\rangle, \text{ and} \tag{4.1.2}$$
$$I_A \otimes I_B |\psi\rangle \approx_\epsilon |\widetilde{\psi}\rangle \otimes |aux\rangle. \tag{4.1.3}$$

for all $(a, b, x, y) \in A \times B \times X \times Y$.

Note that, in the above definition, Equations (4.1.1) to (4.1.3) imply

$$I_A M_a^x I_A^* \otimes \mathbb{1} \, |\widetilde{\psi}, aux\rangle \approx_{2\epsilon} \left(\widetilde{M}_a^x \otimes \mathbb{1} \, |\widetilde{\psi}\rangle\right) \otimes |aux\rangle, \tag{4.1.4}$$

$$\mathbb{1} \otimes I_B N_b^y I_B^* \, |\widetilde{\psi}, aux\rangle \approx_{2\epsilon} \left(\mathbb{1} \otimes \widetilde{N}_b^y \, |\widetilde{\psi}\rangle\right) \otimes |aux\rangle, \text{ and} \tag{4.1.5}$$

$$I_A \otimes I_B\big(M_a^x \otimes N_b^y \, |\psi\rangle\big) \approx_{3\epsilon} \left(\widetilde{M}_a^x \otimes \widetilde{N}_b^y \, |\widetilde{\psi}\rangle\right) \otimes |aux\rangle. \tag{4.1.6}$$

We often use Equation (4.1.6) (with 3ϵ replaced by ϵ) as the definition of $S \succeq_\epsilon \widetilde{S}$.

Definition 4.1.2. *Let $\mathcal{C}$ be a class of quantum models. We say a quantum correlation $p \in C_q$ is a **robust self-test** for $\mathcal{C}$ if there is an ideal model $\widetilde{S} \in \mathcal{C}$ such that the following holds. For any $\delta \geqslant 0$, there is an $\epsilon \geqslant 0$ such that $S \succeq_\delta \widetilde{S}$ for any model $S \in \mathcal{C}$ satisfying $\|p_S - p\|_1 \leqslant \epsilon$.*

Here the 1-norm of a vector $v \in \mathbb{R}^{A\times B\times X\times Y}$ is given by $\|v\|_1 := \sum_{a,b,x,y}|v(a,b|x,y)|$. Taking $\delta = 0$ in the above definition, we see that every robust self-test is a self-test. On the other hand, the following question is still open for quantum correlations.

Question 4.1.3. *Is every self-test a robust self-test?*

We'll also discuss robust self-testing for nonlocal games in Section 4.2. Question 4.1.3 has a negative answer in this context: Mančinska and Simon construct a nonlocal game $\mathcal{G}$ which is a self-test but not a robust self-test [MS23]. In their example, the game $\mathcal{G}$ has a unique perfect quantum correlation p and p is a self-test, so $\mathcal{G}$ is a self-test as is p. However, $\mathcal{G}$ also has a perfect quantum approximate correlation $p' \in C_{qa}$ that is not in C_q. One can take a sequence of quantum models $S_n, n \in \mathbb{N}$ such that $\|p_{S_n} - p'\|_1 \to 0$ as $n \to \infty$. While S_n has an increasing winning probability for $\mathcal{G}$ as $n \to \infty$, it becomes "far away" from the ideal model under local dilations. This illustrates that this self-test is not robust.

In Section 3.1, we have seen an operator-algebraic formulation of self-testing. Suppose $p \in C_q(X, Y, A, B)$ is a self-test for all quantum models. Then there is a unique finite-dimensional state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ for p. In this section, we attempt to give an operator-algebraic formulation of robust self-testing. The following theorem states that if in addition, p is a robust self-test, then f is indeed the unique state on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ that can achieve p.

Theorem 4.1.4. *If $p \in C_q(X, Y, A, B)$ is a robust self-test for all quantum models, then p is an abstract state self-test for all states on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$.*

This theorem looks very similar to the "only if" direction of Corollary 3.1.6, part (a), which states that if $p \in C_q(X, Y, A, B)$ is a self-test for all quantum models then p is an abstract state self-test for finite-dimensional states on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$. Compared to Corollary 3.1.6, Theorem 4.1.4 replaces "self-test" and "finite-dimensional states" with "robust self-test" and "all states" respectively.

Note that a quantum correlation $p \in C_q$ can always be achieved by *some* finite-dimensional states. So if f is the unique state for a quantum correlation, then f must be finite-dimensional. This gives an alternative way to phrase Theorem 4.1.4:

Theorem 4.1.5 (Restated from Theorem 4.1.4)**.** *If $p \in C_q(X, Y, A, B)$ is a robust self-test for all quantum models, then*

(i) there is a unique finite-dimensional state on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ for p and

(ii) there is no infinite-dimensional state on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ that can achieve p.

We prove this theorem at the end of this section. Part (a) of Corollary 3.1.6 is an if-and-only-if statement, so we ask whether the converse of Theorem 4.1.4 holds or not:

Question 4.1.6. *Let $p \in C_q(X, Y, A, B)$ be an extreme point in C_q. Suppose p is an abstract state self-test for all states on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$. Is p a robust self-test for all quantum models?*

Through Sections 4.2 to 4.4, we aim to give an affirmative answer to Question 4.1.6 for a large class of quantum correlations.

Theorem 4.1.7. *Suppose $p \in C_q(X, Y, A, B)$ is the unique perfect quantum correlation for a synchronous game, or the unique optimal quantum correlation for an XOR game. Then p is a robust self-test for all quantum models if and only if p is an abstract state self-test for all states on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$.*

Our proof approach is based on algebraic characterizations of synchronous games and XOR games established in [Slo11, HMPS19, KPS18]. For any synchronous game (resp. XOR game) $\mathcal{G}$, one can associate a finitely-presented algebra $C^*(\mathcal{G})$ such that perfect (resp. optimal) strategies for $\mathcal{G}$ correspond to tracial states on $C^*(\mathcal{G})$. Furthermore, as shown in [Pad24], any near-perfect (resp. near-optimal) strategy S for $\mathcal{G}$ defines an approximate state ϕ on $C^*(\mathcal{G})$ which is also approximately tracial. Finally, using a lifting theorem for $C^*(\mathcal{G})$, we lift ϕ to a ucp map θ on $C^*(\mathcal{G})$ and construct the desired local dilation $I_A \otimes I_B$ from the Stinespring dilation of θ. This last step is inspired by [MPS21].

The proof approach outlined above applies to any nonlocal game that exhibits structures similar to synchronous or XOR games. In particular, Theorem 4.1.7 also holds if p is the unique perfect quantum correlation for a Boolean constraint system (BCS) game. Indeed, we'll prove a general result (Theorem 4.4.9). Given a nonlocal game $\mathcal{G}$, we say an algebra $C^*(\mathcal{G})$ is the associated game algebra for $\mathcal{G}$ if (i) every optimal strategy for $\mathcal{G}$ corresponds to a tracial state on $C^*(\mathcal{G})$ and (ii) every near-optimal strategy for $\mathcal{G}$ corresponds to an approximate state on $C^*(\mathcal{G})$ which is also approximately tracial. In Theorem 4.4.9, we show that if p is the unique optimal quantum correlation for a game $\mathcal{G}$ which has an associated game algebra, then p is a robust self-test for all quantum models if and only if p is an abstract state self-test for all abstract states.

This general result also provides a convenient way to examine whether a nonlocal game is an exact self-test or a robust self-test by studying the tracial states on the associated game algebras.

Theorem 4.1.8 (Restated from part of Theorem 4.3.22 and Corollary 4.4.11, informal)**.** *Suppose a nonlocal game $\mathcal{G}$ has an associated game algebra $C^*(\mathcal{G})$.*

(a) $\mathcal{G}$ is a self-test for its optimal quantum strategies if and only if $C^*(\mathcal{G})$ has a unique finite-dimensional tracial state.

(b) $\mathcal{G}$ is a robust self-test for its optimal quantum strategies if $C^*(\mathcal{G})$ has a unique tracial state τ and τ is finite-dimensional.

Part (b) of Theorem 4.1.8 provides one-line proofs for many robust self-testing results. For example, CHSH game is a robust self-test because the associate game algebra Cl_2, the Clifford algebra of rank 2, has a unique tracial state τ and τ is finite-dimensional. This tracial-state characterization of robust self-testing also raises the prospect of constructing new robust self-tests from C^*-algebras which are known to have a unique tracial state (e.g., matrix algebras, Clifford algebras of even rank, etc.).

For the practical use of robust self-testing, it is important to study the $\epsilon-\delta$ dependence in Definition 4.1.2, which is also known as the *robustness* of a self-test. In many cases, the robustness of a self-test is closely related to the stability of some groups/algebras under approximate representations. We discuss some concrete examples in Chapter 5.

Finally, we conjecture that the answer to Question 4.1.6 is true for all extreme quantum correlations.

Conjecture 4.1.9. *Suppose $p \in C_q(X, Y, A, B)$ is an extreme point in C_q. Then p is a robust self-test for all quantum models if and only if p is an abstract state self-test for all states on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$.*

4.1.1 Robust self-tests are abstract state self-tests

We prove Theorem 4.1.4 in this subsection. Recall that for any residually finite-dimensional C^*-algebras $\mathcal{A}$ and $\mathcal{B}$, the C^*-algebra $\mathcal{A} \otimes_{min} \mathcal{B}$ is also residually finite-dimensional, so the set of finite-dimensional states on $\mathcal{A} \otimes_{\min} \mathcal{B}$ forms a weak*-dense subset of the state space of $\mathcal{A} \otimes_{\min} \mathcal{B}$. Taking $\mathcal{A} = \mathcal{A}_{POVM}^{X,A}$ and $\mathcal{B} = \mathcal{A}_{POVM}^{Y,B}$, we have:

Proposition 4.1.10. *For every state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ there is a sequence of quantum models $S_n, n \in \mathbb{N}$ such that $\lim_{n\to\infty} f_{S_n} = f$ in the weak*-topology.*

For the completeness of this thesis, we present a proof of Proposition 4.1.10 in Appendix A. Before we prove Theorem 4.1.4, we need the following proposition, which is the robust version of Proposition 3.1.18.

Proposition 4.1.11. *Let*

$$S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\right) \text{ and}$$
$$\widetilde{S} = \left(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\widetilde{\psi}\rangle\right)$$

be two quantum models with associated representations $\pi_A \otimes \pi_B$ and $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$ respectively. If $\widetilde{S}$ is centrally supported and $S \succeq_\epsilon \widetilde{S}$ via local isometry $I_A \otimes I_B$ and vector state $|aux\rangle$, then for every $k, \ell \in \mathbb{N}$ and monomials $\alpha = m_{a_1}^{x_1} \cdots m_{x_k}^{a_k} \in \mathcal{A}_{POVM}^{X,A}, \beta = n_{b_1}^{y_1} \cdots n_{b_\ell}^{y_\ell} \in \mathcal{A}_{POVM}^{Y,B}$ we have

$$\left(\widetilde{\pi}_A(\alpha) \otimes \mathbb{1} \, |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \approx_{(2k+1)\epsilon} I_A \pi_A(\alpha) I_A^* \otimes \mathbb{1} \, |\widetilde{\psi}, aux\rangle\,, \tag{4.1.7}$$
$$\left(\mathbb{1} \otimes \widetilde{\pi}_B(\beta) \, |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \approx_{(2\ell+1)\epsilon} \mathbb{1} \otimes I_B \pi_B(\beta) I_B^* \, |\widetilde{\psi}, aux\rangle \tag{4.1.8}$$

and $|f_S(\alpha \otimes \beta) - f_{\widetilde{S}}(\alpha \otimes \beta)| \leqslant 2(k + \ell + 1)\epsilon$.

Proof. We first prove Equation (4.1.7) by induction on the monomial degree $k \in \mathbb{N}$. The base cases $k = 0, 1$ follow straight Equation (4.1.4). Suppose Equation (4.1.7) holds for all monomials in $\mathcal{A}_{POVM}^{X,A}$ of degree k. For any given monomial $\alpha = \alpha_1 \cdots \alpha_k \alpha_{k+1}$ in $\mathcal{A}_{POVM}^{X,A}$ of degree $k+1$, let $\alpha' := \alpha_1 \cdots \alpha_k$. Since $\widetilde{S}$ is centrally supported, there is an operator $\widetilde{F} \in \mathcal{B}(\widetilde{\mathcal{H}}_B)$ with $\|\widetilde{F}\| \leqslant \|\widetilde{\pi}_A(\alpha_{k+1})\| \leqslant 1$ such that $\widetilde{\pi}_A(\alpha_{k+1}) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle = \mathbb{1}_{\widetilde{\mathcal{H}}_A} \otimes \widetilde{F} \, |\widetilde{\psi}\rangle$. Note that $\|\widetilde{\pi}_A(\alpha')\| \leqslant 1$ and $\|I_A \pi_A(\alpha') I_A^*\| \leqslant 1$. Thus by the inductive hypothesis,

$$\begin{aligned}
\left(\widetilde{\pi}_A(\alpha) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle\right) \otimes |aux\rangle &= \left(\widetilde{\pi}_A(\alpha')\widetilde{\pi}_A(\alpha_{k+1}) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \\
&= \left(\widetilde{\pi}_A(\alpha') \otimes \widetilde{F} \, |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \\
&\approx_{(2k+1)\epsilon} I_A \pi_A(\alpha') I_A^* \otimes \widetilde{F} \otimes \mathbb{1}_{\mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \\
&= \left(I_A \pi_A(\alpha') I_A^* \left(\widetilde{\pi}_A(\alpha_{k+1}) \otimes \mathbb{1}_{\mathcal{H}_A^{aux}}\right)\right) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \\
&\approx_{2\epsilon} I_A \pi_A(\alpha') I_A^* I_A \pi_A(\alpha_{k+1}) I_A^* \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B \otimes \mathcal{H}_B^{aux}} |\widetilde{\psi}, aux\rangle \\
&= I_A \pi_A(\alpha) I_A^* \otimes \mathbb{1} \, |\widetilde{\psi}, aux\rangle\,.
\end{aligned}$$

This implies $\left(\widetilde{\pi}_A(\alpha) \otimes \mathbb{1} \, |\widetilde{\psi}\rangle\right) \otimes |aux\rangle \approx_{\left(2(k+1)+1\right)\epsilon} I_A \pi_A(\alpha) I_A^* \otimes \mathbb{1} \, |\widetilde{\psi}, aux\rangle$. We conclude that Equation (4.1.7) holds for all $k \in \mathbb{N}$ and monomials in $\mathcal{A}_{POVM}^{X,A}$ of degree k. The

proof of Equation (4.1.8) is similar. The rest follows from the following lemma by taking $|\alpha\rangle = I_A\pi_A(\alpha)I_A^* \otimes \mathbb{1}\,|\widetilde{\psi}, aux\rangle$, $|\beta\rangle = I_B\pi_B(\beta)I_B^*\,|\widetilde{\psi}, aux\rangle$, $|\widetilde{\alpha}\rangle = \big(\widetilde{\pi}_A(\alpha)\otimes\mathbb{1}\,|\widetilde{\psi}\rangle\big)\otimes|aux\rangle$, and $|\widetilde{\beta}\rangle = \big(\mathbb{1}\otimes\widetilde{\pi}_B(\beta)\,|\widetilde{\psi}\rangle\big)\otimes|aux\rangle$. □

Lemma 4.1.12. *If $|\alpha\rangle, |\widetilde{\alpha}\rangle, |\beta\rangle, |\widetilde{\beta}\rangle$ are four vectors with norm $\leqslant 1$ such that $|\alpha\rangle \approx_{\delta_1} |\widetilde{\alpha}\rangle$ and $|\beta\rangle \approx_{\delta_2} |\widetilde{\beta}\rangle$, then $|\langle\alpha|\beta\rangle - \langle\widetilde{\alpha}|\widetilde{\beta}\rangle| \leqslant \delta_1 + \delta_2$.*

Proof. Observe that $\langle\alpha|\beta\rangle - \langle\widetilde{\alpha}|\widetilde{\beta}\rangle = \big(\langle\alpha| - \langle\widetilde{\alpha}|\,\big)\,|\beta\rangle + \langle\widetilde{\alpha}|\,\big(\,|\beta\rangle - |\widetilde{\beta}\rangle\big)$. The lemma follows from the Cauchy-Schwartz inequality. □

Now we are ready to prove Theorem 4.1.4.

Proof of Theorem 4.1.4. Suppose $\widetilde{p} \in C_q(X, Y, A, B)$ is a robust self-test for all quantum models, and let $\widetilde{S}$ be an ideal model. By Corollary 3.1.6, there is a unique finite-dimensional state $\widetilde{f}$ on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ achieving $\widetilde{p}$. Assume for the sake of contradiction that there is an infinite-dimensional state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ achieving $\widetilde{p}$. By Proposition 4.1.10 there exists a sequence of quantum models $S_n, n \in \mathbb{N}$ such that $f = \lim_{n\to\infty} f_{S_n}$ in the weak*-topology. This implies $\widetilde{p}(a,b|x,y) = f(m_a^x \otimes n_b^y) = \lim_{n\to\infty} f_{S_n}(m_a^x \otimes n_b^y) = \lim_{n\to\infty} p_{S_n}(a,b|x,y)$ for all x, y, a, b. By the definition of robust self-testing, there is a function $\eta : \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ with $\lim_{n\to\infty} \eta(n) = 0$ such that $S_n \geq_{\eta(n)} \widetilde{S}$ for all $n \in \mathbb{N}$. Then for all monomials $\alpha \in \mathcal{A}_{POVM}^{X,A}$ and $\beta \in \mathcal{A}_{POVM}^{Y,B}$, by Proposition 4.1.11, $|f_{S_n}(\alpha\otimes\beta) - \widetilde{f}(\alpha\otimes\beta)| \leqslant 2\big(\deg(\alpha)+\deg(\beta)+1\big)\eta(n) \to 0$ as $n \to \infty$. This means $\lim_{n\to\infty} f_{S_n} = \widetilde{f}$ in the weak*-topology. Hence $\widetilde{f} = f$, a contradiction. We conclude that there is no infinite-dimensional state on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ for p. □

4.2 From correlations to nonlocal games

We discuss self-testing for nonlocal games in this section. We often refer to models as strategies when working with nonlocal games. For any nonlocal game $\mathcal{G} = (X, Y, A, B, \mu, V)$, we define its *game polynomial* to be the $*$-polynomial

$$\Phi_{\mathcal{G}} := \sum_{x,y,a,b} \mu(x,y)V(a,b|x,y)m_a^x \otimes n_b^y$$

in $\mathbb{C}^*\langle m_a^x : x \in X, a \in A\rangle \otimes \mathbb{C}^*\langle n_b^y : y \in Y, b \in B\rangle$. The optimal quantum value $w_q(\mathcal{G})$ of the game $\mathcal{G}$ is equal to the supremum value of $f(\Phi_\mathcal{G})$ over all states f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. The same conclusion holds if we replace $\mathcal{A}_{POVM}$ with $\mathcal{A}_{PVM}$.

We say a state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ (or $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$) is optimal for $\mathcal{G}$ if $f(\Phi_\mathcal{G}) = w_q(\mathcal{G})$. Equivalently, f is optimal for $\mathcal{G}$ if the quantum approximate correlation achieved by f is optimal for $\mathcal{G}$. Since C_q consists of correlations that can be achieved by finite-dimensional states, $\mathcal{G}$ has an optimal quantum strategy if and only if there exists a finite-dimensional optimal state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ for $\mathcal{G}$. The following lemma is straightforward from the GNS construction.

Lemma 4.2.1. *Let $\mathcal{G} = (X, Y, A, B, \mu, V)$ be a nonlocal game. For any $*$-representation π of $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$, the operator $\pi(\Phi_\mathcal{G})$ has spectrum* $\text{spec}\left(\pi(\Phi_\mathcal{G})\right) \subseteq [0, w_q(\mathcal{G})]$.

Now we define self-testing for nonlocal games.

Definition 4.2.2. *Let $\mathcal{C}$ be a class of quantum models. A nonlocal game $\mathcal{G}$ is a self-test for its optimal quantum strategies in $\mathcal{C}$ if there is an optimal quantum strategy $\widetilde{S} \in \mathcal{C}$ for $\mathcal{G}$ such that $S \geq \widetilde{S}$ for any optimal quantum strategy $S \in \mathcal{C}$ for $\mathcal{G}$.*

In Definition 4.2.2, $\widetilde{S}$ is referred to as an *ideal optimal quantum strategy for $\mathcal{G}$*. When $\mathcal{C}$ is the class of all quantum models, we simply say that $\mathcal{G}$ is a self-test for its optimal quantum strategies; when $\mathcal{C}$ is the class of all projective quantum models, we say that $\mathcal{G}$ is a self-test for its projective optimal quantum strategies. Combining with Definition 3.1.2, we immediately see that:

Lemma 4.2.3. *A nonlocal game $\mathcal{G}$ is a self-test for its optimal quantum strategies (resp. projective optimal quantum strategies) if and only if $\mathcal{G}$ has a unique optimal quantum correlation p and p is a self-test for all quantum models (resp. projective quantum models).*

The following lemma implies that if a nonlocal game is a self-test for its optimal quantum strategies (or optimal projective quantum strategies), then its unique optimal quantum correlation must be an extreme point in C_q.

Lemma 4.2.4. *If a nonlocal game $\mathcal{G}$ has a unique optimal quantum correlation p, then p must be an extreme point in C_q.*

Proof. Suppose $\mathcal{G}$ has a unique optimal quantum correlation p. Assume for the sake of contradiction that p is not an extreme point in C_q. Then $p = \lambda p_1 + (1-\lambda)p_2$ for some $0 < \lambda < 1$ and $p_1 \neq p_2$ in C_q. Note that p is optimal. So

$$w(\mathcal{G};p) = \lambda w(\mathcal{G};p_1) + (1-\lambda)w(\mathcal{G};p_2) \leqslant \lambda w(\mathcal{G};p) + (1-\lambda)w(\mathcal{G};p) = w(\mathcal{G};p).$$

It follows that $w(\mathcal{G};p_1) = w(\mathcal{G};p_2) = w(\mathcal{G};p)$. The uniqueness of p implies that $p = p_1 = p_2$, which is a contradiction. Hence p must be an extreme point in C_q. □

On the other hand, if a nonlocal game has a unique optimal state f, then f is an extreme point in the state space:

Lemma 4.2.5. *Let $\mathcal{G} = (X, Y, A, B, \mu, V)$ be a nonlocal game. Suppose that there is a unique finite-dimensional optimal state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ (or $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$) for $\mathcal{G}$. Then f is a pure state, and the correlation p achieved by f is the unique optimal quantum correlation for $\mathcal{G}$.*

Proof. Let p be the correlation achieved by f. Since $w(\mathcal{G};p) = f(\Phi_{\mathcal{G}}) = w_q(\mathcal{G})$, p is optimal for $\mathcal{G}$. Assume $\mathcal{G}$ has another optimal quantum correlation p'. Then there is a finite-dimensional state f' that can achieve p'. So f' is optimal for $\mathcal{G}$, but $f' \neq f$, a contradiction. We conclude that p is the unique optimal quantum correlation for p. By Lemma 4.2.3, p is an extreme point in C_q. Since any state that can achieve p is optimal for $\mathcal{G}$, f must be the unique finite-dimensional state for $\mathcal{G}$. By Corollary 3.2.4, the GNS representation of f is irreducible. It follows that f is a pure state. □

Lemmas 4.2.4 and 4.2.5 allows us to translate many self-testing results established for extremal quantum correlations in Section 3.1 to self-testing for nonlocal games.

Theorem 4.2.6 (Corollary 3.1.6, game version)**.** *Let $\mathcal{G} = (X, Y, A, B, \mu, V)$ be a nonlocal game.*

(a) *$\mathcal{G}$ is a self-test for its optimal quantum strategies if and only if there is a unique finite-dimensional optimal state on $\mathcal{A}^{X,A}_{POVM} \otimes_{min} \mathcal{A}^{Y,B}_{POVM}$ for $\mathcal{G}$.*

(b) *If $\mathcal{G}$ has a full-rank projective optimal quantum strategy, then $\mathcal{G}$ is a self-test for its projective optimal strategies if and only if there is a unique finite-dimensional optimal state on $\mathcal{A}^{X,A}_{PVM} \otimes_{min} \mathcal{A}^{Y,B}_{PVM}$ for $\mathcal{G}$.*

Theorem 4.2.7 (Theorem 3.1.7, game version)**.** *For any nonlocal game $\mathcal{G}$, the following statements hold.*

(a) *If $\mathcal{G}$ is a self-test for its optimal quantum strategies, then $\mathcal{G}$ has a full-rank projective ideal optimal strategy and $\mathcal{G}$ is a self-test for its projective optimal quantum strategies.*

(b) *If $\mathcal{G}$ is a self-test for its projective optimal quantum strategies and $\mathcal{G}$ has a full-rank projective optimal strategy, then $\mathcal{G}$ is a self-test for its optimal quantum strategies.*

Corollary 4.2.8 (Corollary 3.1.8, game version)**.** *If $\mathcal{G}$ has a full-rank projective optimal quantum strategy, then the following statements are equivalent.*

(1) *$\mathcal{G}$ is a self-test for its optimal quantum strategies.*

(2) *$\mathcal{G}$ is a self-test for its projective optimal quantum strategies.*

(3) *There is a unique finite-dimensional optimal state on $\mathcal{A}^{X,A}_{POVM} \otimes \mathcal{A}^{Y,B}_{POVM}$ for $\mathcal{G}$.*

(4) *There is a unique finite-dimensional optimal state on $\mathcal{A}^{X,A}_{PVM} \otimes \mathcal{A}^{Y,B}_{PVM}$ for $\mathcal{G}$.*

Recall from Corollary 3.2.4 that if there is a unique finite-dimensional state f achieving an extreme quantum correlation p, then f has a GNS representation $(\mathcal{H}, \pi, |\psi\rangle)$ where $\pi = \pi_A \otimes \pi_B$ is a tensor product of two irreducible representations. Furthermore, p is a self-test for quantum models and there is an ideal model with an associated representation $\pi_A \otimes \pi_B$. We can sharpen this statement when working with self-testing for nonlocal games:

Theorem 4.2.9. *Suppose a nonlocal game $\mathcal{G} = (X, Y, A, B, \mu, V)$ has a unique finite-dimensional optimal state $\widetilde{f}$ on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. Then the following statement holds.*

(a) $\widetilde{f}$ has a GNS representation $(\widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B, \widetilde{\pi}_A \otimes \widetilde{\pi}_B, |\widetilde{\psi}\rangle)$ where $\widetilde{\pi}_A$ and $\widetilde{\pi}_B$ are irreducible $*$-representations of $\mathcal{A}_{POVM}^{X,A}$ and $\mathcal{A}_{POVM}^{Y,B}$ respectively.

(b) Let $\widetilde{M}_a^x := \widetilde{\pi}_A(m_a^x)$ and $\widetilde{N}_b^y := \widetilde{\pi}_B(n_b^y)$. Then $\mathcal{G}$ is a self-test for its optimal quantum strategies with an ideal optimal strategy

$$\widetilde{S} = \big(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\widetilde{\psi}\rangle\big).$$

(c) $\widetilde{\pi} := \widetilde{\pi}_A \otimes \widetilde{\pi}_B$ is the unique (up to unitary equivalence) finite-dimensional irreducible $*$-representation of $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ with the property that the maximal eigenvalue of $\widetilde{\pi}(\Phi_{\mathcal{G}})$ is $w_q(\mathcal{G})$.

(d) The $w_q(\mathcal{G})$-eigenspace of $\widetilde{\pi}(\Phi_{\mathcal{G}})$ is the one-dimensional space spanned by $|\widetilde{\psi}\rangle$.

Proof. Let p be the correlation achieved by $\widetilde{f}$. Then by Lemmas 4.2.3 and 4.2.5, p is an extreme point in C_q, p is the unique optimal quantum correlation for $\mathcal{G}$, and $\widetilde{f}$ is the unique finite-dimensional state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ achieving p. So parts (a) and (b) follow from Corollary 3.2.4.

Now suppose $\pi : \mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B} \to \mathcal{B}(\mathcal{H})$ is a finite-dimensional irreducible $*$-representation such that the maximal eigenvalue of $\pi(\mathcal{G})$ is $w_q(\mathcal{G})$. Let $|\psi\rangle$ be a unit vector in the $w_q(\mathcal{G})$-eigenspace of $\pi(\mathcal{G})$. Since $\pi(\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}) = \mathcal{B}(\mathcal{H})$, the vector $|\psi\rangle$ is cyclic for π. Hence $(\mathcal{H}, \pi, |\psi\rangle)$ is a GNS representation of the state f given by $f(\alpha) := \langle\psi| \pi(\alpha) |\psi\rangle, \alpha \in \mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. This also means f is a finite-dimensional state on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ such that $f(\Phi_{\mathcal{G}}) = \langle\psi| \pi(\Phi_{\mathcal{G}}) |\psi\rangle = w_q(\mathcal{G})$. By the uniqueness of $\widetilde{f}$, we have $f = \widetilde{f}$, and hence $(\mathcal{H}, \pi, |\psi\rangle)$ is unitarily equivalent to $(\widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B, \widetilde{\pi}, |\widetilde{\psi}\rangle)$. This proves part (c).

To see part (d), take an arbitrary unit vector $|\psi\rangle$ in the $w_q(\mathcal{G})$-eigenspace of $\widetilde{\pi}(\Phi_{\mathcal{G}})$. Then the state f defined by $f(\alpha) := \langle\psi| \widetilde{\pi}(\alpha) |\psi\rangle, \alpha \in \mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ is optimal for

$\mathcal{G}$. So $f = \widetilde{f}$. It follows that $(\widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B, \widetilde{\pi}, |\psi\rangle)$ is a GNS representation for $\widetilde{f}$. This means there is a unitary U on $\widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B$ such that

$$U|\psi\rangle = |\widetilde{\psi}\rangle, \text{ and} \tag{4.2.1}$$

$$U\widetilde{\pi}(\alpha)U^* = \widetilde{\pi}(\alpha) \tag{4.2.2}$$

for all $\alpha \in \mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. Note that $\widetilde{\pi}$ is irreducible. Equation (4.2.2) implies $U = \lambda \mathbb{1}$ for some $\lambda \in \mathbb{C}$. Then Equation (4.2.1) implies $|\psi\rangle$ is linearly dependent with $|\widetilde{\psi}\rangle$. Since $|\psi\rangle$ was arbitrary, part (d) follows. □

4.2.1 Robust self-testing for nonlocal games

We also define robust self-testing for nonlocal games. We say a strategy S is ϵ-optimal for a nonlocal game $\mathcal{G}$ if $w(\mathcal{G}; S) \geqslant w_q(\mathcal{G}) - \epsilon$.

Definition 4.2.10. *Let $\mathcal{C}$ be a class of quantum models. A nonlocal game $\mathcal{G}$ is a robust self-test for its optimal strategies in $\mathcal{C}$ if there is an ideal optimal quantum strategy $\widetilde{S} \in \mathcal{C}$ for $\mathcal{G}$ such that the following statement holds. For any $\delta \geqslant 0$, there is an $\epsilon \geqslant 0$ such that $S \succeq_\delta \widetilde{S}$ for any ϵ-optimal strategy $S \in \mathcal{C}$ for $\mathcal{G}$.*

Recall that the set of quantum approximate correlations C_{qa} is the closure of C_q. The following lemma is a robust version of Lemma 4.2.3, although the proof is less straightforward.

Lemma 4.2.11. *A nonlocal game $\mathcal{G}$ is a robust self-test for its optimal quantum strategies (resp. projective optimal quantum strategies) if and only if $\mathcal{G}$ has a unique quantum approximate correlation p and p is a robust self-test for all quantum models[1] (resp. projective quantum models).*

Proof. For the "only if" direction, suppose $\mathcal{G} = (X, Y, A, B, V)$ is a robust self-test for its optimal quantum strategies, and let $\widetilde{S}$ be an ideal optimal strategy. By Lemma 4.2.3, the

[1]This last condition automatically implies that p is in C_q.

quantum correlation $\widetilde{p}$ generated by $\widetilde{S}$ is the unique optimal quantum correlation for $\mathcal{G}$. We claim that $\widetilde{p}$ is indeed the unique optimal quantum approximate correlation for $\mathcal{G}$. Assume for the sake of contradiction that $\mathcal{G}$ has an optimal correlation $p \in C_{qa}$ while p is not in C_q. Then there is an infinite-dimensional state f achieving p. By Proposition 4.1.10, there is a sequence of quantum models $S_n, n \in \mathbb{N}$ such that $\lim_{n\to\infty} f_{S_n} = f$ in the weak-$*$ topology. This implies $w(\mathcal{G}; S_n) = f_{S_n}(\Phi_{\mathcal{G}}) \to f(\Phi_{\mathcal{G}}) = w_q(\mathcal{G})$ as $n \to \infty$. Since $\mathcal{G}$ is a robust self-test for its optimal quantum strategies, there is a function $\eta : \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ with $\lim_{n\to\infty} \eta(n) = 0$ such that $S_n \succeq_{\eta(n)} \widetilde{S}$. It follows that $p = \lim_{n\to\infty} p_{S_n} = p_{\widetilde{S}} = \widetilde{p}$, which contradicts to the assumption that p is not in C_q. We conclude that $\widetilde{p}$ is the unique quantum approximate correlation for $\mathcal{G}$. Note that for any quantum model S, $\|p_S - \widetilde{p}\|_1 \leqslant \epsilon$ implies $w(\mathcal{G}; S) \geqslant w_q(\mathcal{G}) - \epsilon$. So $\mathcal{G}$ is a robust self-test as is p.

For the "if" direction, suppose that $\mathcal{G}$ has a unique optimal quantum approximate correlation $\widetilde{p}$ and that $\widetilde{p}$ is a robust self-test for quantum models, and let $\widetilde{S}$ be an ideal model for $\widetilde{p}$. Then $\widetilde{p}$ must be in C_q. Assume for the sake of contradiction that $\mathcal{G}$ is not a robust self-test. This means there exists a $\delta > 0$ and a sequence of quantum models $S_n, n \in \mathbb{N}$ with $\epsilon_n := w_q(\mathcal{G}) - w(\mathcal{G}; S_n) \to 0$ as $n \to \infty$ such that for all $n \in \mathbb{N}$, $S_n \succeq_\delta \widetilde{S}$ does not hold. Let p be an accumulation point of $\{p_{S_n}, n \in \mathbb{N}\}$. Then p is in C_{qa} and p is optimal for $\mathcal{G}$. The uniqueness of $\widetilde{p}$ implies that $p = \widetilde{p}$. By passing a subsequence, we may assume without loss of generality that $\lim_{n\to\infty} p_{S_n} = \widetilde{p}$. Since $\widetilde{p}$ is a robust self-test for quantum models, there is a function $\eta : \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ with $\lim_{n\to\infty} \eta(n) = 0$ such that $S_n \succeq_{\eta(n)} \widetilde{S}$ for all $n \in \mathbb{N}$. Take a large enough N such that $\eta(N) \leqslant \delta$, we see that $S_N \succeq_\delta \widetilde{S}$, a contradiction. We conclude that $\mathcal{G}$ is a robust self-test for its optimal quantum strategies. □

We can also state a game version of Theorem 4.1.4 (or equivalently Theorem 4.1.5).

Theorem 4.2.12 (Theorem 4.1.5, game version)**.** *If $\mathcal{G} = (X, Y, A, B, \mu, V)$ is a robust self-test for its optimal quantum strategies, then*

(i) there is a unique finite-dimensional optimal state on $\mathcal{A}^{X,A}_{POVM} \otimes_{min} \mathcal{A}^{Y,B}_{POVM}$ for $\mathcal{G}$ and

(ii) there is no infinite-dimensional optimal state for $\mathcal{G}$.

The following proposition will be used frequently in the proof of robust self-testing results.

Proposition 4.2.13. *Suppose a nonlocal game $\mathcal{G} = (X, Y, A, B, \mu, V)$ has a unique finite-dimensional optimal state $\widetilde{f}$ on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. Let $\widetilde{S} = \big(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\widetilde{\psi}\rangle\big)$ and $\widetilde{\pi} = \widetilde{\pi}_A \otimes \widetilde{\pi}_B$ be as in Theorem 4.2.9. Let Δ be the spectral gap of $\widetilde{\pi}(\Phi_G)$ (i.e., the second largest eigenvale of $\widetilde{\pi}(\Phi_G)$ is $w_q(\mathcal{G}) - \Delta$). Suppose*

$$S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\big)$$

is an ϵ-optimal quantum strategy for $\mathcal{G}$. Let $I_A : \mathcal{H}_A \to \widetilde{\mathcal{H}}_A \otimes \mathcal{K}_A$ and $I_B : \mathcal{H}_B \to \widetilde{\mathcal{H}}_B \otimes \mathcal{K}_B$ be two isometries. For every $(x, y, a, b) \in X \times Y \times A \times B$, let

$$\delta_{x,a}^A := \|I_A^*(\widetilde{M}_a^x \otimes \mathbb{1}_{\mathcal{K}_A})I_A - M_a^x\|_{\rho_A} \text{ and } \delta_{y,b}^B := \|I_B^*(\widetilde{N}_b^y \otimes \mathbb{1}_{\mathcal{K}_B})I_B - N_b^y\|_{\rho_B}$$

where $\rho_A := \mathrm{Tr}_{\mathcal{H}_B}\big(|\psi\rangle\langle\psi|\big), \rho_B := \mathrm{Tr}_{\mathcal{H}_A}\big(|\psi\rangle\langle\psi|\big)$, and let

$$\delta := \sum_{x,y,a,b} \mu(x,y)V(a,b|x,y)\left(\delta_{x,a}^A + \delta_{y,b}^B\right).$$

Then there exists a unit vector $|aux\rangle \in \mathcal{K}_A \otimes \mathcal{K}_B$ such that

$$\|I_A \otimes I_B\,|\psi\rangle - |\widetilde{\psi}\rangle \otimes |aux\rangle\| \leqslant \frac{\sqrt{2}\big(\delta + \sqrt{\epsilon}\big)}{\Delta}. \tag{4.2.3}$$

Moreover, for every $(x, y, a, b) \in X \times Y \times A \times B$,

$$\|I_A \otimes I_B\big(M_a^x \otimes N_b^y\,|\psi\rangle\big) - \big(\widetilde{M}_a^x \otimes \widetilde{N}_b^y\,|\widetilde{\psi}\rangle\big) \otimes |aux\rangle\| \leqslant \delta_{x,a}^A + \delta_{y,b}^B + \frac{\sqrt{2}\big(\delta + \sqrt{\epsilon}\big)}{\Delta}. \tag{4.2.4}$$

Proof. Let $\pi := \pi_A \otimes \pi_B$ be the associated representation of S, let $I = I_A \otimes I_B$, and let $\mathcal{K} := \mathcal{K}_A \otimes \mathcal{K}_B$. By Lemma 4.1.12,

$$\begin{aligned}
&\|\Big(I^*\big(\widetilde{\pi}(m_a^x \otimes n_b^y) \otimes \mathbb{1}_{\mathcal{K}}\big)I - \pi(m_a^x \otimes n_b^y)\Big)\,|\psi\rangle\| \\
&\qquad \leqslant \|I_A^*\big(\widetilde{\pi}_A(m_a^x) \otimes \mathbb{1}_{\mathcal{K}_A}\big)I_A - \pi_A(m_a^x)\|_{\rho_A} + \|I_B^*\big(\widetilde{\pi}_B(n_b^y) \otimes \mathbb{1}_{\mathcal{K}_B}\big)I_B - \pi_B(n_b^y)\|_{\rho_B} \\
&\qquad = \delta_{x,a}^A + \delta_{y,b}^B.
\end{aligned}$$

This implies

$$\|\Big(I^*\big(\widetilde{\pi}(\Phi_{\mathcal{G}})\otimes \mathbb{1}_{\mathcal{K}}\big)I-\pi(\Phi_{\mathcal{G}})\Big)\,|\psi\rangle\| \leqslant \sum_{x,y,a,b}\mu(x,y)V(a,b|x,y)\left(\delta^A_{x,a}+\delta^B_{y,b}\right)=\delta.$$

Since S is an ϵ-optimal strategy for $\mathcal{G}$, by Lemma 4.2.1, $w_q(\mathcal{G})\mathbb{1}-\pi(\Phi_{\mathcal{G}})$ is a positive operator such that $\|w_q(\mathcal{G})\mathbb{1}-\pi(\Phi_{\mathcal{G}})\|_{op}\leqslant 1$ and $\langle\psi|\left(w_q(\mathcal{G})\mathbb{1}-\pi(\Phi_{\mathcal{G}})\right)|\psi\rangle\leqslant\epsilon$. So

$$\begin{aligned}\|\left(w_q(\mathcal{G})\mathbb{1}-\pi(\Phi_{\mathcal{G}})\right)|\psi\rangle\| &\leqslant \|\left(w_q(\mathcal{G})\mathbb{1}-\pi(\Phi_{\mathcal{G}})\right)^{1/2}\|_{op}\cdot\|\left(w_q(\mathcal{G})\mathbb{1}-\pi(\Phi_{\mathcal{G}})\right)^{1/2}|\psi\rangle\|\\ &\leqslant\sqrt{\langle\psi|\left(w_q(\mathcal{G})\mathbb{1}-\pi(\Phi_{\mathcal{G}})\right)|\psi\rangle}\leqslant\sqrt{\epsilon}.\end{aligned}$$

Let $\widetilde{\Phi}:=w_q(\mathcal{G})\mathbb{1}-\widetilde{\pi}(\Phi_{\mathcal{G}})$. It follows that

$$\|I^*(\widetilde{\Phi}\otimes\mathbb{1})I\,|\psi\rangle\|\leqslant\|\Big(I^*\big(\widetilde{\pi}(\Phi_{\mathcal{G}})\otimes\mathbb{1}\big)I-\pi(\Phi_{\mathcal{G}})\Big)\,|\psi\rangle\|+\|\left(w_q(\mathcal{G})\mathbb{1}-\pi(\Phi_{\mathcal{G}})\right)|\psi\rangle\|\leqslant\delta+\sqrt{\epsilon}.$$

Now we fix orthonormal bases $\{|\alpha_i\rangle\}_i$ and $\{|\beta_j\rangle\}_j$ for $\mathcal{K}_A$ and $\mathcal{K}_B$ respectively. We can write $I\,|\psi\rangle=\sum_{i,j}\lambda_{ij}\,|\psi_{ij}\rangle\otimes|\alpha_i,\beta_j\rangle$ for some unit vectors $|\psi_{ij}\rangle\in\widetilde{\mathcal{H}}_A\otimes\widetilde{\mathcal{H}}_B$ and some $\lambda_{ij}\in\mathbb{C}$ where $\sum_{ij}|\lambda_{ij}|^2=1$. By absorbing phase of $|\psi_{ij}\rangle$ into λ_{ij}, we may assume without loss of generality that every $\delta_{ij}:=\langle\psi_{ij}|\widetilde{\psi}\rangle\geqslant 0$. So we can write $|\psi_{ij}\rangle=\delta_{ij}\,|\widetilde{\psi}\rangle+\sqrt{1-\delta_{ij}^2}\,|\kappa_{ij}\rangle$ for some unit vector $|\kappa_{ij}\rangle\in\widetilde{\mathcal{H}}_A\otimes\widetilde{\mathcal{H}}_B$ that is orthogonal to $|\widetilde{\psi}\rangle$. Theorem 4.2.9 implies $\|\widetilde{\Phi}\,|\widetilde{\psi}\rangle\|=0$ and $\|\widetilde{\Phi}\,|\kappa_{ij}\rangle\|\geqslant\Delta$ for all i,j. Hence

$$\begin{aligned}(\delta+\sqrt{\epsilon})^2\geqslant\|I^*(\widetilde{\Phi}\otimes\mathbb{1})I\,|\psi\rangle\|^2&=\sum_{i,j}|\lambda_{ij}|^2\|\widetilde{\Phi}\,|\psi_{ij}\rangle\|^2\\ &=\sum_{i,j}|\lambda_{ij}|^2(1-\delta_{ij}^2)\|\widetilde{\Phi}\,|\kappa_{ij}\rangle\|^2\geqslant\Delta^2\sum_{i,j}|\lambda_{ij}|^2(1-\delta_{ij}^2)\\ &\geqslant\Delta^2\sum_{i,j}|\lambda_{ij}|^2(1-\delta_{ij})=\Delta^2\left(1-\sum_{i,j}|\lambda_{ij}|^2\delta_{ij}\right).\end{aligned}$$

The last inequality uses the fact that $\delta_{ij}\leqslant 1$ for all i,j. Let $|\kappa\rangle:=\sum_{i,j}\lambda\,|\alpha_i,\beta_j\rangle$. Then

$$\|I\,|\psi\rangle-|\widetilde{\psi}\rangle\otimes|\kappa\rangle\|^2=2\left(1-\sum_{i,j}|\lambda_{ij}|^2\delta_{ij}\right)\leqslant\frac{2(\delta+\sqrt{\epsilon})^2}{\Delta^2}$$

So Equation (4.2.3) follows. For any $(x,y,a,b)\in X\times Y\times A\times B$, observe that

$$I\big(M_a^x\otimes N_b^y\,|\psi\rangle\big)-\big(\widetilde{M}_a^x\otimes\widetilde{N}_b^y\,|\widetilde{\psi}\rangle\big)\otimes|aux\rangle=\big(I_AM_a^x-(\widetilde{M}_a^x\otimes\mathbb{1}_{\mathcal{K}_A})I_A\big)\otimes I_BN_b^y\,|\psi\rangle$$

$$+ (\widetilde{M}_A^x \otimes \mathbb{1}_{\mathcal{K}_A}) \otimes \big(I_B N_b^y - (\widetilde{N_b^y} \otimes \mathbb{1}_{\mathcal{K}_B}) I_B\big) |\psi\rangle$$
$$+ \widetilde{M}_a^x \otimes \widetilde{N}_b^y \otimes \mathbb{1}\big(I |\psi\rangle - |\widetilde{\psi}\rangle \otimes |aux\rangle\big).$$

Since $I_B N_b^y$, $\widetilde{M}_a^x$, and $\widetilde{M}_a^x \otimes \widetilde{N}_b^y$ all have operator norms $\leqslant 1$, we conclude that

$$\begin{aligned}\|I\big(M_a^x \otimes N_b^y |\psi\rangle\big) - \big(\widetilde{M}_a^x \otimes \widetilde{N}_b^y |\widetilde{\psi}\rangle\big) \otimes |aux\rangle\| \leqslant{}& \|I_A^*(\widetilde{M}_a^x \otimes \mathbb{1}_{\mathcal{K}_A}) I_A - M_a^x\|_{\rho_A} \\ &+ \|I_B^*(\widetilde{N}_b^y \otimes \mathbb{1}_{\mathcal{K}_B}) I_B - N_b^y\|_{\rho_B} \\ &+ \|I |\psi\rangle - |\widetilde{\psi}\rangle \otimes |aux\rangle\|.\end{aligned}$$

So Equation (4.2.4) follows. □

Remark 4.2.14. *We remark that Theorem 4.2.9 and Proposition 4.2.13 also hold if all $\mathcal{A}_{POVM}$ are replaced by $\mathcal{A}_{PVM}$ and "optimal quantum strategies" is replaced by "projective optimal strategies". The proofs follow similarly.*

4.3 A tracial-state characterization of self-testing

4.3.1 Tracial states

In this subsection, we discuss some properties of tracial states that will be used later. Recall that, in this thesis, all C^*-algebras are assumed to be unital and separable. A tracial state τ on a C^*-algebra $\mathcal{A}$ is a state satisfying $\tau(ab) = \tau(ba)$ for all $a, b \in \mathcal{A}$. We denote by $T(\mathcal{A})$ the set of tracial states on $\mathcal{A}$. It is a convex set and is compact and closed in the weak*-topology. We use $\partial_e T(\mathcal{A})$ to denote the extreme points in $T(\mathcal{A})$. We say a tracial state τ on $\mathcal{A}$ *factors through* another C^*-algebra $\mathcal{B}$ if there are some $*$-homomorphism $\varphi : \mathcal{A} \to \mathcal{B}$ and some tracial state $\widetilde{\tau}$ on $\mathcal{B}$ such that $\tau = \widetilde{\tau} \circ \varphi$. If in addition, φ is surjective, we say τ *factors surjectively through* $\mathcal{B}$.

For any $\tau \in T(\mathcal{A})$, the *kernel* of τ, defined by

$$\mathcal{I}_\tau := \{a \in \mathcal{A} : \tau(a^* a) = 0\}, \tag{4.3.1}$$

is a two-sided closed ideal. So $\langle a + \mathcal{I}_\tau, b + \mathcal{I}_\tau \rangle := \tau(a^* b), a, b \in \mathcal{A}$ defines an inner product on $\mathcal{A}/\mathcal{I}_\tau$. Completing $\mathcal{A}/\mathcal{I}_\tau$ with respect to this inner product gives the Hilbert space $L^2(\mathcal{A}, \tau)$. For any $a \in \mathcal{A}$, we use $\widehat{a}$ to denote the canonical image of a in $L^2(\mathcal{A}, \tau)$. Let $\pi_\tau : \mathcal{A} \to \mathcal{B}(L^2(\mathcal{A}, \tau))$ be the $*$-representation of $\mathcal{A}$ given by

$$\pi_\tau(a)\widehat{b} := \widehat{ab} \text{ for all } a, b \in \mathcal{A},$$

and let $|\tau\rangle := \widehat{1}$. Then the triple $\big(L^2(\mathcal{A}, \tau), \pi_\tau, |\tau\rangle\big)$ is a GNS representation for τ. We refer to π_τ as the *left regular representatin* of τ, and refer to $\big(L^2(\mathcal{A}, \tau), \pi_\tau, |\tau\rangle\big)$ as the *standard GNS* for τ. One can also define the *right regular representation* π_τ^{op}, which is the $*$-representation from $\mathcal{A}^{\mathrm{op}} \to \mathcal{B}(L^2(\mathcal{A}, \tau))$ given by

$$\pi_\tau^{\mathrm{op}}(a^{\mathrm{op}})\widehat{b} := \widehat{ba} \text{ for all } a, b \in \mathcal{A}.$$

Here $\mathcal{A}^{\mathrm{op}}$ denotes the *opposite algebra* of $\mathcal{A}$. That is, $\mathcal{A}^{\mathrm{op}} = \mathcal{A}$ as a Banach space, but the multiplication on $\mathcal{A}^{\mathrm{op}}$ is reversed: if we use a^{op} to denote any $a \in \mathcal{A}$ in $\mathcal{A}^{\mathrm{op}}$, then $a^{\mathrm{op}} \cdot b^{\mathrm{op}} = (ba)^{\mathrm{op}}$. It is clear that $\pi_\tau(\mathcal{A})' \subset \pi_\tau^{\mathrm{op}}(\mathcal{A}^{op})$. So the left and right regular representations commute.

The following characterization of extreme tracial states is well-known (see e.g., [Dix82, Theorem 6.7.3])

Lemma 4.3.1. *Suppose τ is a tracial state on a C^*-algebra $\mathcal{A}$. Then τ is an extreme point in $T(\mathcal{A})$ if and only if the enveloping von Neumann algebra $\pi_\tau(\mathcal{A})''$ is a factor.*

Note that in the "if" direction of the above lemma, the hypothesis that $\pi_\tau(\mathcal{A})''$ is a factor does not necessarily mean π_τ is irreducible. In fact, if an extreme tracial state τ has an irreducible GNS representation π_τ, then π_τ must be a one-dimensional representation. In other words, for any $\tau \in \partial_e T(\mathcal{A})$, τ is a pure state if and only if τ is a character.

Finite-dimensional tracial states

When working with quantum correlations, we are particularly interested in finite-dimensional tracial states and their convex structure. A tracial state is said to be finite-dimensional if

its GNS representation is finite-dimensional. The set of finite-dimensional tracial states on $\mathcal{A}$ is denoted by $T_{\text{fin}}(\mathcal{A})$. The following characterization of finite-dimensional tracial states is well-known (see e.g., [MR19]).

Lemma 4.3.2. *A tracial state τ on a C^*-algebra $\mathcal{A}$ is finite-dimensional if and only if one of the following equivalent statements holds.*

(a) $\mathcal{A}/\mathcal{I}_\tau$ is finite-dimensional.

(b) τ factors through a finite-dimensional C^*-algebras.

(c) $\pi_\tau(\mathcal{A})''$ is finite-dimensional.

(d) The linear functional $\phi : \mathcal{A}^{\text{op}} \otimes \mathcal{A} \to \mathbb{C}$ defined by $\phi(a^{\text{op}} \otimes b) = \tau(ab), a, b \in \mathcal{A}$ is a finite-dimensional state.

Later in Proposition 4.3.6 we'll show that $T_{\text{fin}}(\mathcal{A})$ is a convex face of $T(\mathcal{A})$. We first need to establish the following lemmas.

Lemma 4.3.3. *For any C^*-algebra $\mathcal{A}$, the set $T_{\text{fin}}(\mathcal{A})$ is convex.*

Proof. Let τ_1 and τ_2 be two finite-dimensional tracial states on a C^*-algebra $\mathcal{A}$. Then there are finite-dimensional C^*-algebras $\mathcal{B}_1$ and $\mathcal{B}_2$, $*$-homomorphisms $\varphi_1 : \mathcal{A} \to \mathcal{B}_1$ and $\varphi_2 : \mathcal{A} \to \mathcal{B}_2$, and tracial states $\widetilde{\tau_1}$ and $\widetilde{\tau_2}$ on $\mathcal{B}_1$ and $\mathcal{B}_2$ respectively such that $\tau_1 = \widetilde{\tau_1} \circ \varphi_1$ and $\tau_2 = \widetilde{\tau_1} \circ \varphi_2$. For any $0 < \lambda < 1$, let $\widetilde{\tau}$ be the tracial state on $\mathcal{B}_1 \oplus \mathcal{B}_2$ defined by

$$\widetilde{\tau}(\beta_1, \beta_2) = \lambda\widetilde{\tau_1}(\beta_1) + (1-\lambda)\widetilde{\tau_2}(\beta_2)$$

for all $(\beta_1, \beta_2) \in \mathcal{B}_1 \oplus \mathcal{B}_2$. Then $\lambda\tau_1 + (1-\lambda)\tau_2 = \widetilde{\tau} \circ \varphi$ where $\varphi := \lambda\varphi_1 \oplus (1-\lambda)\varphi_2$ is a $*$-homomorphism from $\mathcal{A} \to \mathcal{B}_1 \oplus \mathcal{B}_2$. This means the tracial state $\lambda\tau_1 + (1-\lambda)\tau_2$ factors through the finite-dimensional C^*-algebra $\mathcal{B}_1 \oplus \mathcal{B}_2$, so $\lambda\tau_1 + (1-\lambda)\tau_2 \in T_{\text{fin}}(\mathcal{A})$. Since τ_1, τ_2, and λ were arbitrary, we conclude that $T_{\text{fin}}(\mathcal{A})$ is a convex set. □

We use $\partial_e T_{\text{fin}}(\mathcal{A})$ to denote the extreme points in $T_{\text{fin}}(\mathcal{A})$.

Lemma 4.3.4. *Let τ be a finite-dimensional tracial state on a C^*-algebra $\mathcal{A}$. Suppose $\tau = \lambda\tau_1 + (1-\lambda)\tau_2$ for some $\tau_1, \tau_2 \in T(\mathcal{A})$ and $0 < \lambda < 1$. Then τ_1 and τ_2 must be finite-dimensional.*

Proof. Since $\tau \in T_{\text{fin}}(\mathcal{A})$, the algebra $\mathcal{A}/\mathcal{I}_\tau$ is finite-dimensional. Observe that for any $a \in \mathcal{A}$, $\tau(a^*a) = 0$ if and only if $\tau_1(a^*a) = \tau_2(a^*a) = 0$. This means $\mathcal{I}_\tau = \mathcal{I}_{\tau_1} \cap \mathcal{I}_{\tau_2}$. Hence $\mathcal{A}/\mathcal{I}_{\tau_1}$ and $\mathcal{A}/\mathcal{I}_{\tau_2}$ are both C^*-subalgebras of $\mathcal{A}/\mathcal{I}_\tau$, so they are finite-dimensional. It follows that $\tau_1, \tau_2 \in T_{\text{fin}}(\mathcal{A})$. □

Lemma 4.3.5. *Let $\mathcal{A}$ be a C^*-algebra. Then $T_{\text{fin}}(\mathcal{A})$ is the convex hull of tracial states on $\mathcal{A}$ that factor surjectively through full matrix algebras.*

Proof. Any $\tau \in T_{\text{fin}}(\mathcal{A})$ drops to a tracial state $\widetilde{\tau}$ on $\mathcal{A}/\mathcal{I}_\tau$ so that $\tau = \widetilde{\tau} \circ q$, where $q : \mathcal{A} \to \mathcal{A}/\mathcal{I}_\tau$ is the quotient map. Since $\mathcal{A}/\mathcal{I}_\tau$ is finite-dimensional, we can write

$$\mathcal{A}/\mathcal{I}_\tau = \mathsf{M}_{d_1} \oplus \cdots \oplus \mathsf{M}_{d_k}$$

for some $d_1, \ldots, d_k \geqslant 1$. For every $1 \leqslant i \leqslant k$, let $\Pi_i : \mathcal{A}/\mathcal{I}_\tau \to \mathsf{M}_{d_i}$ be the canonical projection. Then every $\varphi_i := \Pi_i \circ q$ is a surjective $*$-homomorphism from $\mathcal{A} \to \mathsf{M}_{d_i}$, and hence every $\tau_i := \operatorname{tr}_{d_i} \circ \varphi_i$ is a tracial state on $\mathcal{A}$ that factors surjectively through the matrix algebra M_{d_i}. Since each $\widetilde{\tau}|_{\mathsf{M}_{d_i}}$ is a tracial linear functional on M_{d_i}, we must have $\widetilde{\tau}|_{\mathsf{M}_{d_i}} = \lambda_i \operatorname{tr}_{d_i}$ where $\lambda_i = \widetilde{\tau}(\mathbb{1}_{d_i})$. This implies $\tau = \lambda_1\tau_1 + \cdots \lambda_k\tau_k$. We conclude that every $\tau \in T_{\text{fin}}(\mathcal{A})$ is a convex combination of tracial states that factor surjectively through full matrix algebras. □

The following proposition states that $T_{\text{fin}}(\mathcal{A})$ is a convex face of $T(\mathcal{A})$ and $\partial_e T_{\text{fin}}(\mathcal{A})$ consists of tracial states that factor surjectively through *full matrix algebras*.

Proposition 4.3.6. *Suppose $\mathcal{A}$ is a C^*-algebra such that $T_{\text{fin}}(\mathcal{A})$ is non-empty.*

(a) $\partial_e T_{\text{fin}}(\mathcal{A}) = \partial_e T(\mathcal{A}) \cap T_{\text{fin}}(\mathcal{A})$.

(b) A tracial state τ is in $\partial_e T_{\text{fin}}(\mathcal{A})$ if and only if it factors surjectively through a full matrix algebra, and

(c) $T_{\text{fin}}(\mathcal{A}) = conv\big(\partial_e T_{\text{fin}}(\mathcal{A})\big)$.

Proof. For part (a), it is clear that $\partial_e T(\mathcal{A}) \cap T_{\text{fin}}(\mathcal{A}) \subseteq \partial_e T_{\text{fin}}(\mathcal{A})$, so it only left to show the inverse inclusion. Now assume that there is a $\tau \in \partial_e T_{\text{fin}}(\mathcal{A})$ which is not in $\partial_e T(\mathcal{A})$. Then there are distinct $\tau_1, \tau_2 \in T(\mathcal{A})$ and $0 < \lambda < 1$ such that $\tau = \lambda\tau_1 + (1-\lambda)\tau_2$. By Lemma 4.3.4, τ_1 and τ_2 are finite-dimensional. This implies τ is not an extreme point of $T_{\text{fin}}(\mathcal{A})$, a contradiction. Hence $\partial_e T_{\text{fin}}(\mathcal{A}) \subseteq \partial_e T(\mathcal{A})$. We conclude that $\partial_e T_{\text{fin}}(\mathcal{A}) = \partial_e T(\mathcal{A}) \cap T_{\text{fin}}(\mathcal{A})$.

For part (b), let $\tau \in T_{\text{fin}}(\mathcal{A})$. Then τ has a convex combination $\lambda_1\tau_1 + \cdots \lambda_k\tau_k$ where every τ_i factors surjectively through a full matrix algebra, as shown in Lemma 4.3.5. For the "only if" direction, suppose τ is in $\partial_e T_{\text{fin}}(\mathcal{A})$. Then we must have $\tau_1 = \cdots = \tau_k$, and hence τ factors surjectively through a full matrix algebra. For the "if" direction, suppose τ factors surjectively through a full matrix algebra. Let $\big(L^2(\mathcal{A},\tau), \pi_\tau, |\tau\rangle\big)$ be the standard GNS of τ. Then $\tau = \text{tr}_d \circ \varphi$ for some surjective $*$-homomorphism $\varphi : \mathcal{A} \to \mathsf{M}_d$, and hence

$$\mathcal{I}_\tau = \{a \in A : \text{tr}_d\left(\varphi(a^*a)\right) = 0\} = \{a \in \mathcal{A} : \varphi(a) = 0\} = \ker(\varphi).$$

This implies $\pi_\tau(\mathcal{A}) \cong \mathcal{A}/\mathcal{I}_\tau = \mathcal{A}/\ker(\varphi) \cong \mathsf{M}_d$ is a full matrix algebra. So $\pi_\tau(\mathcal{A})''$ is a factor, and hence $\tau \in \partial_e T(\mathcal{A})$. Then by part (a), $\tau \in \partial_e T_{\text{fin}}(\mathcal{A})$. We conclude that a tracial state τ is in $\partial_e T_{\text{fin}}(\mathcal{A})$ if and only if τ factors surjectively through a full matrix algebra.

Part (c) follows straightforward from part (b) and Lemma 4.3.5. □

From the proofs of Proposition 4.3.6 and Lemma 4.3.5, we immediately see that:

Corollary 4.3.7. *Let $\mathcal{A}$ be a C^*-algebra. A tracial state τ on $\mathcal{A}$ is in $\partial_e T_{\text{fin}}(\mathcal{A})$ if and only if $\mathcal{A}/\mathcal{I}_\tau$ is a full matrix algebra.*

We now study the GNS construction of states in $\partial_e T_{\text{fin}}(\mathcal{A})$. Given a $\tau \in \partial_e T_{\text{fin}}(\mathcal{A})$, let $\big(L^2(\mathcal{A},\tau), \pi_\tau, |\tau\rangle\big)$ be the standard GNS for τ. Since $L^2(\mathcal{A},\tau)$ is finite-dimensional, $\mathcal{A}/\mathcal{I}_\tau = L^2(\mathcal{A},\tau)$ as a Hilbert space. Let $q : \mathcal{A} \to \mathcal{A}/\mathcal{I}_\tau$ be the quotient map. Then τ drops to a tracial state $\widetilde{\tau}$ on $L^2(\mathcal{A},\tau)$ so that $\tau = \widetilde{\tau} \circ q$. By Corollary 4.3.7, we can identify

$L^2(\mathcal{A},\tau)$ with[2] M_d for some $d \geqslant 1$. Under this identification, $\widetilde{\tau} = \mathrm{tr}_d$ and $|\tau\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d e_{ii}$, where $\{e_{ij} : 1 \leqslant i,j \leqslant d\}$ is the standard basis for M_d. While all GNS representations of τ are unitarily equivalent to the standard one, some of them have a more "concrete" form. The following proposition illustrates that any extreme finite-dimensional tracial state has a GNS representation that employs a maximally entangled state.

Proposition 4.3.8. *Let $\mathcal{A}$ be a C^*-algebra. A state τ on $\mathcal{A}$ is an extreme point in $T_{\mathrm{fin}}(\mathcal{A})$ if and only if τ has a GNS representation $\big(\mathbb{C}^d \otimes \mathbb{C}^d, \mathbb{1} \otimes \pi(\cdot), |\varphi_d\rangle\big)$, where $d \geqslant 1$, π is an irreducible $*$-representation of $\mathcal{A}$ on $\mathbb{C}^d$, and $|\varphi_d\rangle := \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle \otimes |i\rangle$.*

Proof. For the "if" direction, observe that π is a surjective $*$-homomorphism from $\mathcal{A} \to M_d(\mathbb{C})$ such that

$$\tau(a) = \langle \varphi_d | \, \mathbb{1} \otimes \pi(a) \, |\varphi_d\rangle = \mathrm{tr}_d\big(\pi(a)\big)$$

for all $a \in \mathcal{A}$. This means τ is a tracial state that factors surjectively through the full matrix algebra $M_d(\mathbb{C}) \cong \mathsf{M}_d$. By part (b) of Proposition 4.3.6, we have $\tau \in \partial_e T_{\mathrm{fin}}(\mathcal{A})$.

Now we prove the "only if" direction. Suppose $\tau \in \partial_e T_{\mathrm{fin}}(\mathcal{A})$. Then the standard GNS of τ has the form $(\mathsf{M}_d, \pi_\tau, |\tau\rangle)$, where $|\tau\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d e_{ii}$ and $\{e_{ij} : 1 \leqslant i,j \leqslant d\}$ is the standard basis for M_d. Let $U : \mathsf{M}_d \to \mathbb{C}^d \otimes \mathbb{C}^d$ be the unitary map sending $e_{ij} \mapsto |j\rangle \otimes |i\rangle$. Then $U|\tau\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle \otimes |i\rangle =: |\varphi_d\rangle$. Let $\Phi : \mathsf{M}_d \to M_d(\mathbb{C})$ be the isomorphism sending $e_{ij} \mapsto |i\rangle\langle j|$ for all $1 \leqslant i,j \leqslant d$. Then $\pi := \Phi \circ \pi_\tau$ is a surjective $*$-homomorphism from $\mathcal{A} \to M_n(\mathbb{C})$, and hence π is an irreducible $*$-representation. For any $a \in \mathcal{A}$, $\pi_\tau(a)$ can be written uniquely as $\sum_{i,j=1}^d a_{ij} e_{ij}$ for some $a_{ij} \in \mathbb{C}$, so

$$\begin{aligned} U\pi_\tau(a)U^* \, |k,\ell\rangle = U \sum_{i,j=1}^d a_{ij} e_{ij} e_{\ell k} = U \sum_{i=1}^d a_{i\ell} e_{ik} = \sum_{i=1}^d a_{i\ell} \, |k,i\rangle = |k\rangle \otimes \Big(\sum_{i=1}^d a_{i\ell} \, |i\rangle \Big) \\ = |k\rangle \otimes \Big(\sum_{i=1}^d a_{i\ell} \, |i\rangle\langle \ell|\ell\rangle \Big) = |k\rangle \otimes \Big(\sum_{i,j=1}^d a_{ij} \, |i\rangle\langle j|\ell\rangle \Big) \\ = |k\rangle \otimes \Big(\Phi\big(\pi_\tau(a)\big) \, |\ell\rangle \Big) = |k\rangle \otimes \big(\pi(a) \, |\ell\rangle \big) \end{aligned}$$

[2] Here we think of M_d as a Hilbert space with inner product $\langle A, B\rangle = \mathrm{tr}_d(A^*B)$

for all $|k,\ell\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$. This implies $U\pi_\tau(a)U^* = \mathbb{1} \otimes \pi(a)$ for all $a \in \mathcal{A}$. It follows that $\big(\mathbb{C}^d \otimes \mathbb{C}^d, \mathbb{1} \otimes \pi(\cdot), |\varphi_d\rangle\big)$ is unitarily equivalent to the standard GNS of τ, and hence itself is a GNS representation of τ. □

The unitary operator U in the proof of Proposition 4.3.8 is known as the transformation of the operator-vector correspondence. From the proof, we see that the left regular representation π_τ satisfies $\pi_\tau(a) = U^*\big(\mathbb{1} \otimes \pi(a)\big)U$ for all $a \in \mathcal{A}$. Consequently, the right regular representation π_τ^{op} is given by $\pi_\tau^{\mathrm{op}}(a) = U^*\big(\pi(a)^T \otimes \mathbb{1}\big)U$.

For every $\tau \in \partial_e T_{\mathrm{fin}}(\mathcal{A})$, the irreducible representation π in the statement of Proposition 4.3.8 is unique up to unitary equivalence. This gives a one-to-one correspondence between extreme finite-dimensional tracial states on $\mathcal{A}$ and finite-dimensional irreducible representations of $\mathcal{A}$.

Corollary 4.3.9. *For any C^*-algebra $\mathcal{A}$, let $\mathrm{Irr}_{\mathrm{fin}}(\mathcal{A})$ be the set of inequivalent finite-dimensional irreducible $*$-representations of $\mathcal{A}$. There is a bijective correspondence between $\mathrm{Irr}_{\mathrm{fin}}(\mathcal{A})$ and $\partial_e T_{\mathrm{fin}}(\mathcal{A})$, sending a representation $\pi \in \mathrm{Irr}_{\mathrm{fin}}(\mathcal{A})$ to the tracial state τ given by $\tau(a) = \mathrm{tr}_d\big(\pi(a)\big), a \in \mathcal{A}$, where d is the dimension of π.*

If a closed two-sided ideal $\mathcal{J}$ is contained in $\mathcal{I}_\tau$ for a tracial state τ on $\mathcal{A}$, then it is clear that τ drops to a tracial state on $\mathcal{A}/\mathcal{J}$. The following lemma asserts that the finite dimensionality of τ will also be preserved.

Proposition 4.3.10. *Let $\mathcal{A}$ be a C^*-algebra. Suppose $\mathcal{J}$ is a closed two-sided ideal of $\mathcal{A}$, and let $q : \mathcal{A} \to \mathcal{A}/\mathcal{J}$ be the quotient map. There is a bijective correspondence between tracial states on $\mathcal{A}/\mathcal{J}$ and tracial states on $\mathcal{A}$ whose kernel contains $\mathcal{J}$, sending a $\tau \in T(\mathcal{A}/\mathcal{J})$ to the tracial state $\widetilde{\tau} := \tau \circ q$. Moreover, $\tau \in T(\mathcal{A}/\mathcal{J})$ is finite-dimensional if and only if the corresponding $\widetilde{\tau}$ is finite-dimensional.*

Proof. Observe that $L^2(\mathcal{A}, \widetilde{\tau}) \cong L^2(\mathcal{A}/\mathcal{J}, \tau)$. So the lemma follows. □

Amenable tracial states

In the study of robust self-testing, we need to work with weak*-limit of finite-dimensional tracial states. This leads to the study of amenable tracial states.

Definition 4.3.11. *Let $\mathcal{A}$ be a C^*-algebra, and fix a faithful representation $\mathcal{A} \subset \mathcal{B}(\mathcal{H})$. We say a state τ on $\mathcal{A}$ is an **amenable tracial state** if there is a state ϕ on $\mathcal{B}(\mathcal{H})$ such that $\phi|_{\mathcal{A}} = \tau$ and $\phi(uTu^*) = \phi(T)$ for any $T \in \mathcal{B}(\mathcal{H})$ and unitary $u \in \mathcal{A}$.*

Note that $\phi|_{\mathcal{A}}$ is indeed a tracial state. This is because $\phi(uv) = \phi\big(u(vu)u^*\big) = \phi(vu)$ for all unitaries $u, v \in \mathcal{A}$ and unitaries in $\mathcal{A}$ span the entire $\mathcal{A}$. Another subtle point in this definition is that the amenability of τ is independent of the choice of embedding $\mathcal{A} \subset \mathcal{B}(\mathcal{H})$ (see [BO08, Proposition 6.2.2] for a proof).

The following characterization of amenable tracial states is from [BO08, Theorem 6.2.7].

Lemma 4.3.12. *A tracial state τ on a C^*-algebra $\mathcal{A}$ is amenable if and only if one of the following equivalent conditions holds.*

(a) There exists a sequence of ucp maps $\varphi_n : \mathcal{A} \to \mathsf{M}_{d_n}, n \in \mathbb{N}$ such that $\tau(a) = \lim_{n\to\infty} \mathrm{tr}_{d_n}\big(\varphi_n(a)\big)$ and $\lim_{n\to\infty} \|\varphi_n(ab) - \varphi_n(a)\varphi_n(b)\|_{hs} = 0$ for all $a, b \in \mathcal{A}$.

(b) The linear functional $\phi : \mathcal{A}^{\mathrm{op}} \otimes \mathcal{A} \to \mathbb{C}$ defined by $\phi(a^{\mathrm{op}} \otimes b) := \tau(ab), a, b \in \mathcal{A}$ is a min-continuous state.

(c) The $*$-homomorphism $\pi : \mathcal{A}^{\mathrm{op}} \otimes \mathcal{A} \to \mathcal{B}(L^2(\mathcal{A}, \tau))$ defined by $\pi(a^{\mathrm{op}} \otimes b) = \pi_\tau^{\mathrm{op}}(a^{\mathrm{op}})\pi_\tau(b)$, $a, b \in \mathcal{A}$ is min-continuous.

(d) For any faithful representation $\mathcal{A} \subset \mathcal{B}(\mathcal{H})$ there is a ucp map $\Phi : \mathcal{A}(\mathcal{H}) \to \pi_\tau(\mathcal{A})''$ such that $\Phi(a) = \pi_\tau(a)$ for all $a \in \mathcal{A}$.

For any two-sided ideal $\mathcal{J}$ of $\mathcal{A}$, in Proposition 4.3.10, we have seen the correspondence between tracial states on $\mathcal{A}/\mathcal{J}$ and tracial states on $\mathcal{A}$ whose kernel contains $\mathcal{J}$.

The following proposition asserts that amenability is preserved in one direction of this correspondence.

Proposition 4.3.13. *Let $\mathcal{A}$ be a C^*-algebra. Suppose $\mathcal{J}$ is a closed two-sided ideal of $\mathcal{A}$, and let $q : \mathcal{A} \to \mathcal{A}/\mathcal{J}$ be the quotient map. If a tracial state τ on $\mathcal{A}/\mathcal{J}$ is amenable, then the tracial state $\widetilde{\tau} := \tau \circ q$ on $\mathcal{A}$ is amenable.*

Proof. Suppose τ is an amenable tracial state on $\mathcal{A}/\mathcal{J}$, and let $\widetilde{\tau} := \tau \circ q$. Then there is a sequence of ucp maps $\varphi_n : \mathcal{A}/\mathcal{J} \to \mathsf{M}_{d_n}, n \in \mathbb{N}$ such that $\tau(a) = \lim_{n\to\infty} \mathrm{tr}_{d_n}\left(\varphi_n(a)\right)$ and $\lim_{n\to\infty} \|\varphi_n(ab) - \varphi_n(a)\varphi_n(b)\|_{hs} = 0$ for all $a, b \in \mathcal{A}/\mathcal{J}$. It follows that $\widetilde{\varphi}_n := \varphi_n \circ q : \mathcal{A} \to \mathsf{M}_{d_n}, n \in \mathbb{N}$ is a sequence of ucp maps such that $\lim_{n\to\infty} \mathrm{tr}_{d_n}\left(\widetilde{\varphi}_n(a)\right) = \tau(q(a)) = \widetilde{\tau}(a)$ and $\lim_{n\to\infty} \|\widetilde{\varphi}_n(ab) - \widetilde{\varphi}_n(a)\widetilde{\varphi}_n(b)\|_{hs} = 0$ for all $a, b \in \mathcal{A}$. So $\widetilde{\tau}$ is amenable. □

Remark 4.3.14. *Unlike Proposition 4.3.10, the converse of Proposition 4.3.13 may not hold in general: there are examples where an amenable tracial state $\widetilde{\tau}$ on $\mathcal{A}$ drops to a non-amenable tracial state τ on $\mathcal{A}/\mathcal{J}$. However, as shown in [BO08, Proposition 6.3.5], if $0 \to \mathcal{J} \to \mathcal{A} \to \mathcal{A}/\mathcal{J} \to 0$ is a locally split extension, then any amenable tracial state on $\mathcal{A}$ whose kernel contains $\mathcal{J}$ always drops to an amenable tracial state on $\mathcal{A}/\mathcal{J}$.*

4.3.2 General results

Definition 4.3.15. *Let $\gamma := \{\gamma_a^x : x \in X, a \in A\}$ be a set of self-adjoint $*$-polynomials in $\mathcal{A}_{PVM}^{Y,B}$, and let $\mathcal{R}$ be a set of $*$-polynomials in $\mathcal{A}_{PVM}^{Y,B}$. We say $(\gamma, \mathcal{R})$ is a determining pair for a nonlocal game $\mathcal{G} = (X, Y, A, B, \mu, V)$ if the following conditions hold.*

(i) For every $x \in X$, $\{q(\gamma_a^x)\}_{a\in A}$ is a PVM in the quotient $C^*(\mathcal{G}) := \mathcal{A}_{PVM}^{Y,B}/\langle\mathcal{R}\rangle$, where $\langle\mathcal{R}\rangle$ is the closed two-sided ideal generated by $\mathcal{R}$ and $q : \mathcal{A}_{PVM}^{Y,B} \to C^*(\mathcal{G})$ is the quotient map.

(ii) A state f on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$ is optimal for $\mathcal{G}$ if and only if

(a) $f\left((m_a^x \otimes 1 - 1 \otimes \gamma_a^x)^2\right) = 0$ for all $x \in X, a \in A$, and

(b) the linear functional $\tau := f|_{1\otimes\mathcal{A}_{PVM}^{Y,B}}$ *is a tracial state on* $\mathcal{A}_{PVM}^{Y,B}$ *that satisfies* $\tau(r^*r) = 0$ *for all* $r \in \mathcal{R}$.

Given a nonlocal game $\mathcal{G}$ with a determining pair $(\gamma, \mathcal{R})$, we refer to the C^*-algebra $C^*(\mathcal{G})$ defined in condition (i) of Definition 4.3.15 as the *associated game algebra* of $\mathcal{G}$. $\{q(\gamma_a^x) : a \in A\}$ is a PVM in $C^*(\mathcal{G})$ means that $q(\sum_{a\in A}\gamma_a^x) = 1$, $q\big((\gamma_a^x)^*\big) = q(\gamma_a^x) = q\big((\gamma_a^x)^2\big)$, and $q\big(\gamma_a^x\gamma_{a'}^x\big) = 0$ for all $a \neq a'$ in $C^*(\mathcal{G})$. We usually express γ_a^x as a $*$-polynomial over $\{n_b^y : y \in Y, b \in B\}$. Since the quotient map sends each generator n_b^y for $\mathcal{A}_{PVM}^{Y,B}$ to the generator n_b^y for $C^*(\mathcal{G})$, in condition (i), we often just say $\{\gamma_a^x : a \in A\}$ is a PVM in $C^*(\mathcal{G})$.

For any correlation $p \in C_{qc}(A, B, X, Y)$, we use $T^{(p)}(\gamma, \mathcal{R})$ to denote the set of tracial states τ on $\mathcal{A}_{PVM}^{Y,B}$ which satisfies

(1) $\tau(\gamma_a^x n_b^y) = p(a, b|x, y)$ for all x, y, a, b, and

(2) $\tau(r^*r) = 0$ for all $r \in \mathcal{R}$.

We denote by $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ the set of finite-dimensional tracial states in $T^{(p)}(\gamma, \mathcal{R})$. From the hypothesis (1) and (2), it is clear that both $T^{(p)}(\gamma, \mathcal{R})$ and $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ are convex sets. We denote by $\partial_e T^{(p)}(\gamma, \mathcal{R})$ and $\partial_e T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ the extreme points in $T^{(p)}(\gamma, \mathcal{R})$ and $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ respectively. Later, in Lemma 4.3.20, we'll show that $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ is a convex face of $T_{\text{fin}}(\mathcal{A}_{PVM}^{Y,B})$ whenever p is an extreme point in C_q.

In condition (ii) of Definition 4.3.15, although we are working with all states (or equivalently, max-continuous states) on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$, the optimal value of $\mathcal{G}$ still refers to the quantum value $w_q(\mathcal{G})$. Here $\tau = f|_{1\otimes\mathcal{A}_{PVM}^{Y,B}}$ means $\tau(\alpha) = f(1 \otimes \alpha)$ for all $\alpha \in \mathcal{A}_{PVM}^{Y,B}$. Later, in Proposition 4.3.18, we'll show that if f is an optimal state for a nonlocal game with determining pair $(\gamma, \mathcal{R})$, then $\tau = f|_{1\otimes\mathcal{A}_{PVM}^{Y,B}}$ is a tracial state in $T^{(p)}(\gamma, \mathcal{R})$ where p is the correlation achieved by f.

In this section, we present a tracial-state characterization of self-testing for nonlocal games that have determining pairs. For such a nonlocal game $\mathcal{G}$, we show that the self-testing property of $\mathcal{G}$ is witnessed by tracial states on the associated game algebra $C^*(\mathcal{G})$,

and the self-testing property of any extreme optimal quantum correlation p for $\mathcal{G}$ can be characterized by tracial states in $T^{(p)}_{\text{fin}}(\gamma, \mathcal{R})$. We prove these two general results in this subsection. In Section 4.3.3, we show that every synchronous game or XOR game has a determining pair. So their self-testing properties can be characterized by tracial states on the respect game algebras.

General results for correlations

We first prove the following general statement for extreme quantum correlations.

Theorem 4.3.16. *Suppose a nonlocal game $\mathcal{G}$ has a determining pair $(\gamma, \mathcal{R})$. Let $C^*(\mathcal{G})$ be the associated game algebra, and let $q : \mathcal{A}^{Y,B}_{PVM} \to C^*(\mathcal{G})$ be the quotient map. If an extreme quantum correlation p is optimal for $\mathcal{G}$, then the following statements are equivalent.*

(a) p is a self-test for all quantum models.

(b) p is an abstract state self-test for finite-dimensional states on $\mathcal{A}^{X,A}_{PVM} \otimes_{min} \mathcal{A}^{Y,B}_{PVM}$.

(c) There is a unique tracial state in $T^{(p)}_{\text{fin}}(\gamma, \mathcal{R})$.

(d) There is a unique finite-dimensional irreducible $*$-representation $\pi : \mathcal{A}^{Y,B}_{PVM} \to M_d(\mathbb{C})$ such that the linear functional $\tau : \mathcal{A}^{Y,B}_{PVM} \to \mathbb{C}$ defined by

$$\tau(\alpha) := \text{tr}_d\left(\pi(\alpha)\right), \alpha \in \mathcal{A}^{Y,B}_{PVM} \tag{4.3.2}$$

is a tracial state in $T^{(p)}_{\text{fin}}(\gamma, \mathcal{R})$.

The proof is established on a sequence of technical lemmas that characterize the nonlocal games that have determining pairs.

Lemma 4.3.17. *Suppose a nonlocal game $\mathcal{G} = (X, Y, A, B, \mu, V)$ has a determining pair $(\gamma, \mathcal{R})$. If a tracial state τ on $\mathcal{A}^{Y,B}_{PVM}$ satisfies $\tau(r^*r) = 0$ for all $r \in \mathcal{R}$, then τ extends uniquely to a state f on $\mathcal{A}^{X,A}_{PVM} \otimes \mathcal{A}^{Y,B}_{PVM}$ which is optimal for $\mathcal{G}$ and satisfies*

$$f(m^{x_1}_{a_1} \cdots m^{x_k}_{a_k} \otimes n^{y_1}_{b_1} \cdots n^{y_\ell}_{b_\ell}) = \tau(\gamma^{x_k}_{a_k} \cdots \gamma^{x_1}_{a_1} n^{y_1}_{b_1} \cdots n^{y_\ell}_{b_\ell}) \tag{4.3.3}$$

for all $k, \ell \in \mathbb{N}$ and $x_1, \ldots, x_k \in X$, $a_1, \ldots, a_k \in A$, $y_1, \ldots, y_\ell \in Y$, $b_1, \ldots, b_\ell \in B$. If in addition, τ is finite-dimensional (resp. amenable), then f is finite-dimensional (resp. min-continuous).

Proof. Suppose τ is a tracial state on $\mathcal{A}_{PVM}^{Y,B}$ such that $\tau(r^*r) = 0$ for all $r \in \mathcal{R}$. Then τ drops to a tracial state $\widetilde{\tau}$ on the quotient $C^*(\mathcal{G})$ such that $\tau = \widetilde{\tau} \circ q$, where $q : \mathcal{A}_{PVM}^{Y,B} \to C^*(\mathcal{G})$ is the quotient map. Let $(\mathcal{H}_{\widetilde{\tau}}, \pi_{\widetilde{\tau}}, |\widetilde{\tau}\rangle)$ be the standard GNS for $\widetilde{\tau}$. Here $\pi_{\widetilde{\tau}}$ is the left regular representation for $\widetilde{\tau}$. Then $\pi_\tau := \pi_{\widetilde{\tau}} \circ q$ is the left regular representation for τ, and $(\mathcal{H}_{\widetilde{\tau}}, \pi_\tau, |\widetilde{\tau}\rangle)$ is the standard GNS for τ.

Note that for every $x \in X$, $\{q(\gamma_a^x) : a \in A\}$ is a PVM in the quotient $C^*(\mathcal{G})$. This means every $\{\pi_{\widetilde{\tau}}^{\mathrm{op}}\big(q(\gamma_a^x)\big) : a \in A\}$ is a PVM on $\mathcal{H}_{\widetilde{\tau}}$. It follows that every $\{\pi_\tau^{\mathrm{op}}(\gamma_a^x) : a \in A\}$ is a PVM on $\mathcal{H}_{\widetilde{\tau}}$. Hence there is a $*$-representation $\pi : \mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B} \to \mathcal{B}(\mathcal{H}_{\widetilde{\tau}})$ sending $m_a^x \otimes 1 \mapsto \pi_\tau^{op}(\gamma_a^x)$ and $1 \otimes n_b^y \mapsto \pi_\tau(n_b^y)$ for all a, b, x, y. Let f be the state on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$ defined by $f(\alpha) := \langle\widetilde{\tau}| \pi(\alpha) |\widetilde{\tau}\rangle, \alpha \in \mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$. Then

$$\begin{aligned} f(m_{a_1}^{x_1} \cdots m_{a_k}^{x_k} \otimes n_{b_1}^{y_1} \cdots n_{b_\ell}^{y_\ell}) &= \langle\widetilde{\tau}| \pi_\tau^{\mathrm{op}}(\gamma_{a_k}^{x_k} \cdots \gamma_{a_1}^{x_1}) \pi_\tau(n_{b_1}^{y_1} \cdots n_{b_\ell}^{y_\ell}) |\widetilde{\tau}\rangle \\ &= \langle\widetilde{\tau}| \pi_\tau(\gamma_{a_k}^{x_k} \cdots \gamma_{a_1}^{x_1} n_{b_1}^{y_1} \cdots n_{b_\ell}^{y_\ell}) |\widetilde{\tau}\rangle \\ &= \tau(\gamma_{a_k}^{x_k} \cdots \gamma_{a_1}^{x_1} n_{b_1}^{y_1} \cdots n_{b_\ell}^{y_\ell}) \end{aligned}$$

for all $k, \ell \in \mathbb{N}$ and $x_1, \ldots, x_k \in X$, $a_1, \ldots, a_k \in A$, $y_1, \ldots, y_\ell \in Y$, $b_1, \ldots, b_\ell \in B$. This proves Equation (4.3.3). Meanwhile,

$$\pi(m_a^x \otimes 1) |\widetilde{\tau}\rangle = \pi_\tau^{\mathrm{op}}(\gamma_a^x) |\widetilde{\tau}\rangle = \pi_\tau(\gamma_a^x) |\widetilde{\tau}\rangle = \pi(1 \otimes \gamma_a^x) |\widetilde{\tau}\rangle .$$

This implies $f\big((m_a^x \otimes 1 - 1 \otimes \gamma_a^x)^2\big) = 0$. So f satisfies part (a) of condition (ii) in Definition 4.3.15. Part (b) of condition (ii) follows from Equation (4.3.3). We conclude that f is optimal for $\mathcal{G}$. Since monomials of the form $m_{a_1}^{x_1} \cdots m_{a_k}^{x_k} \otimes n_{b_1}^{y_1} \cdots n_{b_\ell}^{y_\ell}$ span a dense subset of $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$. Equation (4.3.3) implies that f is uniquely determined by τ.

If τ is amenable, then $\pi_\tau^{\mathrm{op}} \times \pi_\tau$ is min-continuous, and hence f is min-continuous. If τ is finite-dimensional, then $\mathcal{H}_{\widetilde{\tau}}$ is finite-dimensional, and hence f is finite-dimensional. □

Proposition 4.3.18. *Suppose $\mathcal{G}$ has a determining pair $(\gamma, \mathcal{R})$ and $p \in C_{qc}$ is optimal for $\mathcal{G}$. There is a bijective correspondence between states on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$ for p and tracial states in $T^{(p)}(\gamma, \mathcal{R})$, sending an f to the tracial state $\tau := f|_{1 \otimes \mathcal{A}_{PVM}^{Y,B}}$. Moreover,*

(a) f is finite-dimensional if and only if the corresponding τ is finite-dimensional, and

(b) f is min-continuous if the corresponding τ is amenable.

Proof. Let f be a state on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$ for p. Since p is optimal for $\mathcal{G}$, f is an optimal state for $\mathcal{G}$. So

$$f\big((m_a^x \otimes 1 - 1 \otimes \gamma_a^x)^2\big) = 0 \tag{4.3.4}$$

for all $x \in X, a \in A$, and $\tau := f|_{1 \otimes \mathcal{A}_{PVM}^{Y,B}}$ is a tracial state on $\mathcal{A}_{PVM}^{Y,B}$ satisfying $\tau(r^* r) = 0$ for all $r \in \mathcal{R}$. Let $(\mathcal{H}, \pi, |\psi\rangle)$ be a GNS representation for f. Equation (4.3.4) implies

$$\pi(m_a^x \otimes 1) |\psi\rangle = \pi(1 \otimes \gamma_a^x) |\psi\rangle$$

for all $x \in X, a \in A$. It follows that

$$\tau(\gamma_a^x n_b^y) = \langle\psi| \pi(1 \otimes \gamma_a^x n_b^y) |\psi\rangle = \langle\psi| \pi(m_a^x \otimes n_b^y) |\psi\rangle = f(m_a^x \otimes n_b^y) = p(a, b|x, y)$$

for all a, b, x, y. So τ is a tracial state in $T^{(p)}(\gamma, \mathcal{R})$. Moreover, if f is finite-dimensional, then τ factors through the finite-dimensional C^*-algebra $\pi(1 \otimes \mathcal{A}_{PVM}^{Y,B})$, and hence τ is finite-dimensional. The rest of the proof follows straightforwardly from Lemma 4.3.17. □

Lemma 4.3.19. *Suppose $\mathcal{G} = (X, Y, A, B, \mu, V)$ has a determining pair $(\gamma, \mathcal{R})$. If a quantum correlation $p \in C_q(X, Y, A, B)$ is optimal for $\mathcal{G}$, then p has a full-rank projective model.*

Proof. Let f be a finite-dimensional state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ for p, and let τ be the corresponding tracial state in $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ given by Proposition 4.3.18. Since τ is a finite-dimensional tracial state on $\mathcal{A}_{PVM}^{Y,B}$, by Proposition 4.3.6, τ has a convex combination $\tau = \lambda_1 \tau_1 + \cdots + \lambda_k \tau_k$ of tracial states $\tau_1, \ldots, \tau_k \in \partial_e T_{\text{fin}}(\mathcal{A}_{PVM}^{X,A})$. By Proposition 4.3.8, every τ_i has a GNS representation $\big(\mathbb{C}^{d_i} \otimes \mathbb{C}^{d_i}, \mathbb{1} \otimes \pi_i(\cdot), |\varphi_{d_i}\rangle\big)$, where $d_i \geqslant 1$, $\pi_i : \mathcal{A} \to M_{d_i}(\mathbb{C})$

is an irreducible $*$-representation, and $|\varphi_{d_i}\rangle = \frac{1}{\sqrt{d_i}} \sum_{j=1}^{d_i} |j\rangle \otimes |j\rangle$. Note that $\lambda_1, \ldots, \lambda_k > 0$, so $\tau(r^* r) = 0$ for all $r \in \mathcal{R}$ implies $\tau_i(r^* r) = 0$ for all $r \in \mathcal{R}$ and $1 \leqslant i \leqslant k$. Since every $\{\gamma_a^x : a \in A\}$ is a PVM in the quotient $\mathcal{A}_{PVM}^{Y,B}/\langle \mathcal{R} \rangle$, every $\{\pi_i(\gamma_a^x)^T : a \in A\}$ is a PVM on $\mathbb{C}^{d_i}$. Let $M_a^x := \bigoplus_{i=1}^k \pi_i(\gamma_a^x)^T$, $N_b^y := \bigoplus_{i=1}^k \pi_i(n_b^y)$ for all a, b, x, y, and let $|\psi\rangle = \bigoplus_{i=1}^k \sqrt{\lambda_i} |\varphi_{d_i}\rangle$. Then

$$S := \left(\bigoplus_{i=1}^k \mathbb{C}^{d_i}, \bigoplus_{i=1}^k \mathbb{C}^{d_i}, \{M_a^x\}, \{N_b^y\}, |\psi\rangle \right)$$

is a full-rank projective quantum model such that

$$\begin{aligned} p_S(a,b|x,y) &= \sum_{i=1}^k \lambda_i \langle \varphi_{d_i}| \pi_i(\gamma_a^x)^T \otimes \pi_i(n_b^y) |\varphi_{d_i}\rangle = \sum_{i=1}^k \lambda_i \langle \varphi_{d_i}| \mathbb{1} \otimes \pi_i(\gamma_a^x)\pi_i(n_b^y) |\varphi_{d_i}\rangle \\ &= \sum_{i=1}^k \lambda_i \langle \varphi_{d_i}| \mathbb{1} \otimes \pi_i(\gamma_a^x n_b^y) |\varphi_{d_i}\rangle = \sum_{i=1}^k \lambda_i \tau_i(\gamma_a^x n_b^y) = \tau(\gamma_a^x n_b^y) = p(a,b|x,y) \end{aligned}$$

for all a, b, x, y. This completes the proof. □

In the proof of Lemma 4.3.19, we see that the model S employs a direct sum of maximally entangled states. When p is an extreme point in C_q, we can strengthen Lemma 4.3.19: p has a projective model which employs a single maximally entangled state. The proof is based on the observation that $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ is a convex face of $T_{\text{fin}}(\mathcal{A}_{PVM}^{Y,B})$ whenever p is extreme.

Lemma 4.3.20. *Suppose $\mathcal{G}$ has a determine pair $(\gamma, \mathcal{R})$ and $p \in C_q$ is optimal for $\mathcal{G}$. If p is an extreme point in C_q, then*

(a) $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R}) \cap \partial_e T_{\text{fin}}(\mathcal{A}_{PVM}^{Y,B}) = \partial_e T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$,

(b) $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R}) = \text{conv}\big(\partial_e T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})\big)$, *and*

(c) p has a projective quantum model that employs a maximally entangled state.

Proof. For part (a), it is clear that $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R}) \cap \partial_e T_{\text{fin}}(\mathcal{A}_{PVM}^{Y,B}) \subseteq \partial_e T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$. To see the converse inclusion, we assume for the sake of contradiction that there is a $\tau \in \partial_e T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$

which is not in $\partial_e T_{\text{fin}}(\mathcal{A}_{PVM}^{Y,B})$. Then there are distinct $\tau_1, \tau_2 \in T_{\text{fin}}(\mathcal{A}_{PVM}^{Y,B})$ and $0 < \lambda < 1$ such that $\tau = \lambda\tau_1 + (1-\lambda)\tau_2$. τ is in $T^{(p)}(\gamma, \mathcal{R})$, so $\tau(r^*r) = 0$ for all $r \in \mathcal{R}$. Since $\lambda > 0$, $1 - \lambda > 0$, and $\tau_1(r^*r), \tau_2(r^*r) \geqslant 0$, it follows that

$$\tau_1(r^*r) = \tau_2(r^*r) = 0 \tag{4.3.5}$$

for all $r \in \mathcal{R}$. By Lemma 4.3.17, the vectors $p_1, p_2 \in \mathbb{R}^{A\times B\times X\times Y}$ defined by $p_i(a,b|x,y) = \tau_i(\gamma_a^x n_b^y), i \in \{1,2\}$ are optimal quantum correlations for $\mathcal{G}$ such that $p = \lambda p_1 + (1-\lambda)p_2$. Because p is an extreme point in C_q, we have $p_1 = p_2 = p$. Equation (4.3.5) implies $\tau_1, \tau_2 \in T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$, which contradicts the assumption that τ is an extreme point in $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$. We conclude that $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R}) \cap \partial_e T_{\text{fin}}(\mathcal{A}_{PVM}^{Y,B}) = \partial_e T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$.

Now we prove part (b). For any $\tau \in T_{\text{fin}}^{(p)}(\gamma.\mathcal{R})$, by Proposition 4.3.6, τ is a convex combination $\tau = \lambda_1\lambda_1 + \cdots + \lambda_k\lambda_k$ of $\tau_1, \ldots, \tau_k \in T_{\text{fin}}(\mathcal{A}_{PVM}^{Y,B})$. Since every $\lambda_1 > 0$, $\tau(r^*r) = 0$ for all $r \in \mathcal{R}$ implies $\tau_i(r^*r) = 0$ for all $1 \leqslant i \leqslant k$ and $r \in \mathcal{R}$. Again, by Lemma 4.3.17 and the extremality of p, every τ_i is on $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$. Hence by part (a), every τ_i is in $\partial_e T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$. This proves part (b).

For (c), we first note that $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ is non-empty, because p is optimal for $\mathcal{G}$. Let $\tau \in \partial_e T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$. Then by part (a), $\tau \in \partial_e T_{\text{fin}}(\mathcal{A}_{PVM}^{Y,B})$. By Proposition 4.3.8, τ has a GNS representation $\left(\mathbb{C}^d \otimes \mathbb{C}^d, \mathbb{1} \otimes \pi(\cdot), |\varphi_d\rangle\right)$ where $\pi : \mathcal{A}_{PVM}^{Y,B} \to M_d(\mathbb{C}^d)$ is an irreducible $*$-representation and $|\varphi_d\rangle$ is a maximally entangled state. Let $M_a^x := \pi(\gamma_a^x)^T$ and $N_b^y := \pi(n_b^y)$ for all a, b, x, y. Then following the same reasoning as in the proof of Lemma 4.3.19,

$$S := \left(\mathbb{C}^d, \mathbb{C}^d, \{M_a^x\}, \{N_b^y\}, |\varphi_d\rangle\right)$$

is a projective quantum model for p that employs a maximally entangled state. □

Now we are ready to proof Theorem 4.3.16.

Proof of Theorem 4.3.16. (a)⇔(b): By Lemma 4.3.19, p has a full-rank projective quantum model. Then by Corollary 3.1.8, p is a self-test for all quantum models if and only if p is an abstract state self-test for projective finite-dimensional states. So (a)⇔(b) follows.

(b)⇔(c) follows directly from the bijective correspondence between finite-dimensional states on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ for p and tracial states in $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$, as shown in Proposition 4.3.18.

(c)⇔(d): By Lemma 4.3.20, $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ contains a unique element if and only if $\partial_e T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ contains a unique element. So (c)⇔(d) follows from the correspondence between tracial states in $\partial_e T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ and representations in $\text{Irr}_{\text{fin}}\big(\mathcal{A}_{PVM}^{Y,B}\big)$ which satisfy Equation (4.3.2), as shown in Corollary 4.3.9. □

Corollary 4.3.21. *Let $\mathcal{G}$ be a nonlocal game with a determining pair $(\gamma, \mathcal{R})$. Suppose an extreme quantum correlation $p \in \partial_e C_q$ is optimal for $\mathcal{G}$ and is a self-test for quantum models. Let f, τ, and $\pi : \mathcal{A}_{PVM}^{Y,B} \to M_d(\mathbb{C})$ be unique finite-dimensional state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ for p, then unique tracial stat in $T_{\text{fin}}(\gamma, \mathcal{R})$, and the unique representation in $\text{Irr}_{\text{fin}}(\mathcal{A}_{PVM}^{Y,B})$ satisfying Equation (4.3.2) given by part (b), (d), and (d) of Theorem 4.3.16 respectively. Let $\widetilde{M}_a^x := \pi(\gamma_a^x)^T$ and $\widetilde{N}_b^y := \pi(n_b^y)$ for all a, b, x, y, and let $|\varphi_d\rangle := \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \otimes |i\rangle$. Then*

(a) the tuple $\big(\mathbb{C}^d \otimes \mathbb{C}^d, \mathbb{1} \otimes \pi(\cdot), |\varphi_d\rangle\big)$ is a GNS representation for τ,

(b) $\widetilde{S} := \big(\mathbb{C}^d, \mathbb{C}^d, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\varphi_d\rangle\big)$ is an ideal model for p, and

(c) the tuple $\big(\mathbb{C}^d \otimes \mathbb{C}^d, \pi_A \otimes \pi_B, |\varphi_d\rangle\big)$ is a GNS representation for f, where $\pi_A \otimes \pi_B$ is the associated representation of $\widetilde{S}$.

General results for nonlocal games

We also prove the following general statement for nonlocal games.

Theorem 4.3.22. *Let $\mathcal{G}$ be a nonlocal game with a determining pair $(\gamma, \mathcal{R})$, and let $C^*(\mathcal{G})$ be the associated game algebra. Then the following statements are equivalent.*

(a) $\mathcal{G}$ is a self-test for its optimal quantum strategies.

(b) There is a unique finite-dimensional optimal state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ for $\mathcal{G}$.

(c) $C^*(\mathcal{G})$ *has a unique finite-dimensional tracial state.*

(d) $C^*(\mathcal{G})$ *has a unique finite-dimensional irreducible* $*$*-representation (up to unitary equivalence).*

For the proof, we need to establish a correspondence between optimal states for $\mathcal{G}$ and tracial states on $C^*(\mathcal{G})$. Given a nonlocal game $\mathcal{G}$ with a determining pair $(\gamma, \mathcal{R})$, we say a tracial state τ on $\mathcal{A}_{PVM}^{Y,B}$ is optimal for $\mathcal{G}$ if $\tau(r^*r) = 0$ for all $r \in \mathcal{R}$. By Lemma 4.3.17, if τ is an optimal tracial state for $\mathcal{G}$, then the correlation defined by $p(a, b|x, y) = \tau(\gamma_a^x n_b^y)$ is optimal for $\mathcal{G}$. Hence a tracial state τ on $\mathcal{A}_{PVM}^{Y,B}$ is optimal for $\mathcal{G}$ if and only if τ is in $T^{(p)}(\gamma, \mathcal{R})$ for some optimal $p \in C_{qc}$ for $\mathcal{G}$. The following correspondence between optimal states on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$ for $\mathcal{G}$ and optimal tracial states on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$ for $\mathcal{G}$ is an immediate consequence of Proposition 4.3.18.

Lemma 4.3.23. *Suppose* $\mathcal{G}$ *has a determining pair* $(\gamma, \mathcal{R})$*. There is a bijective correspondence between optimal states on* $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$ *for* $\mathcal{G}$ *and optimal tracial states on* $\mathcal{A}_{PVM}^{Y,B}$ *for* $\mathcal{G}$*, sending an* f *to the tracial state* $\tau := f|_{1 \otimes \mathcal{A}_{PVM}^{Y,B}}$*. Moreover,*

(a) f *is finite-dimensional if and only if the corresponding* τ *is finite-dimensional, and*

(b) f *is min-continuous if the corresponding* τ *is amenable.*

Any optimal tracial state for a nonlocal game $\mathcal{G}$ with determining pair $(\gamma, \mathcal{R})$ drops to a tracial state on the quotient $C^*(\mathcal{G})$ and vice versa. The following correspondence between optimal tracial states for $\mathcal{G}$ and tracial states on the associated game algebra $C^*(\mathcal{G})$ follows straight from Propositions 4.3.10 and 4.3.13.

Lemma 4.3.24. *Suppose* $\mathcal{G}$ *has a determining pair* $(\gamma, \mathcal{R})$*, and let* $C^*(\mathcal{G})$ *be the associated game algebra. Then there is a bijective correspondence between optimal tracial states on* $\mathcal{A}_{PVM}^{Y,B}$ *for* $\mathcal{G}$ *with respect to* $(\gamma, \mathcal{R})$ *and tracial states on* $C^*(\mathcal{G})$*. Moreover,*

(a) an optimal tracial state on $\mathcal{A}_{PVM}^{Y,B}$ *is finite-dimensional if and only if the corresponding tracial state on* $C^*(\mathcal{G})$ *is finite-dimensional, and*

(b) an optimal tracial state on $\mathcal{A}_{PVM}^{Y,B}$ is amenable if the corresponding tracial state on $C^*(\mathcal{G})$ is amenable.

Put everything together, we conclude that:

Proposition 4.3.25. *Suppose $\mathcal{G}$ has a determining pair $(\gamma, \mathcal{R})$. Then there is a bijective correspondence between optimal states on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$ for $\mathcal{G}$ and tracial states on $C^*(\mathcal{G})$. Moreover,*

(a) an optimal state is finite-dimensional if and only if the corresponding tracial state is finite-dimensional, and

(b) an optimal state is min-continuous if the corresponding tracial state is amenable.

Now we are ready to prove Theorem 4.3.22

Proof of Theorem 4.3.22. (a)⇔(b): By Lemmas 4.2.4 and 4.2.5, both (a) and (b) imply that $\mathcal{G}$ has a unique optimal quantum correlation p and p is an extreme point in C_q. So (a)⇔(b) follows from (a)⇔(b) in Theorem 4.3.16.

(b)⇔(c) follows directly from the correspondence between finite-dimensional optimal states on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ for $\mathcal{G}$ and finite-dimensional tracial states on $C^*(\mathcal{G})$, as shown in Proposition 4.3.25.

(c)⇔(d): By Proposition 4.3.6, $T_{\text{fin}}\big(C^*(\mathcal{G})\big)$ contains a unique element if and only if $\partial_e T_{\text{fin}}\big(C^*(\mathcal{G})\big)$ contains a unique element. So (b)⇔(c) follows from Corollary 4.3.9. □

Corollary 4.3.26. *Let $\mathcal{G}$ be a nonlocal game with a determining pair $(\gamma, \mathcal{R})$. Let $C^*(\mathcal{G})$ be the associated game algebra, and let $q : \mathcal{A}_{PVM}^{Y,B} \to C^*(\mathcal{G})$ be the quotient map. Suppose $\mathcal{G}$ is a self-test for its optimal quantum strategies. Let $p \in \partial_e C_q$ be the unique optimal quantum correlation for $\mathcal{G}$ given by Lemma 4.2.3. Then p is a self-test for quantum models. Let $\widetilde{\pi}$ be the unique $*$-representation in $\text{Irr}_{\text{fin}}\big(C^*(\mathcal{G})\big)$ given by the part (d) of Theorem 4.3.22, and let π be the irreducible $*$-representation on $\mathcal{A}_{PVM}^{Y,B}$ given by part (d) of Theorem 4.3.16. Then $\pi = \widetilde{\pi} \circ q$.*

4.3.3 Self-testing for synchronous and XOR games

Synchronous games

Recall that a nonlocal game $\mathcal{G} = (X, Y, A, B, \mu, V)$ is said to a synchronous game if $A = B, X = Y$, and $V(a, a'|x, x) = 0$ for all $x \in X$ and $a \neq a'$ in A. We make the convention that the question distribution in a synchronous game is uniform on $X \times Y$, and we use $\mathcal{G} = (X, A, V)$ to denote a synchronous game.

Given a synchronous game $\mathcal{G} = (X, A, V)$ and a projective commuting operator strategy $S = (\mathcal{H}, \{M_a^x\}, \{N_b^y\}, |\psi\rangle)$ for $\mathcal{G}$. The strategy S is perfect for $\mathcal{G}$ if and only if

$$\langle\psi| M_a^x N_b^y |\psi\rangle = 0 \tag{4.3.6}$$

whenever $V(a, b|x, y) = 0$. As shown in [PSS+16, Theorem 5.5], if S is perfect for $\mathcal{G}$, then

$$M_a^x |\psi\rangle = N_a^x |\psi\rangle \tag{4.3.7}$$

for all $a \in A$ and $b \in B$.

Proposition 4.3.27. *Suppose $\mathcal{G} = (X, A, V)$ is a synchronous game with $w_q(\mathcal{G}) = 1$. Then $\mathcal{G}$ has a determining pair $(\gamma, \mathcal{R})$ where*

- *$\gamma_a^x = n_a^x$ for all $a \in A$ and $x \in X$, and*
- *$\mathcal{R} = \{n_a^x n_b^y : V(a, b|x, y) = 0\}$.*

Proof. Since every $\{n_a^x : a \in A\}$ is a PVM in $\mathcal{A}_{PVM}^{X,A}$, every γ_a^x is self-adjoint in $\mathcal{A}_{PVM}^{X,A}$ and every $\{\gamma_a^x : a \in A\}$ is a PVM in $C^*(\mathcal{G}) := \mathcal{A}_{PVM}^{X,A}/\langle\mathcal{R}\rangle$. Condition (i) of Definition 4.3.15 holds.

Next we examine condition (ii). Let f be a state on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$, and let $(\mathcal{H}, \pi, |\psi\rangle)$ be a GNS representation for f. Let $M_a^x := \pi(m_a^x), N_a^x := \pi(n_a^x)$ for all $a \in A, x \in X$, and let $S := (\mathcal{H}, \{M_a^x\}, \{N_b^y\}, |\psi\rangle)$ be a projective commuting operator strategy for $\mathcal{G}$

Suppose f is perfect for $\mathcal{G}$. Then S is perfect for $\mathcal{G}$. Equation (4.3.7) implies that

$$f\big((m_a^x \otimes 1 - 1 \otimes \gamma_a^x)^2\big) = \|(M_a^x - N_a^x)\,|\psi\rangle\|^2 = 0$$

for all $a \in A$ and $x \in X$. Hence f satisfies part (b) of condition (ii) in Definition 4.3.15. Let $w_1 = n_{a_1}^{x_1} \cdots n_{a_k}^{x_k}$ and $w_2 = n_{b_1}^{y_1} \cdots n_{b_\ell}^{y_\ell}$ be two monomials in $\mathcal{A}_{PVM}^{X,A}$. Note that every M_a^x is self-adjoint and commutes with every N_b^y. By Equation (4.3.7) again,

$$\begin{aligned} f(1 \otimes w_2 w_1) &= \langle\psi|\, N_{b_1}^{y_1} \cdots N_{b_\ell}^{y_\ell} N_{a_1}^{x_1} \cdots N_{a_k}^{x_k}\,|\psi\rangle = \langle\psi|\, M_{a_k}^{x_k} \cdots M_{a_1}^{x_1} N_{b_1}^{y_1} \cdots N_{b_\ell}^{y_\ell}\,|\psi\rangle \\ &= \langle\psi|\, N_{a_1}^{x_1} \cdots N_{a_k}^{x_k} N_{b_1}^{y_1} \cdots N_{b_\ell}^{y_\ell} N_{a_1}^{x_1} \cdots N_{a_k}^{x_k}\,|\psi\rangle = f(1 \otimes w_1 w_2). \end{aligned}$$

Since w_1 and w_2 were arbitrary and monomials over $\{n_b^y : y \in X, b \in A\}$ form a dense subset of $\mathcal{A}_{PVM}^{X,A}$, the linearly functional $\tau := f|_{1 \otimes \mathcal{A}_{PVM}^{X,A}}$ is a tracial state on $\mathcal{A}_{PVM}^{X,A}$. For any relation $r = n_a^x n_b^y$ in $\mathcal{R}$, by Equations (4.3.6) and (4.3.7),

$$\tau(r^* r) = \tau(n_b^y n_a^x n_a^x n_b^y) = \tau(n_a^x n_b^y) = \langle\psi|\, N_a^x N_b^y\,|\psi\rangle = \langle\psi|\, M_a^x N_b^y\,|\psi\rangle = 0.$$

We conclude that f satisfies condition (ii) in Definition 4.3.15.

Now suppose f satisfies condition (ii) in Definition 4.3.15. By part (a) of condition (ii), the strategy S satisfies Equation (4.3.7) for all $a \in A$ and $x \in X$. Part (b) of condition (ii) implies that $\tau := f|_{1 \otimes \mathcal{A}_{PVM}^{X,A}}$ is a tracial state satisfying

$$0 = \tau\big((n_a^x n_b^y)^*(n_a^x n_b^y)\big) = \tau(n_a^x n_b^y) = \langle\psi|\, N_a^y N_b^y\,|\psi\rangle\,|\psi\rangle = \langle\psi|\, M_a^x N_b^y\,|\psi\rangle\,.$$

whenever $V(a,b|x,y) = 0$. This implies S is perfect for $\mathcal{G}$, and hence f is perfect for $\mathcal{G}$. □

We refer to $C^*(\mathcal{G}) := \mathcal{A}_{PVM}^{X,A}/\langle\mathcal{R}\rangle$, with $\mathcal{R}$ defined in Proposition 4.3.27, as the *synchronous algebra* for $\mathcal{G}$.

Note that for any synchronous correlation $p \in C_{qc}^{syn}(X,A)$, one can define a synchronous game $\mathcal{G} = (X, A, V)$ such that p is perfect for $\mathcal{G}$. So Theorem 4.3.16 applies to all synchronous correlations.

Theorem 4.3.28. *Suppose a synchronous quantum correlation $p \in C_q^{syn}(X,A)$ is an extreme point in C_q. Then p is a self-test for quantum models if and only there is a unique finite-dimensional tracial state on $\mathcal{A}_{PVM}^{Y,B}$ such that $\tau(n_a^x n_b^y) = p(a,b|x,y)$ for all a, b, x, y.*

Proof. Let $\mathcal{G} = (X, A, V)$ be the nonlocal synchronous game defined by $V(a, b|x, y) = 0$ if and only if $p(a, b|x, y) = 0$. Then p is a perfect quantum correlation for $\mathcal{G}$. Let $(\gamma, \mathcal{R})$ be the determining pair of $\mathcal{G}$ defined in Proposition 4.3.27. Then a finite-dimensional tracial state τ on $\mathcal{A}_{PVM}^{X,A}$ is in $T_{\text{fin}}^{p}(\gamma, \mathcal{R})$ if and only if

(i) $\tau(n_a^x n_b^y) = p(a, b|x, y)$ for all a, b, x, y, and

(ii) $\tau\big((n_a^x n_b^y)^*(n_a^x n_b^y)\big) = \tau(n_a^x n_b^y) = 0$ whenever $V(a, b|x, y) = 0$.

Note that (ii) is equivalent to $\tau(n_a^x n_b^y) = 0$ whenever $p(a, b|x, y) = 0$, and this is already implied by (i). So $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$ consists of all finite-dimensional tracial states that satisfy (i). The theorem follows from (a)$\Leftrightarrow$(c) in Theorem 4.3.16. □

XOR games

Recall that a nonlocal game $\mathcal{G} = (I, J, A, B, \mu, V)$ is an XOR game if $A = B = \{0, 1\}$, and there is a matrix $(t_{ij}) \in \{0, 1\}^{I \times J}$ such that

$$V(a, b|i, j) = \begin{cases} 1 & \text{if } a \oplus b = t_{ij} \\ 0 & \text{otherwise.} \end{cases}$$

We also define the cost matrix (ω_{ij}) for $\mathcal{G}$ where $\omega_{ij} := (-1)^{t_{ij}}\mu(i, j)$. We always assume μ is non-degenerate, meaning that $\mu(i, j) \neq 0$ for all $i \in X, j \in Y$. So the cost matrix completely determines (t_{ij}) and μ. We use $\mathcal{G} = \big(I, J, (\omega_{ij})\big)$ to denote an XOR game. When working with XOR games, we usually use binary observable generators $x_i := m_0^i - m_1^i, i \in I$ for $\mathcal{A}_{PVM}^{I,\{0,1\}}$ and $y_j := n_0^j - n_1^j, j \in J$ for $\mathcal{A}_{PVM}^{J,\{0,1\}}$.

Every XOR game $\mathcal{G} = \big(I, J, (\omega_{ij})\big)$ has associated marginal row biases $\{r_i; i \in I\}$ and associated column biases $\{c_j : j \in J\}$, where $r_i > 0$ and $c_j > 0$[3] for all $i, j \in I$. Let f be state on $\mathcal{A}_{PVM}^{I,\{0,1\}} \otimes \mathcal{A}_{PVM}^{J,\{0,1\}}$, let $(\mathcal{H}, \pi, |\psi\rangle)$ be a GNS representation for f, and let

$$X_i := \pi\big(x_i \otimes 1\big), i \in I \text{ and } Y_j := \pi\big(1 \otimes y_j\big), j \in J$$

[3]In general, if μ is degenerate, then the cost matrix (ω_{ij}) may have a all-zero row or column and there could be a zero row or column bias.

be the binary observables employed by Alice and Bob. Then $\{X_i |\psi\rangle : i \in I\}, \{Y_j |\psi\rangle : j \in J\}$ is a vector strategy for $\mathcal{G}$. As shown in [Slo11, Corollary 3.2], f is optimal for $\mathcal{G}$ if and only if

$$\frac{1}{r_i} \sum_{j \in J} \omega_{ij} Y_j |\psi\rangle = X_i |\psi\rangle \tag{4.3.8}$$

for all $i \in I$. Equation (4.3.8) can also be replaced by

$$\frac{1}{c_j} \sum_{i \in I} \omega_{ij} X_i |\psi\rangle = Y_j |\psi\rangle \tag{4.3.9}$$

for all $j \in J$.

Proposition 4.3.29. *Let $\mathcal{G} = \big(I, J, (\omega_{ij})\big)$ be an XOR game, and let $\{r_i : i \in I\}$ be the associated row biases. Then $\mathcal{G}$ has a determining pair $(\gamma, \mathcal{R})$, where $\gamma = \{\gamma_a^i : i \in I, a \in \{0,1\}\}$ is given by*

$$\gamma_a^i = \frac{1}{2}\Big(1 - \frac{1}{r_i} \sum_{j \in J} \omega_{ij}(1 - 2n_a^j)\Big), \tag{4.3.10}$$

and the relations $\mathcal{R}$ consists of

$$\Big(\sum_{j \in J} \omega_{ij}(n_0^j - n_1^j)\Big)^2 - r_i^2 \tag{4.3.11}$$

for all $i \in I$.

Proof. Since every n_a^j is self-adjoint in $\mathcal{A}_{PVM}^{J,\{0,1\}}$, every γ_a^i is self-adjoint in $\mathcal{A}_{PVM}^{J,\{0,1\}}$. Equation (4.3.10) implies that

$$\gamma_0^i - \gamma_1^i = \frac{1}{r_i} \sum_{j \in J} \omega_{ij}(n_0^j - n_1^j),$$

so the relations in $\mathcal{R}$ can be expressed as $(\gamma_0^i - \gamma_1^i)^2 - 1, i \in I$. Hence every $\gamma_0^i - \gamma_1^i$ is a binary observable in $C^*(\mathcal{G}) := \mathcal{A}_{PVM}^{J,\{0,1\}}/\langle\mathcal{R}\rangle$. This means every $\{\gamma_0^i, \gamma_1^i\}$ is a PVM in $C^*(\mathcal{G})$. Condition (i) of Definition 4.3.15 holds.

Now we examine Condition (ii) of Definition 4.3.15. Let f be state on $\mathcal{A}_{PVM}^{I,\{0,1\}} \otimes \mathcal{A}_{PVM}^{J,\{0,1\}}$, let $(\mathcal{H}, \pi, |\psi\rangle)$ be a GNS representation for f, and let $X_i := \pi\big(x_i \otimes 1\big), Y_j := \pi\big(1 \otimes y_j\big)$, and $\widehat{Y}_j := \frac{1}{c_j} \sum_{i \in I} \omega_{ij} X_i$ for all $i \in I, j \in J$, where $\{c_j : j \in J\}$ is the column biases.

Suppose f is optimal. Then X_i, Y_j satisfy Equations (4.3.8) and (4.3.9). This implies

$$\pi\big(1 \otimes (\gamma_0^i - \gamma_1^i)\big) |\psi\rangle = \frac{1}{r_j} \sum_{j \in J} w_{ij} Y_j |\psi\rangle = X_i |\psi\rangle$$

for all $i \in I$. Replacing the binary observables with the corresponding PVM elements in the above equation, we have

$$\pi(1 \otimes \gamma_a^i) |\psi\rangle = \pi(m_a^i \otimes 1) |\psi\rangle .$$

It follows that

$$f\left(\left(m_a^i \otimes 1 - 1 \otimes \gamma_a^i\right)^2\right) = 0$$

for all $i \in I$ and $a \in \{0, 1\}$. Hence f satisfies part (a) of condition (ii). Note that $\widehat{Y}_j, Y_\ell$ are self-adjoint and $[\widehat{Y}_j, Y_\ell] = 0$ for all $j, \ell \in J$. Then for any monomials $W_1 := y_{i_1} \cdots y_{i_k}$ and $W_2 := y_{j_1} \cdots y_{j_\ell}$ in $\mathcal{A}_{PVM}^{J,\{0,1\}}$, Equation (4.3.9) implies that

$$\begin{aligned} f(1 \otimes W_1 W_2) &= \langle\psi| Y_{i_1} \cdots Y_{i_k} Y_{j_1} \cdots Y_{j_\ell} |\psi\rangle = \langle\psi| \widehat{Y}_{j_\ell} \cdots \widehat{Y}_{j_1} Y_{i_1} \cdots Y_{i_k} |\psi\rangle \\ &= \langle\psi| Y_{j_1} \cdots Y_{j_\ell} Y_{i_1} \cdots Y_{i_k} |\psi\rangle = f(1 \otimes W_2 W_1). \end{aligned}$$

It follows that $\tau := f|_{1 \otimes \mathcal{A}_{PVM}^{J,\{0,1\}}}$ is a tracial state. For any relation $s = \big(\sum_{j \in J} \omega_{ij} y_i\big)^2 - r_i^2 \in \mathcal{R}$, by Equation (4.3.8),

$$\begin{aligned} \pi(1 \otimes s) |\psi\rangle &= r_i^2 \big(\widehat{Y}_j^2 |\psi\rangle - |\psi\rangle\big) = r_i^2 \big(\widehat{Y}_j Y_j |\psi\rangle - |\psi\rangle\big) \\ &= r_i^2 \big(Y_j \widehat{Y}_j |\psi\rangle - |\psi\rangle\big) = r_i^2 \big(Y_j^2 |\psi\rangle - |\psi\rangle\big) = 0. \end{aligned}$$

The last equality uses the fact that $Y_j^2 = \mathbb{1}$. Hence $\tau(s^* s) = \langle\psi| \pi(1 \otimes s^* s) |\psi\rangle = 0$ for all $s \in \mathcal{R}$. We conclude that f satisfies part (b) condition (ii) in Definition 4.3.15.

On the other hand, suppose f satisfies parts (a) and (b) in condition (ii). Then in part (a), by replacing the PVM elements with the corresponding binary observables, we see that Equation (4.3.8) holds. This means f is optimal. We conclude that $(\gamma, \mathcal{R})$ satisfies condition (ii) in Definition 4.3.15. Hence $(\gamma, \mathcal{R})$ is a determining pair for $\mathcal{G}$. □

We refer to $C^*(\mathcal{G}) := \mathcal{A}_{PVM}^{J,\{0,1\}}/\langle\mathcal{R}\rangle$, with $\mathcal{R}$ defined in Proposition 4.3.29, as the *solution algebra* for $\mathcal{G}$. In [Slo11, Proposition 2.8], Slofstra shows that $\mathcal{G}$ has a unique optimal quantum correlation p if and only if the solution algebra for $\mathcal{G}$ is Clifford. Furthermore, the associated XOR correlation c with p has rank r if and only if the corresponding Clifford algebra is of rank r. Here the Clifford algebra Cl_r of rank r refers to the universal C^*-algebra generated by indeterminates $x_1, \cdots, x_r$ and subject to the relations $x_i x_j + x_j x_i = 2\delta_{ij}, 1 \leqslant i, j \leqslant n$. This algebra has either one (when r is even) or two (when r is odd) irreducible $*$-representations of dimension $2^{\lfloor r/2 \rfloor}$.

Theorem 4.3.30. *An XOR game $\mathcal{G}$ is a self-test for its optimal quantum strategies if and only if $\mathcal{G}$ has a unique optimal quantum correlation p and the associated XOR correlation with p has even rank.*

Proof. For the "only if" direction, suppose $\mathcal{G}$ is a self-test for its optimal quantum strategies. Then by Lemma 4.2.3, $\mathcal{G}$ has a unique optimal quantum correlation p. Let r be the rank of the associated XOR correlation with p. By Theorem 4.3.22, the solution algebra Cl_r for $\mathcal{G}$ has a unique finite-dimensional irreducible $*$-representation. So r must be even.

For the "if" direction, suppose $\mathcal{G}$ has a unique optimal quantum correlation p and the associated XOR correlation with p has even rank. This implies the solution algebra Cl_r for $\mathcal{G}$ has a unique finite-dimensional irreducible $*$-representation. By Theorem 4.3.22 again, $\mathcal{G}$ is a self-test for its optimal quantum strategies. □

4.4 Robust self-testing for nonlocal games with stable game algebras

4.4.1 Near-optimal strategies and approximate representations

Definition 4.4.1. *Let $\mathcal{G}$ be a nonlocal game with determining pair $(\gamma, \mathcal{R})$, and let $\nu : \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ be a function such that $\nu(\epsilon) \to 0$ as $\epsilon \to 0$. We say $(\gamma, \mathcal{R})$ is ν-**stable** if for*

any $\epsilon \geqslant 0$ and projective ϵ-optimal quantum strategy

$$S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\big)$$

for $\mathcal{G}$,

(i) $\|\big(\pi_A(m_a^x) \otimes \mathbb{1} - \mathbb{1} \otimes \pi_B(\gamma_a^x)\big)\,|\psi\rangle\| \leqslant \nu(\epsilon)$ *for all $x \in X, a \in A$, where $\pi_A \otimes \pi_B$ is the associated representation of S,*

(ii) $\|\pi_B(r)\|_{\rho_B} \leqslant \nu(\epsilon)$ *for all $r \in \mathcal{R}$, where $\rho_B := \mathrm{Tr}_{\mathcal{H}_B}(|\psi\rangle\langle\psi|)$, and*

(iii) $\|\pi_B(n_b^y)\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(n_b^y)\|_F \leqslant \nu(\epsilon)$ *for all $y \in Y, b \in B$.*

Recall that the big Frobenius norm $\|\cdot\|_F$ on $M_d(\mathbb{C})$ is defined by $\|T\|_F = \sqrt{\mathrm{Tr}(T^*T)}$, and the ρ-norm $\|\cdot\|_\rho$ is defined by $\|T\|_\rho = \sqrt{\mathrm{Tr}(T^*T\rho)}$.

Lemma 4.4.2. *Suppose $\mathcal{G}$ is a nonlocal game with a ν-stable determining pair $(\gamma, \mathcal{R})$. Let*

$$S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\big)$$

be a projective ϵ-optimal quantum strategy for $\mathcal{G}$, and let $\phi := f_S|_{1 \otimes \mathcal{A}_{PVM}^{Y,B}}$ where f_S is the state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ induced by S. Then

(a) $\phi(r^*r) \leqslant \nu(\epsilon)^2$ *for all $r \in \mathcal{R}$,*

(b) $\|\pi_B(W)\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(W)\|_F \leqslant \deg(W)\nu(\epsilon)$ *for any monomial W over $\{n_b^y : b \in B, y \in Y\}$,*

(c) $|\phi(W_1W_2) - \phi(W_2W_1)| \leqslant \big(\deg(W_1) + \deg(W_2)\big)\nu(\epsilon)$ *for any monomials W_1 and W_2 over $\{n_b^y : y \in Y, b \in B\}$, and*

(d) $|\phi(\gamma_a^x n_b^y) - p_S(a,b|x,y)| \leqslant \nu(\epsilon)$ *for all a, b, x, y.*

Proof. Let $\pi_A \otimes \pi_B$ be the associated representation of S, and let $\rho_B := \mathrm{Tr}_{\mathcal{H}_B}(|\psi\rangle\langle\psi|)$. For any $r \in \mathcal{R}$,

$$\phi(r^* r) = \langle\psi| \mathbb{1} \otimes \pi_B(r^* r) |\psi\rangle = \|\pi_B(r)\|_{\rho_B}^2 \leqslant \nu(\epsilon)^2.$$

So (a) follows.

We prove (b) by induction on the degree k of W. $k = 1$ follows from condition (iii) of Definition 4.4.1. Now suppose (b) holds for any monomial of degree k for some $k \geqslant 1$. For any monomial $W = \alpha_1 \cdots \alpha_k \alpha_{k+1}$ in $\mathcal{A}_{PVM}^{Y,B}$ of degree $k+1$, let $W' := \alpha_1 \cdots \alpha_k$ be a monomial of degree k. Then by the induction hypothesis,

$$\|\pi_B(W')\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(W')\|_F \leqslant k\nu(\epsilon).$$

Note that $\|\pi_B(W')\|_{op} \leqslant 1$ and $\|\pi_B(\alpha_{k+1})\|_{op} \leqslant 1$, it follows that

$$\begin{aligned}
\|\pi_B(W)\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(W)\|_F =& \|\pi_B(W')\pi_B(\alpha_{k+1})\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(W')\pi_B(\alpha_{k+1})\|_F \\
\leqslant& \|\pi_B(W')\big(\pi_B(\alpha_{k+1})\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(\alpha_{k+1})\big)\|_F \\
&+ \|\big(\sqrt{\rho_B}\pi_B(W') - \pi_B(W')\sqrt{\rho_B}\big)\pi_B(\alpha_{k+1})\|_F \\
\leqslant& \|\pi_B(W')\|_{op}\|\pi_B(\alpha_{k+1})\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(\alpha_{k+1})\|_F \\
&+ \|\pi_B(\alpha_{k+1})\|_{op}\|\sqrt{\rho_B}\pi_B(W') - \pi_B(W')\sqrt{\rho_B}\|_F \\
\leqslant& \nu(\epsilon) + k\nu(\epsilon) = (k+1)\nu(\epsilon).
\end{aligned}$$

So (b) holds for monomials of degree $k+1$. We conclude that (b) holds.

To prove (c), we first recall that for any matrices S and T,

$$|\mathrm{Tr}(ST)| \leqslant \|S\|_{op} \cdot \|T\|_F.$$

Note that $\|\sqrt{\rho_B}\|_{op} \leqslant 1$, $\|\pi_B(W_1)\|_{op} \leqslant 1$, and $\|\pi_B(W_2)\|_{op} \leqslant 1$. By part (b) we have

$$\begin{aligned}
|\phi(W_1W_2) - \phi(W_2W_1)| =& |\mathrm{Tr}\Big(\sqrt{\rho_B}\pi_B(W_1)\big(\pi_B(W_2)\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(W_2)\big)\Big) \\
&+ \mathrm{Tr}\Big(\sqrt{\rho_B}\pi_B(W_2)\big(\pi_B(W_1)\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(W_1)\big)\Big)| \\
\leqslant& \|\pi_B(W_1)\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(W_1)\|_F + \|\pi_B(W_2)\sqrt{\rho_B} - \sqrt{\rho_B}\pi_B(W_2)\|_F
\end{aligned}$$

$$\leqslant \deg(W_1)\nu(\epsilon) + \deg(W_2)\nu(\epsilon) = \big(\deg(W_1) + \deg(W_2)\big)\nu(\epsilon).$$

This proves (c).

Now we prove (d). Since $\|\pi_B(n_B^y)\|_{op} \leqslant 1$ and $\|\big(\pi_A(m_a^x)\otimes\mathbb{1} - \mathbb{1}\otimes\pi_B(\gamma_a^x)\big)\,|\psi\rangle\| \leqslant \nu(\epsilon)$,

$$\begin{aligned}|\phi(\gamma_a^x n_b^y) - p_S(a,b|x,y)| &= |\langle\psi|\,\mathbb{1}\otimes\pi_B(\gamma_a^x n_b^y)\,|\psi\rangle - \langle\psi|\,\pi_A(m_a^x)\otimes\pi_B(n_b^y)\,|\psi\rangle| \\ &= |\langle\psi|\,\big(\pi_A(m_a^x)\otimes\mathbb{1} - \mathbb{1}\otimes\pi_B(\gamma_a^x)\big)\cdot\big(\mathbb{1}\otimes\pi_B(n_b^y)\big)\,|\psi\rangle| \\ &\leqslant \|\big(\pi_A(m_a^x)\otimes\mathbb{1} - \mathbb{1}\otimes\pi_B(\gamma_a^x)\big)\,|\psi\rangle\| \leqslant \nu(\epsilon)\end{aligned}$$

for all a, b, x, y. This completes the proof. □

Given a quantum model

$$S = \big(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x\}, \{N_b^y\}, |\psi\rangle\big),$$

by picking the Schmidt basis for $|\psi\rangle$ as bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, and dilating Alice or Bob's system so that they have the same dimension, we can always write

$$S = \big(\mathbb{C}^d, \mathbb{C}^d, \{M_a^x\}, \{N_b^y\}, |\psi\rangle = \sum_{i=1}^d \lambda_i\,|i\rangle\otimes|i\rangle\big), \tag{4.4.1}$$

where $d \geqslant 1$ and $\lambda_1, \ldots, \lambda_d \geqslant 0$, without changing the state induced by S. We refer to Equation (4.4.1) as a *balanced form* of S. Indeed, if $s := \dim(\mathcal{H}_B) - \dim(\mathcal{H}_A) > 0$, then we take $\mathcal{H}_A \oplus \mathbb{C}^s$ as the new space for Alice and define her new measurement operators to be $M_a^x \oplus \mathbb{1}$ for one fixed $a \in A$ and $M_{a'}^x \oplus 0$ for the rest $a' \in A$. We can process similarly when $\dim(\mathcal{H}_A) > \dim(\mathcal{H}_B)$. So we can always assume $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = d$ for some $d \geqslant 1$. Consider the Schmidt decomposition $|\psi\rangle = \sum_{i=1}^k \lambda_i\,|\alpha_i\rangle\otimes|\beta_i\rangle$ where $k \leqslant d$, $\lambda_1, \ldots, \lambda_k > 0$, and $\{|\alpha_i\rangle : 1 \leqslant i \leqslant k\}$ and $\{|\beta_i\rangle : 1 \leqslant i \leqslant k\}$ are orthonormal sets in $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. We can expand these two orthonormal sets to orthonormal bases $\{|\alpha_i\rangle : 1 \leqslant i \leqslant d\}$ and $\{|\beta_i\rangle : 1 \leqslant i \leqslant d\}$ for $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, and write $|\psi\rangle = \sum_{i=1}^d \lambda_i\,|\alpha_i\rangle\otimes|\beta_i\rangle$ where $\lambda_{k+1} = \cdots = \lambda_d = 0$. After fixing the bases $\{|\alpha_i\rangle : 1 \leqslant i \leqslant d\}$ and $\{|\beta_i\rangle : 1 \leqslant i \leqslant d\}$, we can identify both $\mathcal{H}_A$ and $\mathcal{H}_B$ with $\mathbb{C}^d$, and identify $|\psi\rangle$ with $\sum_{i=1}^d \lambda_i\,|i\rangle\otimes|i\rangle$. One of the advantages of the balanced form Equation (4.4.1) is that the reduced density matrices of $|\psi\rangle$ on Alice and Bob's sides are both $\rho := \sum_{i=1}^d \lambda_i^2\,|i\rangle\langle i|$. So we have $|\psi\rangle = \sqrt{\rho}\otimes\mathbb{1}\,|\widehat{\varphi}_d\rangle = \mathbb{1}\otimes\sqrt{\rho}\,|\widehat{\varphi}_d\rangle$, where $|\widehat{\varphi}_d\rangle := \sum_{i=1}^d |i\rangle\otimes|i\rangle$.

Proposition 4.4.3. *Let $\mathcal{G} = (X, Y, A, B, \mu, V)$ be a nonlocal game with a ν-stable determining pair $(\gamma, \mathcal{R})$. Suppose $p \in C_q$ is an optimal quantum correlation for $\mathcal{G}$. Let $S_n, n \in \mathbb{N}$ be a sequence of projective quantum models such that $\|p_{S_n} - p\|_1 \to 0$ as $n \to \infty$, and let $\phi_n := f_{S_n}|_{1 \otimes \mathcal{A}_{PVM}^{Y,B}}$ for all $n \in \mathbb{N}$, where f_{S_n} is the state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ induced by S_n. Then any weak*-accumulation point ϕ of $\{\phi_n, n \in \mathbb{N}\}$ is an amenable tracial state on $\mathcal{A}_{PVM}^{Y,B}$ satisfying*

(a) $\phi(\gamma_a^x n_b^y) = p(a, b|x, y)$ for all a, b, x, y, and

(b) $\phi(r^* r) = 0$ for all $r \in \mathcal{R}$.

We remind the reader that using the notation before, there is another way to phrase this proposition: any weak*-accumulation point of $\{\phi_n : n \in \mathbb{N}\}$ is an amenable tracial state in $T^{(p)}(\gamma, \mathcal{R})$.

Proof. By passing a subsequence, we may assume that $\lim_{n\to\infty} \phi_n = \phi$ in the weak*-topology. Note that $\|p_{S_n} - p\|_1 \to 0$ implies $\epsilon_n := w_q(\mathcal{G}) - w(\mathcal{G}; S_n) \to 0$ as $n \to \infty$. By part (d) of Lemma 4.4.2,

$$\begin{aligned}
&|\phi(\gamma_a^x n_b^y) - p(a, b|x, y)| \\
&\qquad \leqslant |\phi(\gamma_a^x n_b^y) - \phi_n(\gamma_a^x n_b^y)| + |\phi_n(\gamma_a^x n_b^y) - p_{S_n}(a, b|x, y)| + |p_{S_n}(a, b|x, y) - p(a, b|x, y)| \\
&\qquad \leqslant |\phi(\gamma_a^x n_b^y) - \phi_n(\gamma_a^x n_b^y)| + |p_{S_n}(a, b|x, y) - p(a, b|x, y)| + \nu(\epsilon_n) \to 0
\end{aligned}$$

as $n \to \infty$. So (a) follows. By part (a) of Lemma 4.4.2, $\phi_n(r^* r) \leqslant \nu(\epsilon_n)^2 \to 0$ as $n \to \infty$ for all $r \in \mathcal{R}$. This proves (b).

It follows from part (c) of Lemma 4.4.2 that ϕ is a tracial state. Now we only need to show ϕ is amenable. Let $\widetilde{f}$ be the state on $(\mathcal{A}_{PVM}^{Y,B})^{\mathrm{op}} \otimes \mathcal{A}_{PVM}^{Y,B}$ defined by $\widetilde{f}(\alpha^{\mathrm{op}} \otimes \beta) := \phi(\alpha\beta), \alpha, \beta \in \mathcal{A}_{PVM}^{Y,B}$. We write every S_n in their balanced form

$$S_n = \left(\mathbb{C}^{d_n}, \mathbb{C}^{d_n}, \{M_a^x(n)\}, \{N_b^y(n)\}, |\psi_n\rangle\right)$$

and denote by ρ_n the reduced density of $|\psi_n\rangle$. For every $n \in \mathbb{N}$, let $\pi_n^A \otimes \pi_n^B$ be the associated representation of S_n (in the balanced form), let $\widetilde{\pi}_n : (\mathcal{A}_{PVM}^{Y,B})^{\mathrm{op}} \otimes \mathcal{A}_{PVM}^{Y,B} \to \mathcal{B}(\mathbb{C}^d \otimes \mathbb{C}^d)$ be the $*$-representation sending

$$1 \otimes n_b^y \mapsto \mathbb{1} \otimes \pi_n^B(n_b^y) \text{ and } n_b^y \otimes 1 \mapsto \pi_n^B(n_b^y)^T \otimes \mathbb{1},$$

and let $\widetilde{f}_n$ be the finite-dimensional state on $(\mathcal{A}_{PVM}^{Y,B})^{\mathrm{op}} \otimes \mathcal{A}_{PVM}^{Y,B}$ defined by

$$\widetilde{f}_n(\alpha) = \langle \psi_n | \, \widetilde{\pi}_n(\alpha) \, |\psi_n\rangle \, , \alpha \in (\mathcal{A}_{PVM}^{Y,B})^{\mathrm{op}} \otimes \mathcal{A}_{PVM}^{Y,B}.$$

For any monomials W_1 and W_2 over $\{n_b^y, y \in Y, b \in B\}$,

$$\begin{aligned}
\widetilde{f}_n(W_1^{\mathrm{op}} \otimes W_2) &= \langle \psi_n | \, \widetilde{\pi}_n(W_1^{op} \otimes W_2) \, |\psi_n\rangle = \langle \psi_n | \, \pi_n^B(W_1)^T \otimes \pi_n^B(W_2) \, |\psi_n\rangle \\
&= \langle \widehat{\varphi}_{d_n} | \, \pi_n^B(W_1)^T \otimes \sqrt{\rho_n} \pi_n^B(W_2) \sqrt{\rho_n} \, |\widehat{\varphi}_{d_n}\rangle \\
&= \langle \widehat{\varphi}_{d_n} | \, \mathbb{1} \otimes \sqrt{\rho_n} \pi_n^B(W_2) \sqrt{\rho_n} \pi_n^B(W_1) \, |\widehat{\varphi}_{d_n}\rangle \\
&= \mathrm{Tr}\big(\sqrt{\rho_n} \pi_n^B(W_2) \sqrt{\rho_n} \pi_n^B(W_1) \, \big),
\end{aligned}$$

where $|\widehat{\varphi}_{d_n}\rangle := \sum_{i=1}^{d_n} |i\rangle \otimes |i\rangle$. So by part (b) of Lemma 4.4.2,

$$\begin{aligned}
|\widetilde{f}_n(W_1^{\mathrm{op}} \otimes W_2) - \phi_n(W_1 W_2)| &= |\mathrm{Tr}\Big(\sqrt{\rho_n} \pi_n(W_1) \big(\sqrt{\rho_n} \pi_n(W_2) - \pi_n(W_2) \sqrt{\rho_n}\big)\Big)| \\
&\leqslant \|\sqrt{\rho_n} \pi_n(W_2) - \pi_n(W_2) \sqrt{\rho_n}\|_F \leqslant \deg(W_2) \nu(\epsilon_n).
\end{aligned}$$

It follows that

$$\begin{aligned}
&|\widetilde{f}_n(W_1^{\mathrm{op}} \otimes W_2) - \widetilde{f}(W_1^{\mathrm{op}} \otimes W_2)| \\
&\quad \leqslant |\widetilde{f}_n(W_1^{\mathrm{op}} \otimes W_2) - \phi_n(W_1 W_2)| + |\phi_n(W_1 W_2) - \phi(W_1 W_2)| + |\phi(W_1 W_2) - \widetilde{f}(W_1^{\mathrm{op}} \otimes W_2)| \\
&\quad \leqslant \deg(W_2) \nu(\epsilon_n) + |\phi_n(W_1 W_2) - \phi(W_1 W_2)| \to 0
\end{aligned}$$

as $n \to \infty$. Since W_1 and W_2 were arbitrary, $\lim_{n \to \infty} \widetilde{f}_n = \widetilde{f}$ in the weak*-topology. This means $\widetilde{f}$ is the weak*-limit of a sequence of finite-dimensional states on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$. Hence $\widetilde{f}$ is min-continuous, and thus ϕ is amenable. □

4.4.2 A lifting theorem for game algebras

Proposition 4.4.4. *Suppose a nonlocal game $\mathcal{G}$ has a determining pair $(\gamma, \mathcal{R})$. Let $C^*(\mathcal{G})$ be the associated game algebra. For every finite-dimensional tracial state τ on $\mathcal{A}_{PVM}^{Y,B}$ that satisfies $\tau(r^*r) = 0$ for all $r \in \mathcal{R}$, there is a ucp map $\theta : C^*(\mathcal{G}) \to \mathcal{A}_{PVM}^{Y,B}$ such that*

$$\tau\Big(\big(\theta(\alpha) - \alpha\big)^*\big(\theta(\alpha) - \alpha\big)\Big) = 0$$

for any $*$-polynomial $\alpha \in \mathbb{C}^*\langle n_b^y, y \in Y, b \in B\rangle$.

Note that $\mathcal{A}_{PVM}^{Y,B}, C^*(\mathcal{G})$, and $\mathcal{A}_{PVM}^{Y,B}/\mathcal{I}_\tau$ all have generating set $\{n_b^y : y \in Y, b \in B\}$. In the expression $\theta(\alpha) - \alpha$, the first α is viewed as an element of $C^*(\mathcal{G})$, while the second α is an element of $\mathcal{A}_{PVM}^{Y,B}$. The proof uses a lifting theorem due to Choi and Effros.

Lemma 4.4.5 ([CE76], see also [Arv77])**.** *Suppose $\mathcal{A}$ and $\mathcal{B}$ are two unital separable C^*-algebras. Suppose $\mathcal{J}$ is a closed two-sided ideal in $\mathcal{B}$. Let $q : \mathcal{B} \to \mathcal{B}/\mathcal{J}$ be the quotient map, and let $\varphi : \mathcal{A} \to \mathcal{B}/\mathcal{J}$ be a ucp map. If φ is nuclear, then there is a ucp map $\theta : \mathcal{A} \to \mathcal{B}$ such that $\varphi = q \circ \theta$.*

Proof of Proposition 4.4.4. Suppose τ is a finite-dimensional tracial state on $\mathcal{A}_{PVM}^{Y,B}$ satisfying $\tau(r^*r) = 0$ for all $r \in \mathcal{R}$. Let $\langle\mathcal{R}\rangle$ be the closed two-sided ideal generated by $\mathcal{R}$. Since $\langle\mathcal{R}\rangle \subset \mathcal{I}_\tau$, there is a surjective $*$-homomorphism $\varphi : C^*(\mathcal{G}) \to \mathcal{A}_{PVM}^{Y,B}/\mathcal{I}_\tau$ sending $\alpha \mapsto \alpha$ for any $*$-polynomial $\alpha \in \mathbb{C}^*\langle n_b^y, y \in Y, b \in B\rangle$. Since τ is finite-dimensional, $\mathcal{A}_{PVM}^{X,A}/\mathcal{I}_\tau$ is a finite-dimensional C^*-algebra, and hence nuclear. It follows that φ is nuclear. By Lemma 4.4.5, there is a ucp map $\theta : \mathcal{A}(\mathcal{G}) \to \mathcal{A}_{PVM}^{Y,B}$ such that $\varphi = q_\tau \circ \theta$, where $q_\tau : \mathcal{A}_{PVM}^{Y,B} \to \mathcal{A}_{PVM}^{Y,B}/\mathcal{I}_\tau$ is the quotient map. For any $*$-polynomial $\alpha \in \mathbb{C}^*\langle n_b^y, y \in Y, b \in B\rangle$,

$$q_\tau\big(\theta(\alpha)\big) = \varphi(\alpha) = \alpha = q_\tau(\alpha)$$

in $\mathcal{A}_{PVM}^{Y,B}/\mathcal{I}_\tau$. Hence $\theta(\alpha) - \alpha \in \ker q_\tau = \mathcal{I}_\tau$. □

Proposition 4.4.4 is used to prove the following proposition.

Proposition 4.4.6. *Let $\mathcal{G} = (X, Y, A, B, \mu, V)$ be a nonlocal game with a ν-stable determine pair $(\gamma, \mathcal{R})$. Suppose $p \in C_q$ is the unique optimal quantum correlation for $\mathcal{G}$ and there is a unique amenable tracial state τ in $T^{(p)}(\gamma, \mathcal{R})$. Then there exists a full-rank projective quantum model $\widetilde{S}$ for p such that the following holds. For any sequence of projective quantum models*

$$S_n = \big(\mathcal{H}_n^A, \mathcal{H}_n^B, \{M_a^x(n)\}, \{N_b^y(n)\}, |\psi_n\rangle\big), n \in \mathbb{N}$$

with $\lim_{n\to\infty} \|p_{S_n} - p\|_1 = 0$, there is a function $\eta : \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ with $\lim_{n\to\infty} \eta(n) = 0$ such that $S_n \geq_{\eta(n)} \widetilde{S}$ for all $n \in \mathbb{N}$.

Proof. By Proposition 4.3.18, τ extends to a state $\widetilde{f}$ which is the unique state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ that can achieve p. Note that p is a quantum correlation. This means $\widetilde{f}$ and τ must be finite-dimensional, and hence $\widetilde{f}$ is the unique finite-dimensional state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ for p, and τ is the unique tracial state in $T_{\text{fin}}^{(p)}(\gamma, \mathcal{R})$. Since p is the unique optimal quantum correlation for $\mathcal{G}$, by Lemma 4.2.4, p is an extreme point in C_q. Hence by Theorem 4.3.16, p is a self-test for all quantum models, and $\mathcal{G}$ is a self-test for its optimal quantum strategies. Let $\pi : \mathcal{A}_{PVM}^{Y,B} \to M_d(\mathbb{C})$ be the finite-dimensional irreducible $*$-representation given by part (d) of Theorem 4.3.16, and let $\widetilde{\pi}$ be the unique irreducible $*$-representation of $C^*(\mathcal{G})$ given by part (d) of Theorem 4.3.22. Then $\pi = \widetilde{\pi} \circ q$ by Corollary 4.3.26, where $q : \mathcal{A}_{PVM}^{Y,B} \to C^*(\mathcal{G})$ is the quotient map. Let $\widetilde{M}_a^x := \pi(\gamma_a^x)^T$ and $\widetilde{N}_b^y := \pi(n_b^y)$ for all a, b, x, y, and let $|\varphi_d\rangle := \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle \otimes |i\rangle$. Then by Corollary 4.3.21,

$$\widetilde{S} := \Big(\mathbb{C}^d, \mathbb{C}^d, \{\widetilde{M}_a^x\}, \{\widetilde{N}_b^y\}, |\varphi_d\rangle\Big)$$

is a quantum model for $\mathcal{G}$, and the triple $(\mathbb{C}^d \otimes \mathbb{C}^d, \widetilde{\pi}_A \otimes \widetilde{\pi}_B, |\varphi_d\rangle)$ is a GNS representation of $\widetilde{f}$, where $\widetilde{\pi}_A \otimes \widetilde{\pi}_B$ is the associated representation of $\widetilde{S}$.

Let $\theta : \mathcal{A}(\mathcal{G}) \to \mathcal{A}_{PVM}^{Y,B}$ be the ucp map given by Proposition 4.4.4 that satisfies

$$\tau\Big(\big(\theta(\alpha) - \alpha\big)^*\big(\theta(\alpha) - \alpha\big)\Big) = 0$$

for any $*$-polynomial α over $\{n_b^y : y \in Y, b \in B\}$. For every $n \in \mathbb{N}$, let $\pi_n^A \otimes \pi_n^B$ be the associated representation of S_n, and let $\rho_n^A := \text{Tr}_{\mathcal{H}_n^B}(|\psi_n\rangle\langle\psi_n|)$ and $\rho_n^B := \text{Tr}_{\mathcal{H}_n^A}(|\psi_n\rangle\langle\psi_n|)$.

Claim 4.4.7. *There are integers $r_n, s_n \in \mathbb{N}$, and isometries $I_{A,n} : \mathcal{H}_n^A \to \mathbb{C}^d \otimes \mathbb{C}^{r_n}$ and $I_{B,n} : \mathcal{H}_n^B \to \mathbb{C}^d \otimes \mathbb{C}^{s_n}$ such that*

$$\delta_{x,a}^A(n) := \|I_{A,n}^*(\widetilde{M}_a^x \otimes \mathbb{1}_{\mathbb{C}^{r_n}})I_{A,n} - M_a^x(n)\|_{\rho_n^A} \to 0, \text{ and} \tag{4.4.2}$$

$$\delta_{y,b}^B(n) := \|I_{B,n}^*(\widetilde{N}_b^y \otimes \mathbb{1}_{\mathbb{C}^{s_n}})I_{B,n} - N_b^y(n)\|_{\rho_n^B} \to 0 \tag{4.4.3}$$

as $n \to \infty$ for all a, b, x, y.

Proof of Claim 4.4.7. Without loss of generality, we can write every S_n in its balanced form

$$S_n = \big(\mathbb{C}^{d_n}, \mathbb{C}^{d_n}, \{M_a^x(n)\}, \{N_b^y(n)\}, |\psi_n\rangle\big).$$

Let ρ_n be the density of $|\psi_n\rangle$ on $\mathbb{C}^{d_n}$, and let $\phi_n := f_{S_n}|_{1 \otimes \mathcal{A}_{PVM}^{Y,B}}$ where f_{S_n} is the state on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$ induced by S_n. By Proposition 4.4.3, any weak*-accumulation point ϕ of $\{\phi_n : n \in \mathbb{N}\}$ is an amenable tracial state in $T^{(p)}(\gamma, \mathcal{R})$. By the hypothesis, $T^{(p)}(\gamma, \mathcal{R})$ has a unique amenable tracial state τ. So we must have $\phi = \tau$. By surpassing a subsequence, we conclude that $\lim_{n\to\infty} \phi_n = \tau$ is the weak*-topology.

Now consider the ucp maps $\theta_n^B := \pi_n^B \circ \theta, n \in \mathbb{N}$ from $C^*(\mathcal{G}) \to \mathcal{B}(\mathbb{C}^{d_n})$. Since $\widetilde{\pi}$ is the unique finite-dimensional irreducible $*$-representation of $C^*(\mathcal{G})$, any finite-dimensional $*$-representation of $C^*(\mathcal{G})$ is a direct sum of $\widetilde{\pi}$'s. By the Stinespring dilation theorem, there are $s_n \in \mathbb{N}$ and isometries $I_{B,n} : \mathbb{C}^{d_n} \to \mathbb{C}^d \otimes \mathbb{C}^{s_n}, n \in \mathbb{N}$ such that

$$\theta_n^B(\alpha) = I_{B,n}^*\big(\widetilde{\pi}(\alpha) \otimes \mathbb{1}_{\mathbb{C}^{s_n}}\big)I_{B,n}$$

for all $\alpha \in C^*(\mathcal{G})$. It follows that

$$\begin{aligned}
\lim_{n\to\infty} \|I_{B,n}^*\big(\widetilde{\pi}(\alpha) \otimes \mathbb{1}_{\mathbb{C}^{s_n}}\big)I_{B,n} - \pi_n^B(\alpha)\|_{\rho_n}^2 &= \lim_{n\to\infty} \|\theta_n^B(\alpha) - \pi_n^B(\alpha)\|_{\rho_n}^2 \\
&= \lim_{n\to\infty} \mathrm{Tr}_{\rho_n} \circ \pi_n^B\Big(\big(\theta(\alpha) - \alpha\big)^*\big(\theta(\alpha) - \alpha\big)\Big) \\
&= \lim_{n\to\infty} \phi_n\Big(\big(\theta(\alpha) - \alpha\big)^*\big(\theta(\alpha) - \alpha\big)\Big) \\
&= \tau\Big(\big(\theta(\alpha) - \alpha\big)^*\big(\theta(\alpha) - \alpha\big)\Big) = 0
\end{aligned}$$

for any $*$-polynomial α over $\{n_b^y : y \in Y, b \in B\}$. Taking $\alpha = n_b^y$, Equation (4.4.3) follows.

Note that every γ_a^x is a $*$-polynomial over $\{n_b^y : y \in Y, b \in B\}$ and is self-adjoint in $\mathcal{A}_{PVM}^{Y,B}$. So $\widetilde{\pi}(\gamma_a^x)$ and $\pi_n^B(\gamma_a^x)$ are self-adjoint, and the above calculation also implies

$$\begin{aligned}\|I_{B,n}^*\big(\widetilde{\pi}(\gamma_a^x)^T \otimes \mathbb{1}_{\mathbb{C}^{s_n}}\big)I_{B,n} - \pi_n^B(\gamma_a^x)^T\|_{\rho_n}^2 &= \|I_{B,n}^*\big(\widetilde{\pi}(\gamma_a^x) \otimes \mathbb{1}_{\mathbb{C}^{s_n}}\big)I_{B,n} - \pi_n^B(\gamma_a^x)\|_{\rho_n}^2 \\ &\to \tau\Big(\big(\theta(\gamma_a^x) - \gamma_a^x\big)^*\big(\theta(\gamma_a^x) - \gamma_a^x\big)\Big) = 0\end{aligned}$$

as $n \to \infty$. Again, since $(\gamma, \mathcal{R})$ is ν-stable, by part (b) of Lemma 4.4.2,

$$\|\pi_n^B(\gamma_a^x)\sqrt{\rho_n} - \sqrt{\rho_n}\pi_n^B(\gamma_a^x)\|_F \leqslant \|\gamma_a^x\|_{1,1}\nu(\epsilon_n),$$

where $\epsilon_n := w_q(\mathcal{G}) - w(\mathcal{G}; S_n) \to 0$ as $n \to \infty$. Here $\|\gamma_a^x\|_{1,1}$ is the first Sobolev 1-seminorm of the $*$-polynomial γ_a^x (see Section 7.3 for a definition). Hence

$$\begin{aligned}\|M_a^x(n) - \pi_n^B(\gamma_a^x)^T\|_{\rho_n} = \|\pi_n^A(m_a^x) - \pi_n^B(\gamma_a^x)^T\|_{\rho_n} &= \|\big(\pi_n^A(m_a^x) - \pi_n^B(\gamma_a^x)^T\big) \otimes \mathbb{1}\,|\psi_n\rangle\| \\ &\leqslant \|\big(\pi_n^A(m_a^x) \otimes \mathbb{1} - \mathbb{1} \otimes \pi_n^B(\gamma_a^x)\big)\,|\psi\rangle\| + \|\big(\pi_n^B(\gamma_a^x)^T \otimes \mathbb{1} - \mathbb{1} \otimes \pi_n^B(\gamma_a^x)\big)\,|\psi\rangle\| \\ &\leqslant \nu(\epsilon_n) + \|\pi_n^B(\gamma_a^x)\sqrt{\rho_n} - \sqrt{\rho_n}\pi_n^B(\gamma_a^x)\|_F \leqslant \big(\|\gamma_a^x\|_{1,1} + 1\big)\nu(\epsilon_n),\end{aligned}$$

$\to 0$ as $n \to \infty$. Note that $\big(\widetilde{\pi}(\gamma_a^x)\big)^T = \widetilde{M}_a^x$. Taking $r_n = s_n$ and $I_{A,n} = I_{B,n}$ for all $n \in \mathbb{N}$, it follows that

$$\begin{aligned}&\|I_{A,n}^*\big(\widetilde{M}_a^x \otimes \mathbb{1}_{\mathbb{C}^{r_n}}\big)I_{A,n} - M_a^x(n)\|_{\rho_n} \\ &\qquad\leqslant \|I_{B,n}^*\big(\widetilde{\pi}(\gamma_a^x)^T \otimes \mathbb{1}_{\mathbb{C}^{s_n}}\big)I_{B,n} - \pi_n^B(\gamma_a^x)^T\|_{\rho_n} + \|M_a^x(n) - \pi_n^B(\gamma_a^x)^T\|_{\rho_n}\end{aligned}$$

$\to 0$ as $n \to \infty$. So Equation (4.4.2) follows. □

Claim 4.4.8. *There are unit vectors $|\kappa_n\rangle \in \mathbb{C}^{r_n} \otimes \mathbb{C}^{s_n}, n \in \mathbb{N}$ such that*

$$\|I_{A,n} \otimes I_{B,n}\big(M_a^x(n) \otimes N_b^y(n)\,|\psi\rangle\big) - \big(\widetilde{M}_a^x \otimes \widetilde{N}_n^y\,|\varphi_d\rangle\big) \otimes |\kappa_n\rangle\| \to 0 \text{ as } n \to \infty \qquad (4.4.4)$$

for all a, b, x, y.

Proof of Claim 4.4.8. Let Δ be the spectral gap of the matrix $\widetilde{\pi}_A \otimes \widetilde{\pi}_B(\Phi_{\mathcal{G}})$, and let

$$\delta(n) := \sum_{a,b,x,y} \mu(x,y)V(a,b|x,y)\left(\delta_{x,a}^A(n) + \delta_{y,b}^B(n)\right), n \in \mathbb{N}.$$

Since $\widetilde{f}$ is the unique finite-dimensional optimal state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{X,A}$ for $\mathcal{G}$, by Proposition 4.2.13 and Remark 4.2.14, there is a unit vector $|\kappa_n\rangle \in \mathbb{C}^{r_n} \otimes \mathbb{C}^{s_n}$ for every $n \in \mathbb{N}$ such that

$$\|I_{A,n} \otimes I_{B,n}\big(M_a^x(n) \otimes N_b^y(n) \,|\psi\rangle\big) - \big(\widetilde{M}_a^x \otimes \widetilde{N}_n^y \,|\varphi_d\rangle\big) \otimes |\kappa_n\rangle\| \leqslant \frac{\sqrt{2}\big(\delta(n) + \sqrt{\epsilon_n}\big)}{\Delta} + \delta_{x,a}^A(n) + \delta_{y,b}^B(n)$$

for all a, b, x, y. By Claim 4.4.7, $\lim\limits_{n\to\infty} \delta_{x,a}^A(n) = \lim\limits_{n\to\infty} \delta_{y,b}^B(n) = 0$, and hence $\lim\limits_{n\to\infty} \delta(n) = 0$. So Equation (4.4.4) follows. □

For every $n \in \mathbb{N}$, let

$$\eta(n) := \max_{x,y,a,b} \left\{ \|I_{A,n} \otimes I_{B,n}\big(M_a^x(n) \otimes N_b^y(n) \,|\psi\rangle\big) - \big(\widetilde{M}_a^x \otimes \widetilde{N}_n^y \,|\varphi_d\rangle\big) \otimes |\kappa_n\rangle\| \right\}.$$

Then $S_n \succeq_{\eta(n)} \widetilde{S}$ for all $n \in \mathbb{N}$, and $\lim\limits_{n\to\infty} \eta(n) = 0$ by Claim 4.4.8. This completes the proof. □

4.4.3 General results

Theorem 4.4.9. *Let $\mathcal{G} = (X, Y, A, B, \mu, V)$ be a nonlocal game with a ν-stable determining pair $(\gamma, \mathcal{R})$. Suppose $p \in C_q$ is the unique optimal quantum correlation for $\mathcal{G}$. Then the following statements are equivalent.*

(a) p is a robust self-test for all quantum models.

(b) p is an abstract state self-test for all states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$.

(c) p is an abstract state self-test for all states on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$.

(d) There is a unique amenable tracial state in $T^{(p)}(\gamma, \mathcal{R})$.

Proof. (a)⇒(b) follows from Theorem 4.1.4.

(b)⇒(c): Suppose p is an abstract state self-test for all states on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$. That is, there is a unique state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ for p. By Lemma 4.3.19, p has a full-rank projective quantum model, so f must be finite-dimensional and projective. Hence f drops to a finite-dimensional state $\widetilde{f}$ on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ and $\widetilde{f}$ is a state for p. Now assume for the sake of contradiction that there is another state $f' \neq \widetilde{f}$ on $\mathcal{A}_{PVM}^{X,A} \otimes \mathcal{A}_{PVM}^{Y,B}$ that can achieve p. Then the pull-back of f' on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ is a state for p but is distinct to f, a contradiction. Hence $\widetilde{f}$ is the unique state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ for p.

(c)⇒(d): By Proposition 4.3.18, any amenable tracial state in $T^{(p)}(\gamma, \mathcal{R})$ extends uniquely to a state on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ for p. If there is a unique state f on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ for p, then $\tau := f|_{1 \otimes \mathcal{A}_{PVM}^{Y,B}}$ must be the unique amenable tracial state in $T^{(p)}(\gamma, \mathcal{R})$.

(d)⇒(a): Suppose there is a unique amenable tracial state τ in $T^{(p)}(\gamma, \mathcal{R})$. Let $\widetilde{S}$ be the full-rank projective quantum model given in Proposition 4.4.6. We first claim the p is a robust self-test for projective quantum models with ideal model $\widetilde{S}$. Assume for the sake of contradiction that there is a $\delta_0 > 0$ and a sequence of projective quantum models $S_n, n \in \mathbb{N}$ such that $\epsilon_n := \|p_{S_n} - p\|_1 \to 0$ as $n \to \infty$, but for every $n \in \mathbb{N}$, the relation $S_n \succeq_{\delta_0} \widetilde{S}$ does not hold. By Proposition 4.4.6, there is a function $\eta : \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ such that $\lim_{n\to\infty} \eta(n) = 0$ and $S_n \succeq_{\eta(n)} \widetilde{S}$ for all $n \in \mathbb{N}$. Take a big enough $N \in \mathbb{N}$ such that $\eta(N) \leqslant \delta_0$. Then $S_N \succeq_{\delta_0} \widetilde{S}$, which contradicts the assumption. We conclude that p is a robust self-test for projective quantum models. Note that the ideal model $\widetilde{S}$ is full-rank and projective. By [BCK+23, Theorem 4.1], p is a robust self-test for all quantum models. □

In terms of robust self-testing for nonlocal games, we state the following theorem.

Theorem 4.4.10. *For any nonlocal game $\mathcal{G}$ that has a ν-stable determining pair $(\gamma, \mathcal{R})$, the following statements are equivalent.*

(a) $\mathcal{G}$ is a robust self-test for its optimal quantum strategies.

(b) There is a unique optimal state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{min} \mathcal{A}_{POVM}^{Y,B}$ for $\mathcal{G}$ and f is finite-dimensional.

(c) *There is a unique optimal state f on $\mathcal{A}_{PVM}^{X,A} \otimes_{min} \mathcal{A}_{PVM}^{Y,B}$ for $\mathcal{G}$ and f is finite-dimensional.*

(d) *There is a unique amenable tracial state τ on $\mathcal{A}_{PVM}^{Y,B}$ such that $\tau(r^*r) = 0$ for all $r \in \mathcal{R}$ and τ is finite-dimensional.*

Proof. Any one of the above four statements implies $\mathcal{G}$ has a unique optimal quantum correlation. So the theorem follows directly from Theorem 4.4.9. □

In Theorem 4.3.22, we have shown that a nonlocal game $\mathcal{G}$ is a self-test if and only if the associated game algebra $C^*(\mathcal{G})$ has a unique finite-dimensional tracial state. Part (d) of Theorem 4.4.10 suggests one may have a similar characterization of robust self-testing: $\mathcal{G}$ is a robust self-test if and only if $C^*(\mathcal{G})$ has a unique amenable tracial state τ. However, as discussed in Remark 4.3.14, it is possible that an amenable tracial state on $\mathcal{A}_{PVM}^{Y,B}$ whose kernel contains $\mathcal{R}$ drops to a non-amenable tracial state on the quotient $C^*(\mathcal{G})$. So it is possible that $C^*(\mathcal{G})$ has a unique amenable tracial state but there are multiple amenable tracial states on $\mathcal{A}_{PVM}^{Y,B}$ that are optimal for $\mathcal{G}$. Nonetheless, if $C^*(\mathcal{G})$ has a unique tracial state $\widetilde{\tau}$ and $\widetilde{\tau}$ is finite-dimensional, then the tracial state τ on $\mathcal{A}_{PVM}^{Y,B}$ induced by $\widetilde{\tau}$ must be the unique tracial state (and hence the unique amenable tracial state) that satisfies $\tau(r^*r) = 0$ for all $r \in \mathcal{R}$. We conclude that:

Corollary 4.4.11. *Suppose a nonlocal game $\mathcal{G}$ has a ν-stable determining pair $(\gamma, \mathcal{R})$. Let $C^*(\mathcal{G})$ be the associated game algebra. If $C^*(\mathcal{G})$ has a unique tracial state τ and τ is finite-dimensional, then $\mathcal{G}$ is a robust self-test for its optimal quantum strategies.*

4.4.4 Robust self-testing for synchronous and XOR games

For XOR games, the stability of the $(\gamma, \mathcal{R})$ determining pair defined in Proposition 4.3.29 was first proved in [Slo11]. For synchronous games, a similar result was observed in [MPS21]. Both cases are also proved in [Pad24]. We summarize these results in the following proposition.

Proposition 4.4.12 (Proposition 5.14 and Proposition 5.23 in [Pad24])**.**

(1) Let $\mathcal{G} = (X, A, V)$ be a synchronous game with $w_q(\mathcal{G}) = 1$, and let $(\gamma, \mathcal{R})$ be as in Proposition 4.3.27. Then $(\gamma, \mathcal{R})$ is a $O(\epsilon^{1/4})$-stable determining pair for $\mathcal{G}$.

(2) Let $\mathcal{G} = (I, J, (\omega_{ij}))$ be an XOR game, and let $(\gamma, \mathcal{R})$ be as in Proposition 4.3.29. Then $(\gamma, \mathcal{R})$ is a $O(\epsilon^{1/4})$-stable determining pair for $\mathcal{G}$.

Hence for synchronous games and XOR games, we have:

Theorem 4.4.13. *Let $\mathcal{G}$ be a synchronous game, and let $C^*(\mathcal{G})$ be the associated synchronous algebra. If $C^*(\mathcal{G})$ has a unique tracial state τ and τ is finite-dimensional, then $\mathcal{G}$ is a robust self-test for its perfect quantum strategies.*

Theorem 4.4.14. *If p is an extreme point of $C_q^{unbiased}$ and the associated XOR correlation c has even rank, then p is a robust self-test for all quantum models.*

Chapter 5

Robustness and group stability

5.1 An enhanced Gowers-Hatami theorem

In this chapter, we look closer at the $\epsilon - \delta$ dependence in a robust self-test.

Definition 5.1.1. *Let $\mathcal{C}$ be a class of quatum models, and let $\eta : \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ be a function such that $\lim_{\epsilon \to 0} \eta(\epsilon) = 0$. A nonlocal game $\mathcal{G}$ is a robust self-test for its optimal strategies in $\mathcal{C}$ with robustness η if there is an ideal optimal strategy $\widetilde{S} \in \mathcal{C}$ such that $S \succeq_{\eta(\epsilon)} \widetilde{S}$ for any $\epsilon \geqslant 0$ and ϵ-optimal stategy $S \in \mathcal{C}$.*

We develop a group-theoretical approach to the robustness of self-testing. For some nonlocal games $\mathcal{G}$, one can associate a group G such that optimal (resp. near-optimal) strategies for $\mathcal{G}$ can be modeled by representations (approximate homomorphism) of G.

Definition 5.1.2. *Let $f : G \to \mathcal{U}(\mathcal{H})$ be a function from a finite group G to unitaries on a Hilbert space $\mathcal{H}$. Given a quantum density ρ on $\mathcal{H}$ and an $\epsilon \geqslant 0$, we say f is an (ϵ, ρ)-homomorphism if*

$$\mathbb{E}_{h \in G} \| f(g) f(h) - f(gh) \|_\rho^2 \leqslant \epsilon \tag{5.1.1}$$

for all $g \in G$. Here, unless specified otherwise, the expectation $\mathbb{E}$ is taken as the uniform distribution over G.

In the above definition, if $\rho = \frac{1}{\dim \mathcal{H}} \mathbb{1}$ is the maximally mixed state, then the ρ-norm $\|\cdot\|_\rho$ is indeed the normalized Hilber-Schmidt norm $\|\cdot\|_{hs}$. The Gowers-Hatami theorem [GH17] states that every finite group is dilation-stable with respect to $\|\cdot\|_{hs}$. In other words, for any $(\epsilon, \frac{1}{\dim(\mathcal{H})}\mathbb{1})$-homomorphism $f : G \to \mathcal{U}(\mathcal{H})$, there is an isometry $I : \mathcal{H} \to \mathcal{K}$ and a representation $\pi : G \to \mathcal{U}(\mathcal{K})$ such that $\|f(g) - I^*\pi(g)I\|_{hs}^2 \leqslant \epsilon$. The following state-dependent Gowers-Hatami theorem is due to Vidick [Vid18].

Theorem 5.1.3. *For any (ϵ, ρ)-homomorphism $f : G \to \mathcal{U}(\mathcal{H})$ of a finite group G on a finite-dimensional space $\mathcal{H}$, there exists a finite-dimensional Hilbert space $\mathcal{K}$, an isometry $I : \mathcal{H} \to \mathcal{K}$, and a representation $\pi : G \to \mathcal{U}(\mathcal{K})$ such that*

$$\|f(g) - I^*\pi(g)I\|_\rho^2 \leqslant \epsilon$$

for all $g \in G$.

Proof. We use $\{|g\rangle : g \in G\}$ to denote the canonical basis of $\ell^2(G)$. For every $g \in G$, the map $I_g := f(g) \otimes |g\rangle$ defines a linear map from $\mathcal{H} \to \mathcal{H} \otimes \ell^2(G)$ sending $|\psi\rangle \mapsto f(g)\,|\psi\rangle \otimes |g\rangle$ for all $|\psi\rangle \in \mathcal{H}$. Since $I_g^* I_g = f(g)^* f(g) = \mathbb{1}$ and $I_g^* I_h = 0$ for all $g \neq h$ in G,

$$I := \frac{1}{\sqrt{|G|}} \sum_{g \in G} I_g$$

is an isometry from $\mathcal{H} \to \mathcal{H} \otimes \ell^2(G)$. Let $R : G \to \ell^2(G)$ be the right regular representation. So $R(g)\,|h\rangle = |hg^{-1}\rangle$ for all $g, h \in G$. Then $\pi := \mathbb{1}_{\mathcal{H}} \otimes R$ defines a representation of G on $\mathcal{H} \otimes \ell^2(G)$ that satisfies

$$\begin{aligned}
f(g) - I^*\pi(g)I &= f(g) - \frac{1}{|G|} \sum_{h,k \in G} f(h)^* f(k)\, \langle h|\, R(g)\, |k\rangle \\
&= f(g) - \frac{1}{|G|} \sum_{h,k \in G} f(h)^* f(k)\, \langle h|kg^{-1}\rangle \\
&= \frac{1}{|G|} \sum_{h \in G} f(h)^* f(h) f(g) - \frac{1}{|G|} \sum_{h \in G} f(h)^* f(hg) \\
&= \frac{1}{|G|} \sum_{h \in G} f(h)^* \big(f(h)f(g) - f(gh)\big)
\end{aligned}$$

for all $g \in G$. Note that the ρ-norm $\|\cdot\|_\rho$ is left unitarily invariant and each $f(h)$ is unitary. It follows that

$$\begin{aligned}\|f(g) - I^*\pi(g)I\|_\rho^2 &= \frac{1}{|G|^2}\|\sum_{h\in G} f(h)^*\big(f(h)f(g) - f(gh)\big)\|_\rho^2 \\ &\leqslant \frac{|G|}{|G|^2}\sum_{h\in G}\|f(h)^*\big(f(h)f(g) - f(gh)\big)\|_\rho^2 \\ &= \mathbb{E}_{h\in G}\|f(g)f(h) - f(gh)\|_\rho^2 \leqslant \epsilon\end{aligned}$$

for all $g \in G$. □

Theorem 5.1.3 is a powerful tool in proving the robustness of self-testing: for some nonlocal game $\mathcal{G}$ with an associated group G, one can show that a near-optimal strategy S induces an approximate homomorphism f and the ideal optimal strategy $\widetilde{S}$ gives the exact representation π in Theorem 5.1.3. Then the desired local isometry $I_A \otimes I_B$ from S to $\widetilde{S}$ can be constructed from the isometry I in Theorem 5.1.3.

However, earlier approaches to proving the robustness using the above framework are often insufficient: the exact representation π given by Theorem 5.1.3 not only carries the ideal optimal strategy $\widetilde{S}$ but also contains some "junk strategies" that need to be disregarded. To tackle this problem, we state and prove an enhanced Gowers-Hatami theorem in Theorem 5.1.4 that allows us to construct an exact representation π containing the ideal model $\widetilde{S}$ exclusively. To motivate the proof approach, we first present a different proof of Theorem 5.1.3.

For any finite group G, we use $\mathrm{Irr}(G)$ to denote a complete set of inequivalent irreducible representations of G, where every $\varphi \in \mathrm{Irr}(G)$ is a (unitary) representation of G on $\mathbb{C}^{d_\varphi}$ for some $d_\varphi \geqslant 1$. Then

$$\ell^2(G) \cong \bigoplus_{\varphi\in\mathrm{Irr}(G)} \mathbb{C}^{d_\varphi} \otimes \mathbb{C}^{d_\varphi},$$

and the regular representation $R \cong \oplus_{\varphi\in\mathrm{Irr}(G)}\varphi^{\oplus d_\varphi}$. So

$$\sum_{\varphi\in\mathrm{Irr}(G)} d_\varphi \mathrm{Tr}\big(\varphi(g)\big) = \chi_R(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{otherwise,} \end{cases}$$

where χ_R is the character of the regular representation R. For any function $f : G \to \mathcal{U}(\mathcal{H})$ and any representation $\pi : G \to \mathcal{U}(\mathbb{C}^d)$, we define the *Fourier transform of f at π* to be the operator

$$\widehat{f}(\pi) := \mathbb{E}_{g\in G} f(g) \otimes \overline{\pi(g)}$$

acting on $\mathcal{H} \otimes \mathbb{C}^d$. Here $\overline{\pi(g)}$ denotes the entry-wise conjugate of the $d \times d$ matrix $\pi(g)$. The following proof was given by Vidick in [Vid18].

A second proof of Theorem 5.1.3. Let

$$\mathcal{K} := \mathcal{H} \otimes \left(\bigoplus_{\varphi\in \mathrm{Irr}(G)} \mathbb{C}^{d_\varphi} \otimes \mathbb{C}^{d_\varphi} \right) = \bigoplus_{\varphi\in \mathrm{Irr}(G)} \mathcal{H} \otimes \mathbb{C}^{d_\varphi} \otimes \mathbb{C}^{d_\varphi},$$

let $I : \mathcal{H} \to \mathcal{K}$ be the linear map sending

$$|\psi\rangle \mapsto \bigoplus_{\varphi\in \mathrm{Irr}(G)} \sqrt{d_\varphi} \sum_{i=1}^{d_\varphi} \Big(\widehat{f}(\varphi)\big(|\psi\rangle \otimes |i\rangle \big) \Big) \otimes |i\rangle,$$

and let

$$\pi := \bigoplus_{\varphi\in \mathrm{Irr}(G)} \mathbb{1}_{\mathcal{H}} \otimes \varphi \otimes \mathbb{1}_{\mathbb{C}^{d_\varphi}}$$

be a representation of G on $\mathcal{H}$. Then

$$\begin{aligned} I^*I &= \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \sum_{i=1}^{d_\varphi} \big(\mathbb{1}_{\mathcal{H}} \otimes \langle i| \big) \widehat{f}(\varphi)^* \widehat{f}(\varphi) \big(\mathbb{1}_{\mathcal{H}} \otimes |i\rangle \big) \\ &= \frac{1}{|G|^2} \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \sum_{g,h\in G} f(g)^* f(h) \mathrm{Tr}\left(\varphi(g)^T \overline{\varphi(h)} \right) \\ &= \frac{1}{|G|^2} \sum_{g,h\in G} f(g)^* f(h) \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \mathrm{Tr}\left(\varphi(g^{-1}h) \right) \\ &= \frac{1}{|G|} \sum_{g,h\in G} f(g)^* f(g) = \mathbb{1}_{\mathcal{H}}. \end{aligned}$$

So I is an isometry. Moreover, for any $g \in G$,

$$\begin{aligned} I^*\pi(g)I &= \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \sum_{i,j=1}^{d_\varphi} \langle i|\, \varphi(g)\, |j\rangle \big(\mathbb{1}_{\mathcal{H}} \otimes \langle i|\,\big) \widehat{f}(\varphi)^* \widehat{f}(\varphi) \big(\mathbb{1}_{\mathcal{H}} \otimes |j\rangle\big) \\ &= \frac{1}{|G|^2} \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \sum_{h,k\in G} f(h)^* f(k) \sum_{i,j=1}^{d_\varphi} \langle i|\, \varphi(g)\, |j\rangle \langle i|\, \varphi(h)^T \overline{\varphi(k)}\, |j\rangle \\ &= \frac{1}{|G|^2} \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \sum_{h,k\in G} f(h)^* f(k) \sum_{i,j=1}^{d_\varphi} \langle i|\, \varphi(g)\, |j\rangle \langle j|\, \varphi(k)^* \varphi(h)\, |i\rangle \\ &= \frac{1}{|G|^2} \sum_{h,k\in G} f(h)^* f(k) \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \mathrm{Tr}\big(\varphi(k^{-1}hg)\big) = \frac{1}{|G|} \sum_{h\in G} f(h)^* f(hg). \end{aligned}$$

This implies

$$f(g) - I^*\pi(g)I = \frac{1}{|G|} \sum_{h\in G} f(h)^* \big(f(h)f(g) - f(hg)\big).$$

The rest follows similarly as in the (first) proof of Theorem 5.1.3. □

In the above proof, the expressions of I^*I and $I^*\pi(g)I$ both contain $\widehat{f}(\varphi)^*\widehat{f}(\varphi)$ for $\varphi \in \mathrm{Irr}(G)$. In some cases, the approximate homomorphism f may satisfy some additional symmetry so that $\widehat{f}(\xi) = 0$ for some $\xi \in \mathrm{Irr}(G)$. When this happens, ignoring such a ξ in the construction of V and π would not affect the statement and the proof. This observation is crucial when we use the Gowers-Hatami theorem to prove many robust self-testing results.

Theorem 5.1.4. *For any (ϵ, ρ)-homomorphism $f : G \to \mathcal{U}(\mathcal{H})$ of a finite group G on a finite-dimensional space $\mathcal{H}$, there exists a finite-dimensional Hilbert space $\mathcal{K}$, an isometry $I : \mathcal{H} \to \mathcal{K}$, and a representation $\pi : G \to \mathcal{U}(\mathcal{K})$ such that*

(i) $\|f(g) - I^*\pi(g)I\|_\rho^2 \leqslant \epsilon$ *for all* $g \in G$, *and*

(ii) $\xi \in \mathrm{Irr}(G)$ *is an irreducible constituent of* π *only if* $\widehat{f}(\xi) \neq 0$.

Proof. Let

$$\mathcal{K} := \mathcal{H} \otimes \left(\bigoplus_{\substack{\varphi \in \mathrm{Irr}(G) \\ \widehat{f}(\varphi) \neq 0}} \mathbb{C}^{d_\varphi} \otimes \mathbb{C}^{d_\varphi} \right),$$

let $I : \mathcal{H} \to \mathcal{K}$ be the linear map sending

$$|\psi\rangle \mapsto \bigoplus_{\substack{\varphi \in \mathrm{Irr}(G) \\ \widehat{f}(\varphi) \neq 0}} \sqrt{d_\varphi} \sum_{i=1}^{d_\varphi} \Big(\widehat{f}(\varphi)\big(|\psi\rangle \otimes |i\rangle \big) \Big) \otimes |i\rangle,$$

and let

$$\pi := \bigoplus_{\substack{\varphi \in \mathrm{Irr}(G) \\ \widehat{f}(\varphi) \neq 0}} \mathbb{1}_{\mathcal{H}} \otimes \varphi \otimes \mathbb{1}_{\mathbb{C}^{d_\varphi}}$$

be a representation of G on $\mathcal{H}$. Then following the second proof of Theorem 5.1.3, we see

$$\begin{aligned}
I^*I &= \sum_{\substack{\varphi \in \mathrm{Irr}(G) \\ \widehat{f}(\varphi) \neq 0}} d_\varphi \sum_{i=1}^{d_\varphi} \big(\mathbb{1}_{\mathcal{H}} \otimes \langle i| \big) \widehat{f}(\varphi)^* \widehat{f}(\varphi) \big(\mathbb{1}_{\mathcal{H}} \otimes |i\rangle \big) \\
&= \sum_{\varphi \in \mathrm{Irr}(G)} d_\varphi \sum_{i=1}^{d_\varphi} \big(\mathbb{1}_{\mathcal{H}} \otimes \langle i| \big) \widehat{f}(\varphi)^* \widehat{f}(\varphi) \big(\mathbb{1}_{\mathcal{H}} \otimes |i\rangle \big) = \mathbb{1}_{\mathcal{H}}, \text{ and} \\
I^*\pi(g)I &= \sum_{\substack{\varphi \in \mathrm{Irr}(G) \\ \widehat{f}(\varphi) \neq 0}} d_\varphi \sum_{i,j=1}^{d_\varphi} \langle i| \varphi(g) |j\rangle \big(\mathbb{1}_{\mathcal{H}} \otimes \langle i| \big) \widehat{f}(\varphi)^* \widehat{f}(\varphi) \big(\mathbb{1}_{\mathcal{H}} \otimes |j\rangle \big) \\
&= \sum_{\varphi \in \mathrm{Irr}(G)} d_\varphi \sum_{i,j=1}^{d_\varphi} \langle i| \varphi(g) |j\rangle \big(\mathbb{1}_{\mathcal{H}} \otimes \langle i| \big) \widehat{f}(\varphi)^* \widehat{f}(\varphi) \big(\mathbb{1}_{\mathcal{H}} \otimes |j\rangle \big) = \frac{1}{|G|} \sum_{h \in G} f(h)^* f(hg).
\end{aligned}$$

So I is an isometry such that

$$\|f(g) - I^*\pi(g)I\|_\rho^2 \leqslant \epsilon.$$

Moreover, the representation π only has constituents $\xi \in \mathrm{Irr}(G)$ that satisfies $\widehat{f}(\xi) \neq 0$. □

5.2 Example: CHSH

In the CHSH game, the verifier samples a pair $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ uniformly at random. Upon receiving x and y, Alice and Bob return $a \in \mathbb{Z}_2$ and $b \in \mathbb{Z}_2$ respectively. They win if and only $a + b = x \cdot y$. The game polynomial of CHSH is given by

$$\Phi_{CHSH} := \frac{1}{2} + \frac{1}{4}(a_0 \otimes b_0 + a_0 \otimes b_1 + a_1 \otimes b_0 - a_1 \otimes b_1).$$

Here we use the convention that $a_x := m_0^x - m_1^x$ and $b_y := n_0^y - n_1^y$ for $x, y \in \{0, 1\}$. So a_x and b_y are binary observables in $\mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$. The quantum value of CHSH is $\frac{1}{2} + \frac{1}{2\sqrt{2}}$ and we have the following sum of squares decomposition

$$\frac{1}{2} + \frac{1}{2\sqrt{2}} - \Phi_{CHSH} = \left(a_0 \otimes 1 - 1 \otimes \frac{b_0 + b_1}{\sqrt{2}}\right)^2 + \left(a_1 \otimes 1 - 1 \otimes \frac{b_0 - b_1}{\sqrt{2}}\right)^2 \tag{5.2.1}$$

in $\mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes \mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$.

Now suppose $\widetilde{f}$ is an optimal state on $\mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes_{min} \mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$ for CHSH. Let $(\mathcal{H}, \pi, |\psi\rangle)$ be a GNS representation for $\widetilde{f}$, and let $A_x := \pi(a_x \otimes 1)$ and $B_y := \pi(1 \otimes b_y)$ for all $x, y \in \{0, 1\}$. Since $\widetilde{f}(\Phi_{CHSH}) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$, Equation (5.2.1) implies that

$$\left(A_0 - \frac{B_0 + B_1}{\sqrt{2}}\right)|\psi\rangle = \left(A_1 - \frac{B_0 - B_1}{\sqrt{2}}\right)|\psi\rangle = 0. \tag{5.2.2}$$

It follows that

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

For any monomial $w := a_{i_1} \cdots a_{i_k} \otimes b_{j_1} \cdots b_{j_\ell}$ in $\mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes \mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$, by Equation (5.2.2)

$$A_{i_1} \cdots A_{i_k} B_{j_1} \cdots B_{j_\ell} |\psi\rangle = B_{j_1} \cdots B_{j_\ell} \frac{B_0 + (-1)^{i_k} B_1}{\sqrt{2}} \cdots \frac{B_0 + (-1)^{i_1} B_1}{\sqrt{2}} |\psi\rangle \tag{5.2.3}$$

$$= A_{i_1} \cdots A_{i_k} \frac{A_0 + (-1)^{j_\ell} A_1}{\sqrt{2}} \cdots \frac{A_0 + (-1)^{j_1} A_1}{\sqrt{2}} |\psi\rangle \tag{5.2.4}$$

Hence by Equation (5.2.3),

$$(A_0A_1 + A_1A_0)\pi(w)\left|\psi\right\rangle = B_{j_1}\cdots B_{j_\ell}\frac{B_0 + (-1)^{i_k}B_1}{\sqrt{2}}\cdots\frac{B_0 + (-1)^{i_1}B_1}{\sqrt{2}}(A_0A_1 + A_1A_0)\left|\psi\right\rangle = 0$$

Since $\left|\psi\right\rangle$ is cyclic for π and w was arbitrary, we conclude that $A_0A_1 + A_1A_0 = 0$. Let D_4 be the rank-4 dihedral group with generators J, X, Z, subject to relations

- $J^2 = X^2 = Z^2 = 1$,
- J is central, and
- $XZ = JZX$.

Then there is a representation $\phi : D_4 \to \mathcal{U}(\mathcal{H})$ sending $J \mapsto -\mathbb{1}_{\mathcal{H}}, X \mapsto A_0$ and $Z \mapsto A_1$. The following property of D_4 is well-known.

Lemma 5.2.1. *The group D_4 has the following properties.*

(a) D_4 has a normal form $\mathcal{N}(w) = J^\alpha X^\beta Z^\gamma, \alpha, \beta, \gamma \in \{0, 1\}$. $|D_4| = 8$.

(b) $\mathrm{Irr}(D_4) = \{\chi_{ij} : i, j \in \{\pm 1\}\} \cup \{\sigma\}$ where each χ_{ij} is a character sending $J \mapsto 1, X \mapsto i, Z \mapsto j$, and σ is an irreducible representation of D_4 on $\mathbb{C}^2$ sending $J \mapsto -\mathbb{1}, X \mapsto \sigma_X, Z \mapsto \sigma_Z$. Here σ_X and σ_Z are the Pauli-X and Pauli-Z matrices.

(c) D_4 has a trace τ that satisfies $\tau(J) = -1$. This trace is given by $\tau(g) = \mathrm{tr}_2\left(\sigma(g)\right), g \in D_4$.

Given any words $w_1 = J^{\alpha_1}X^{\beta_1}Z^{\gamma_1}$ and $w_2 = J^{\alpha_2}X^{\beta_2}Z^{\gamma_2}$ in D_4, by Equation (5.2.3)

$$\begin{aligned}
\left\langle\psi\right|\phi(w_1w_2)\left|\psi\right\rangle &= (-1)^{\alpha_1+\alpha_2}\left\langle\psi\right|A_0^{\beta_1}A_1^{\gamma_1}A_0^{\beta_2}A_1^{\gamma_2}\left|\psi\right\rangle \\
&= (-1)^{\alpha_1+\alpha_2}\left\langle\psi\right|\left(\frac{B_0 - B_1}{\sqrt{2}}\right)^{\gamma_2}\left(\frac{B_0 + B_1}{\sqrt{2}}\right)^{\beta_2}A_0^{\beta_1}A_1^{\gamma_1}\left|\psi\right\rangle \\
&= (-1)^{\alpha_1+\alpha_2}\left\langle\psi\right|A_0^{\beta_2}A_1^{\gamma_2}A_0^{\beta_1}A_1^{\gamma_1}\left|\psi\right\rangle = \left\langle\psi\right|\phi(w_2w_1)\left|\psi\right\rangle.
\end{aligned}$$

So $w \mapsto \langle\psi|\,\phi(w)\,|\psi\rangle$ must be the unique trace τ on D_4 that sends $J \mapsto -1$. Equation (5.2.4) implies that the state $\widetilde{f}$ is completely determined by τ. We conclude that $\widetilde{f}$ is the unique optimal state on $\mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2} \otimes_{min} \mathcal{A}_{PVM}^{\mathbb{Z}_2,\mathbb{Z}_2}$ for CHSH. Lemma 5.2.1 and Equation (5.2.2) also illustrate a GNS representation $(\widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B, \widetilde{\pi}_A \otimes \widetilde{\pi}_B, |\widetilde{\psi}\rangle)$ for $\widetilde{f}$ where

- $\widetilde{\mathcal{H}}_A = \widetilde{\mathcal{H}}_B = \mathbb{C}^2$,
- $\widetilde{\pi}_A$ sends $a_0 \mapsto \sigma_X, a_1 \mapsto \sigma_Z$,
- $\widetilde{\pi}_B$ sends $b_0 \mapsto \frac{\sigma_X+\sigma_Z}{\sqrt{2}}, b_1 \mapsto \frac{\sigma_X-\sigma_Z}{\sqrt{2}}$, and
- $|\widetilde{\psi}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

Let $\widetilde{A}_0 := \sigma_X$, $\widetilde{A}_1 := \sigma_Z$, $\widetilde{B}_0 = \frac{\sigma_X+\sigma_Z}{\sqrt{2}}$, and $\widetilde{B}_1 := \frac{\sigma_X-\sigma_Z}{\sqrt{2}}$. Then CHSH is a self-test for its optimal quantum strategies with an ideal optimal strategy

$$\widetilde{S} := \big(\widetilde{\mathcal{H}}_A, \widetilde{\mathcal{H}}_B, \{\widetilde{A}_0, \widetilde{A}_1\}.\{\widetilde{B}_0, \widetilde{B}_1\}, |\widetilde{\psi}\rangle\big).$$

Let $\widetilde{\pi} := \widetilde{\pi}_A \otimes \widetilde{\pi}_B$. Then

$$\begin{aligned}\widetilde{\pi}(\Phi_{CHSH}) &= \frac{1}{2} + \frac{\sqrt{2}}{4}(\sigma_X \otimes \sigma_X + \sigma_Z \otimes \sigma_Z) \\ &= \frac{1}{2} + \frac{\sqrt{2}}{4}\big(\,|00\rangle + |11\rangle\,\big)\big(\,\langle 00| + \langle 11|\,\big) - \frac{\sqrt{2}}{4}\big(\,|01\rangle - |10\rangle\,\big)\big(\,\langle 01| - \langle 10|\,\big).\end{aligned}$$

So the spectral gap Δ_{CHSH} of $\widetilde{\pi}(\Phi_{CHSH})$ is $\frac{\sqrt{2}}{2}$.

Next, use the enhanced Gowers-Hatami theorem to derive the robustness of this self-test.

Proposition 5.2.2. *CHSH game is a robust self-test for its optimal quantum strategies with robustness $\eta(\epsilon) = O(\sqrt{\epsilon})$.*

Proof. Suppose

$$S = (\mathcal{H}_A, \mathcal{H}_B, \{A_0, A_1\}, \{B_0, B_1\}, |\psi\rangle).$$

is a projective ϵ-optimal strategy for CHSH where $\epsilon \geqslant 0$. Let $\rho_A := \mathrm{Tr}_{\mathcal{H}_B}\big(|\psi\rangle\langle\psi|\big)$ and $\rho_B := \mathrm{Tr}_{\mathcal{H}_A}\big(|\psi\rangle\langle\psi|\big)$.

Claim 5.2.3. $\|A_0A_1 + A_1A_0\|_{\rho_A} \leqslant 6\sqrt{\epsilon}$.

Proof of Claim 5.2.3. Let $r_0 := A_0 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0+B_1}{\sqrt{2}}$ and $r_1 := A_1 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0-B_1}{\sqrt{2}}$. Then

$$\epsilon = \frac{1}{2} + \frac{1}{2\sqrt{2}} - w(CHSH; S) = \frac{1}{8\sqrt{2}}\left(\|r_0|\psi\rangle\|^2 + \|r_1|\psi\rangle\|^2\right).$$

Observe that $(A_0A_1 + A_1A_0) \otimes \mathbb{1} = s_1r_0 + s_0r_1$ where $s_0 := A_0 \otimes \mathbb{1} + \mathbb{1} \otimes \frac{B_0+B_1}{\sqrt{2}}$ and $s_1 := A_1 \otimes \mathbb{1} + \mathbb{1} \otimes \frac{B_0-B_1}{\sqrt{2}}$. Since both s_0 and s_1 have operator norm $\leqslant 1 + \sqrt{2}$,

$$\begin{aligned}\|A_0A_1 + A_1A_0\|^2_{\rho_A} &= \|(A_0A_1 + A_1A_0) \otimes \mathbb{1}|\psi\rangle\|^2 \leqslant \left(\|s_1\|_{op}\|r_0|\psi\rangle\| + \|s_0\|_{op}\|r_1|\psi\rangle\|\right)^2 \\ &\leqslant \frac{(1+\sqrt{2})^2}{2}\left(\|r_0|\psi\rangle\|^2 + \|r_1|\psi\rangle\|^2\right) = 4\sqrt{2}(1+\sqrt{2})^2\epsilon \leqslant 36\epsilon.\end{aligned}$$

So the claim follows. □

Now let f be the function from $D_4 \to \mathcal{U}(\mathcal{H}_A)$ sending

$$J^\alpha X^\beta Z^\gamma \mapsto (-1)^\alpha A_0^\beta A_1^\gamma$$

for every $\alpha, \beta, \gamma \in \{0, 1\}$.

Claim 5.2.4. *f is a $(36\epsilon, \rho_A)$-homomorphism of D_4.*

Proof of Claim 5.2.4. Observe that for any $g, h \in D_4$, $f(g)f(h) - f(gh)$ is either 0 or $U(A_0A_1 + A_1A_0)$ for some unitary U. Since the ρ_A-norm is left unitarily invariant, it follows that $\|f(g)f(h) - f(gh)\|_{\rho_A} \leqslant \|A_0A_1 + A_1A_0\|_{\rho_A}$ for all $g, h \in D_4$. So the claim follows from Claim 5.2.3. □

Claim 5.2.5. *There is an isometry $I_A : \mathcal{H}_A \to \mathbb{C}^2 \otimes \mathbb{C}^k$ such that*

$$\delta_x^A := \|A_x - I_A^*\left(\widetilde{A}_x \otimes \mathbb{1}_{\mathbb{C}^k}\right)I_A\|_{\rho_A} \leqslant 6\sqrt{\epsilon}$$

for all $x \in \{0, 1\}$.

Proof of Claim 5.2.5. For any one-dimensional irreducible representation ξ of D_4,

$$2\widehat{f}(\xi) = \sum_{g\in D_4} \xi(g)f(g) + \sum_{g\in D_4} \xi(Jg)f(Jg) = \sum_{g\in D_4} \xi(g)f(g) - \sum_{g\in D_4} \xi(g)f(g) = 0.$$

So by Claim 5.2.4 and Theorem 5.1.4, there is an isometry $V_A : \mathcal{H} \to \mathcal{K}$ and a representation $\pi : D_4 \to \mathcal{U}(\mathcal{K})$ such that

$$\|f(g) - V_A^*\pi(g)V_A\|_{\rho_A} \leqslant 6\sqrt{\epsilon}$$

for all $g \in G$, and none of the one-dimensional representations of D_4 is a constituent of π. The latter condition implies that π is equivalent to a direct sum of σ's. In other words, there is a unitary $U : \mathcal{K} \to \mathbb{C}^2 \otimes \mathbb{C}^k$ such that $\pi(g) = U^*\big(\sigma(g) \otimes \mathbb{1}_{\mathbb{C}^k}\big)U$ for all $g \in D_4$. Then $I_A := UV_A$ is an isometry from $\mathcal{H} \to \mathbb{C}^2 \otimes \mathbb{C}^k$ such that

$$\|f(g) - I_A^* \left(\sigma(g) \otimes \mathbb{1}_{\mathbb{C}^k}\right) I_A\|_{\rho_A} \leqslant 6\sqrt{\epsilon}.$$

Taking $g = X$ and Z completes the proof. □

Similarly, there is an isometry $I_B : \mathcal{H}_B \to \mathbb{C}^2 \otimes \mathbb{C}^s$ such that

$$\delta_y^B := \|B_y - I_B^* \left(\widetilde{B}_y \otimes \mathbb{1}_{\mathbb{C}^s}\right) I_B\|_{\rho_B} \leqslant 6\sqrt{\epsilon}$$

for all $y \in \{0, 1\}$.

Claim 5.2.6. *There is a unit vector $|\kappa\rangle \in \mathbb{C}^k \otimes \mathbb{C}^s$ such that*

$$\|I_A \otimes I_B |\psi\rangle - |\widetilde{\psi}\rangle \otimes |\kappa\rangle\| \leqslant 26\sqrt{\epsilon}, \text{ and}$$
$$\|I_A \otimes I_B\big(A_x \otimes B_y |\psi\rangle\big) - \big(\widetilde{A}_x \otimes \widetilde{B}_y |\widetilde{\psi}\rangle\big) \otimes |\kappa\rangle\| \leqslant 38\sqrt{\epsilon}$$

for all $x, y \in \{0, 1\}$.

Proof of Claim 5.2.6. Since $\delta := \frac{1}{4}(2\delta_0^A + 2\delta_1^A + 2\delta_0^B + 2\delta_1^B) \leqslant 12\sqrt{\epsilon}$. By Proposition 4.2.13,

$$\|I_A \otimes I_B |\psi\rangle - |\widetilde{\psi}\rangle \otimes |\kappa\rangle\| \leqslant \frac{\sqrt{2}\big(\delta + \sqrt{\epsilon}\big)}{\Delta_{CHSH}} \leqslant 26\sqrt{\epsilon}, \text{ and}$$
$$\|I_A \otimes I_B\big(A_x \otimes B_y |\psi\rangle\big) - \big(\widetilde{A}_x \otimes \widetilde{B}_y |\widetilde{\psi}\rangle\big) \otimes |\kappa\rangle\| \leqslant \delta_x^A + \delta_y^B + \frac{\sqrt{2}\big(\delta + \sqrt{\epsilon}\big)}{\Delta_{CHSH}} \leqslant 38\sqrt{\epsilon}$$

for all $x, y \in \{0, 1\}$. □

Claim 5.2.6 implies that for any $\epsilon \geqslant 0$ and any ϵ-optimal projective quantum strategy S for CHSH, one has $S \succeq_{38\sqrt{\epsilon}} \widetilde{S}$. Then by [BCK+23, Theorem 4.3], taking $\eta(\epsilon) = 5 \times 38\sqrt{\epsilon} = 180\sqrt{\epsilon}$ completes the proof. □

Chapter 6

Quantum delegation and quantum proofs

6.1 Context and overview

As introduced in Section 1.2, we are interested in modeling near-term proof verification and delegation of quantum computations. To this end, we propose a new paradigm that is particularly relevant to the quantum scenario: a verifier having access to an off-the-shelf (OTS) device.

To motivate our OTS model, consider that the complexity class QMA models a verifier having access to fully-trusted polynomial-time quantum computation. While such a verifier is *skeptical* of the prover (and thus needs to verify the claimed proof independently), in the quantum case, a new level of skepticism is possible, namely that the verifier's quantum processing is untrusted. A common solution in this case is to postulate *two* (or more) untrusted and all-powerful devices together with a classical verifier; this is the realm of MIP*. In this chapter, we propose a new paradigm that treats the provers asymmetrically. Starting with a conventional two-prover interactive proof system, we ask that only *one* of the provers do the heavy lifting (via its unbounded computational capabilities), with the second prover becoming efficient and completely generic (for completeness, this prover need

not even be given a description of the task at hand; soundness, however, is shown against *two* unbounded provers).

We first give an overview of background material, together with a summary of the current state-of-the-art approaches to interactive proof systems and delegated computation in the quantum setting, focusing on elements that are relevant to our main questions, and highlighting where existing approaches fail in their applicability to our scenario.

Classical and quantum interactive proof systems

In the model of interactive proof systems (IP), an efficient classical verifier interacts with an all-powerful and untrusted prover in order to verify the correctness of a statement [GMR89]. We note that class NP corresponds to a single-message interaction (with MA being in probabilistic version), while AM incorporates a single round (*i.e.*, *two* messages).

In *a multiprover interactive proof system* (MIP), a verifier interacts with multiple isolated provers [BGKW88]. Each of the models above has been *quantized*, *i.e.,* extended to the setting where some (or all) of the parties are quantum. This is captured, *e.g.* by the classes QMA (the quantum version of MA), QIP (the quantum version of IP) and MIP^* (a version of a multi-prover interactive proof system (MIP) where the unbounded provers share entanglement). Groundbreaking results have characterized some these quantum classes, *e.g.* $\mathsf{QIP} = \mathsf{PSPACE}$ [JJUW11] and $\mathsf{MIP}^* = \mathsf{RE}$ [JNV+20].

Zero-knowledge

A strong motivation for the study of interactive proof systems is the connections to the counter-intuitive concept of a zero-knowledge proof system [GMW91, BGG+90]. Informally, a proof system is *zero-knowledge* when the verifier is unable to learn anything beyond the fact that the agreed-upon instance is true. This is more formally treated by establishing the existence of a *simulator* which can reproduce the transcript of the interaction.

Zero-knowledge proof systems were first extended to the quantum setting by Watrous [Wat09], who considered the setting where the verifier has access to a trusted polynomial-

time quantum device. Subsequently, it was shown that under certain cryptographic assumptions, all problems in QMA admit a zero-knowledge proof system [BJSW16, BJSW20, BG22] (again, assuming the verifier has trusted polynomial-time quantum computation). There have been several approaches in the case of a fully classical verifier. Vidick and Zhang showed that argument protocols can be made to satisfy the zero-knowledge property [VZ20]. Recent work by Crépeau and Stuart [CS23] provides a two-prover one-round zero-knowledge proof system for NP. The work of Chiesa, Forbes, Gur and Spooner provides a two-prover zero-knowledge proof system for NEXP [CFGS18], however, their work requires polynomially many rounds of interaction. Work due to Grilo, Yuen, and Slofstra [GSY19] shows that any proof system for MIP^* can be made zero-knowledge at the cost of adding four additional provers. Although these works provide inspiration for studying zero-knowledge proof systems in the OTS model, as far as we are aware, they do not directly contribute to our main question on ZK. In fact, according to the current state-of-the-art, an implicit open question [Gri19] is the following: *"Does there exists a* relativistic *zero-knowledge proof system for* QMA *with two provers and a classical verifier?"*. We emphasize that our OTS model takes this question further, by requiring one of the provers to operate generically and independently of the problem instance.

Delegation of quantum computations

Delegated quantum computation allows a computationally-weak classical client to delegate a computational task to an untrusted, polynomial-time quantum server. Under certain conditions, an interactive proof system leads in a straightforward way to a protocol for delegated quantum computation. Typically, this is achieved if the interactive proof system captures *e.g.* QMA, and furthermore, given the witness, the prover is efficient; it is also relevant that the QMA witness is used in such a way that we can scale down the proof system in order to achieve a delegation protocol for BQP (*e.g.* [Gri19])[1]. The sketch above is also applicable to the scenario of multiple servers. Note that because of the resemblance between the models of the interactive proof system and delegated quantum computation,

[1] BQP is closed under complementation, hence this is sufficient for delegation

we occasionally confound the two — using the complexity class acronym to refer to the interaction pattern between prover(s) and verifier — but we emphasize that in delegated quantum computation *protocols*, the server is always computationally bounded (as opposed to a prover in interactive *proof systems*).

Following Reichardt, Unger, and Vazirani [RUV13], who showed a delegated quantum computation for the setting of MIP^*, much progress was made, aiming at improving parameters and techniques; despite these efforts, as far as we are aware, none of the existing works are applicable to our model. Notable here is the work of [CGJV19] which uses *quasi-linear* resources for *both* servers, and achieves at best a constant round complexity, as well as [Gri19] which is the first 2-server, 1-round (relativistic) protocol for delegated quantum computations, but uses the full polynomial-power of both servers.

We note that in the protocol of [RUV13], as well as for most of the related works, we have the property that the protocol for delegated quantum computation can be *scaled up* to an interactive proof system for QMA in the following way. We let the unbounded prover derive a QMA witness, then apply the delegation protocol for the circuit of the QMA verifier, where the *other* prover does the computation on the witness, as teleported by the initial prover (and where the outcome of the teleportation measurement is reported to the verifier). In this way, we can closely relate interactive proof systems for QMA with two-prover protocols for delegated quantum computations.

Simulatable codes

Recent works by Grilo, Yuen, and Slofstra [GSY19], as well as Broadbent and Grilo [BG22] introduce the notion of simulatable codes as a tool for establishing zero-knowledge proof systems and protocols in the quantum setting. The idea is to use techniques from quantum error-correcting codes to create a "simulatable" witness or proof for use in the verification process. Here the witness is *simulatable* in the sense that there is an efficient classical algorithm that can reproduce the description of the local density matrix of the witness on any small enough subspace. This is a pivotal tool in establishing zero-knowledge, and the application of the technique consists in developing a verification protocol, (or verification

circuit in the case of [BG22]) which verifies such simulatable witnesses; this can then be applied to the situation of encoding *e.g.*, a witness for QMA into a simulatable code [BG22].

We note that the full power of simulatable codes is best appreciated when thinking of them as for encoding a quantum state: thanks to such codes, we achieve a situation where local descriptions are easy to compute, while *global* correlations might be hard — a situation that has no classical equivalent since a series of local descriptions trivially define a global description.

6.1.1 Summary of results

We denote OTS the set of all languages L that can be decided under a constant completeness-soundness gap, in the model that follows. Before the instance $x \in L$ is selected, the classical verifier is provided with an untrusted off-the-shelf device which only depends on a parameter n, indicating the size of the problem instance (without loss of generality, we can assume that the prover provides such OTS device). For completeness, such a device shares an entangled state $|\psi\rangle_n$ with a quantum prover and will be purported to perform efficient measurements from a predetermined list of available options. The verifier may select any choice $x \in L$ provided $|x| \leqslant n$ and *simultaneously* uses a single question to the prover and to the device; the verifier then determines whether or not to accept based on the responses. We stress that OTS proof systems are sound against both an unbounded prover and unbounded OTS.

We observe that OTS is a refinement of and thus contained in MIP^*. In the other direction, the OTS model is a generalization of AM, where the otherwise classical verifier has additional 1-round query access to a small, off-the-shelf quantum device. In summary, we have the following straightforward containments (see also Figure 6.1)

$$\mathsf{AM} \subseteq \mathsf{OTS} \subseteq \mathsf{MIP}^* \tag{6.1.1}$$

In a classical proof system, an OTS can be understood as an instance-independent hardware token. This device can be used to provide a commitment for a zero-knowledge

proof system for NP [GMW91]; what is more, the one-time property of the OTS can be used as an oblivious transfer device, which then yields a non-interactive zero-knowledge proof system for NP [Kil88]. We note that in the quantum case, our model requires a fully classical verifier and hence the case of zero-knowledge for QMA [BJSW16, BG22] in the OTS model is much more complex, and a classical-verifier analogue to the NP proof systems above is not directly applicable. Other approaches based on using the OTS as a one-time memory [BGS13] also run into a roadblock due to the fact that we require a fully classical verifier.

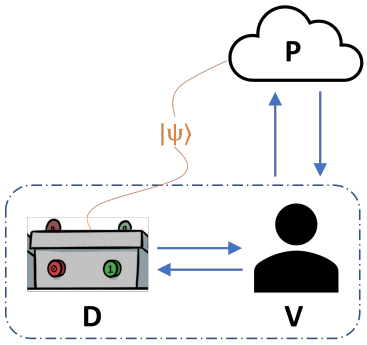


Figure 6.1: Off-the-shelf (OTS) proof system. P is the quantum prover, V is the classical verifier, and D a rudimentary off-the-shelf-device; each arrow represents a single classical message. We can interchangeably think of the model as a strengthening of the verifier in AM (V having access to an additional OTS device D), or a weakening of MIP* (one of the provers, D, is severely restricted).

OTS proof systems for QMA

Our first result is that any language in QMA is also in OTS.

Theorem 6.1.1. *(Restated as part of Theorem 6.5.2)* $\mathsf{QMA} \subseteq \mathsf{OTS}$.

An interpretation of this result is that starting with a conventional proof system for QMA, we can exchange the unwavering trust of the verifier in its quantum verification

process for a classical verifier with two new features: (1) the verifier has access to an untrusted, and instance-independent, off-the-shelf quantum device; and (2) the verifier interacts with the prover (and the device) in a single simultaneous round.

Zero-knowledge OTS proof system for QMA

What is more, we show that the OTS proof system for QMA is also *statistical zero-knowledge*, meaning that we can simulate in classical polynomial time the verifier's transcript when interacting with the provers on a yes-instance.

Theorem 6.1.2. *(Restated in Theorem 6.5.2) For every language L in* QMA*, there exists a statistical zero-knowledge OTS proof system for L.*

Delegated quantum computation in the OTS model

As our final conceptual contribution, we show how our OTS proof system for QMA (Theorem 6.1.1) can be adapted to the setting of delegated quantum computation (see Section 6.1); note that the ZK property as described above also extends to the delegated quantum computation paradigm.

Theorem 6.1.3. *(Restated as Theorem 6.5.3)* BQP *has a relativistic delegated quantum computation protocol in the OTS model with the statistical zero-knowledge property.*

We believe that this result is of particular impact since it addresses a new model for delegated quantum computation that has distinct conceptual benefits over existing delegation protocols:

1. Comparing our delegated quantum computation protocol to single-server protocols, we note that we make an extra assumption of an off-the-shelf, isolated device. However, the benefits are:

   (a) We achieve soundness against an unbounded server; existing single-server, classical-client delegation protocols require computational assumptions [Mah18].

(b) The client does not trust *any* quantum device at all; existing single-server, statistically secure protocols for delegated quantum computation require trust in a small quantum preparation device [Bro18, FK17].

2. Comparing our delegated quantum computation protocol to existing multiple-server (MIP^*) protocols, we note that:

   (a) Our approach only requires a single high-performance quantum server that handles the bulk of the computations; with a secondary efficient and generic device which need not even be given a description of the problem instance. This has practical advantages, especially when we consider that the off-the-shelf device can be acquired ahead of the verification stage (Figure 1.2).

   (b) Our approach is a single round, which means that relativistic means to enforce isolation are possible. The only other known relativistic protocol requires full quantum computational power for both servers and is not ZK [Gri19].

6.1.2 Proof approach

We now give an overview of the approach toward proving our main results.

Obstructions to the straightforward approach

In delegating quantum computations in two- or multi-server models, the classical verifier is able to command quantum provers [RUV13] using two intertwined tests: (1) a computational test, with acceptance probability based on the required quantum computation (*e.g.*, computation-by-teleportation [RUV13] or energy checking of a local Hamiltonian [Ji17, Gri19]); (2) a rigidity test, ensuring provers' actions stay within a known range (*e.g.*, self-test via CHSH game or Pauli braiding test). In order to establish the ZK property, we must show that responses from the provers can be simulated using a classical probabilistic polynomial-time (PPT) device. Generally, approaches used for the rigidity test can be

simulated in a straightforward way, hence the difficulty in obtaining ZK in this setting is in simulating the energy test. Furthermore, even if both tests are simulatable in isolation, this does not guarantee the ZK property since a malicious verifier may form question pairs emanating from different tests, during a single round.

Grilo [Gri19] presents a game $\mathcal{G}(H)$ determined by an "XZ-type"[2] Hamiltonian H. Honest provers for this game share suitably many EPR pairs, and one prover privately holds a ground state for H. The game $\mathcal{G}(H)$ combines an energy test with the Pauli braiding test [NV17, Vid18]. During the energy test, one prover reports measurement results of a randomly chosen term H_i on their side of EPR pairs, and the other provides teleportation keys from a Bell basis measurement on the other EPR pairs and the ground state. Combining the energy test with the Pauli braiding test allows the verifier to ensure that provers share n EPR pairs and that the required Pauli-X/Pauli-Z measurements are performed when measuring the local term H_i.

The straightforward approach to obtaining a two-prover ZK proof system would be to combine recent results on simulatable codes in order to make the measurement results in Grilo's energy test simulatable. More specifically, one could apply the well-known circuit-to-Hamiltonian construction using the family of simulatable verification circuits given in [BG22]. Given such a circuit V, it is shown that local measurements on the ground state of the corresponding Hamiltonian H_V are simulatable and thus this approach would make the results of the energy test simulatable. Unfortunately, this approach fails for two technical reasons.

The choice of encoding. Firstly, one cannot employ previously-known self-testing techniques to show the players perform the required measurements on the simulatable ground states given in [BG22]. On the one hand, previously-studied single-round self-testing techniques can only be used to show the players perform Pauli-X, and Pauli-Z measurements. On the other hand, the choice of physical gates used by Broadbent and Grilo during the

[2]These are Hamiltonians where each local term H_i is a real linear combination of tensor products of the Pauli-X and Pauli-Z operators.

encoding of logic gates may result in a local Hamiltonian that is not of XZ-type and thus local terms H_i may require measurements that have no known self-test.

The size of the measurement. The second obstruction arises from the fact that existing rigidity tests in this setting require both players to make large-sized measurements on their shared state. These large measurements can provide an avenue for attack by a malicious verifier which compromises the zero-knowledge property. In particular, since the Pauli braiding test allows for requests for measurements on all qubits, a malicious verifier may indicate to one player that an energy test is being played and simultaneously request Pauli-X and Pauli-Z measurements on a large number of qubits. Such a measurement result cannot be simulated using simulatable codes, which only protect against constant-sized measurements, and thus this compromises zero-knowledge.

Overview of proof and technical results

In order to correct for an appropriate choice of encoding, we prove that one can re-instantiate the verification circuit given by Broadbent and Grilo using an approach to simulatable codes given in [GSY19]. This change allows us to encode logical gates of the verification circuit given by Broadbent and Grilo using a different set of physical gates and consequently, we show that the local Hamiltonian corresponding to the circuit is of XZ-type, while preserving simulatability.

Theorem 6.1.4 (Informal version of Theorem 6.4.1)**.** *For any language $L = (L_{yes}, L_{no})$ in* QMA*, there is a family of verification circuits V_x satisfying (1) the circuit-to-Hamiltonian construction applied to V_x produces a Hamiltonian H_x which is of XZ-type, and (2) if $x \in L_{yes}$ there exists a polynomial-time algorithm that can approximate the reduced density matrix obtained by tracing out all but 6 qubits of the ground state of H_x.*

In order to overcome the large measurement problem, we introduce a new nonlocal game called the *low-weight Pauli braiding test* (LWPBT) which can self-test the low-weight tensor

products of Pauli measurements and n EPR pairs but only requires the players to make measurements on a constant number of qubits.

Theorem 6.1.5 (Informal version of Theorem 6.2.12)**.** *The low-weight Pauli braiding test can self-test for n EPR pairs and 6-qubit Pauli measurements. This self-test is robust with robustness $poly(n)\epsilon^{1/4}$.*

We use the group-theoretical approach developed in the previous chapter to prove the robustness of the LWPBT. Here, we briefly describe the challenges associated with achieving this result. We first recall the notation of approximate representations and approximate homomorphisms for groups. Informally, given a group presentation $\langle S : R \rangle$ for a group G, a map $f : S \to \mathcal{U}$ from the generating set S to the set of unitary operators $\mathcal{U}$ is called an *ϵ-representation* if it respects the relations in R, up to error ϵ. The more general notion of an *ϵ-homomorphism* refers to a map $f : G \to \mathcal{U}$ that respects the multiplication of elements in the group, up to error ϵ. When $\epsilon = 0$, these two notions coincide. The well-known Gowers-Hatami theorem [GH17] states that every approximate homomorphism of a finite group must be close to an exact homomorphism.

Implicitly in [Vid18] for the robustness of the n-qubit Pauli braiding test, a presentation is taken for the n-qubit Weyl-Heisenberg group which has $exp(n)$ generators subject to $exp(n)$ relations. It is then shown that any ϵ-perfect strategy forms an $O(\sqrt{\epsilon})$-approximate representation, and given the large presentation one can straightforwardly show that this approximate representation is indeed an $O(\sqrt{\epsilon})$-approximate homomorphism.

The analysis of the LWPBT requires a presentation for the n-qubit Weyl-Heisenberg group with only $poly(n)$ generators and $poly(n)$ relations. Having fewer generators and relations makes the rigidity analysis more technical. In particular, to show that the approximate representation given by a near-perfect strategy is indeed an approximate homomorphism, we need to specify a normal form of the Weyl-Heisenberg group with respect to this "small" presentation and find a rewriting procedure that takes arbitrary words of the group into its normal form. This allows us to track the precise error bounds on the approximate homomorphism we obtain and conclude that any ϵ-perfect strategy forms a $poly(n)\sqrt{\epsilon}$-approximate homomorphism.

In order to finally round an approximate homomorphism to an exact homomorphism, we use the enhanced version of the Gowers-Hatami theorem (Theorem 5.1.4) introduced in the previous chapter to analyze the stability of the Weyl-Heisenberg group with respect to the "small" presentation described above.

We use the above technical results to derive a modified version of [Gri19] by interleaving the following tests: (1) a computational test consisting of an energy test in which a simulatable witness uses low-weight Pauli-X and Pauli-Z measurements and, (2) a rigidity test consisting of the LWPBT. The result of this modified Grilo protocol gives a ZK OTS protocol with an inverse polynomial completeness-soundness gap. Finally, we apply a threshold parallel repetition theorem to the above protocol to amplify the completeness-soundness gap to be constant, thus demonstrating both Theorem 6.1.1 and Theorem 6.1.2. We then show that the proof system is of a form that can be scaled down to yield a delegation protocol, yielding Theorem 6.1.3.

6.1.3 Open problems

In this chapter, we show that the OTS model displays many interesting properties that are related to both the single- and multi-prover models for interactive proofs. We believe that there is tremendous scope for further investigation of the model, and also that our novel techniques will find applications elsewhere. We collect some open problems below.

Do both provers need to be all-powerful to recover MIP^*? Our results show that $\mathsf{QMA} \subset \mathsf{OTS}$. We leave it as an open question to determine if the same can be said about larger complexity classes such as QIP. Going further, perhaps one can characterize how powerful the untrusted set-up device needs to be in order to recover all of MIP^*. More specifically, if we allow the untrusted device to make arbitrary measurements but still require independence from the input, would we be able to recover MIP^*? Somewhat dual to this question would be to ask if one can prove a natural upper bound for our new model. One plausible candidate would be the class QIP but even this is not immediately

straightforward if only for the reason that the off-the-shelf device may share arbitrary amounts of entanglement with the prover.

Applications to proofs of quantum knowledge. As an extension to the concept of ZK, in a *proof of knowledge (PoK)*, the verifier further becomes convinced that the prover has "knowledge" of an accepting witness. This is formally treated by showing the existence of an efficient *knowledge extractor* which outputs a witness given oracle access to the prover; this concept has recently been extended to the quantum setting [BG22], [CVZ19]. We conjecture that the assurances given by self-testing provide a different approach to convincing the verifier that the prover(s) are in possession of an actual quantum witness; it may be possible to refine our approach to self-testing by showing the result for a more complete game. Namely, we leave it as an open question to find a 2-prover, 1-round protocol that self-tests for ground states of a local Hamiltonian, and to determine how this yields a new approach to a quantum PoK.

OTS devices for delegated quantum computation. We have shown that the OTS model is powerful enough for the delegated quantum computations of BQP; while it seems unlikely that we can do away with the OTS device completely [ACGK19], an open question is to determine the *minimal* power required by this device (assuming $\mathsf{BQP} \neq \mathsf{BPP}$).

Further uses and refinements of the LWPBT. We believe the new LWPBT may be more widely applicable since it may be further generalized to provide a straightforward tradeoff of question/answer size for robustness in a self-test for EPR pairs and Pauli measurements. For example, one may analyze the same game as in our main result, but allow for measurements of size $\log(n)$ instead of constant. We leave for future work the study of this model and its consequences.

Further Applications. There are a variety of interesting applications and considerations made of interactive proof systems in the quantum setting aside from the ones that

we studied. Recent works have introduced the notion of state/unitary complexity classes [RY22]. Informally, the approach is to study the ability of an efficient quantum verifier to output a target quantum state, given access to an untrusted quantum prover. Similar considerations can be made in our OTS model, in which a classical verifier may want to certify the existence of a target state on the register of the untrusted set-up device.

6.1.4 Notation and preliminaries

In this chapter, we use $\|\cdot\|_{tr}$ to denote the trace norm defined by $\|A\|_{tr} := \mathrm{Tr}\sqrt{A^*A}$ for any matrix A. All Hilbert spaces are assumed to be finite-dimensional. Given two quantum states ρ and σ on a Hilbert space $\mathcal{H}$, we define their trace distance $D(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_{tr} = \max_P \mathrm{Tr}(P(\rho-\sigma))$ where the max is taken over all projections $P \in \mathcal{B}(\mathcal{H})$.

We use $|\Phi_{\mathrm{EPR}}\rangle$ to denote the EPR pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ in $\mathbb{C}^2 \otimes \mathbb{C}^2$ and use $|\Phi_{\mathrm{EPR}}^{\otimes n}\rangle$ to denote the n-qubit EPR pair. Recall that we take σ_I, σ_X, and σ_Z to denote the following Pauli operators:

$$\sigma_I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \text{ and } \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{6.1.2}$$

For every $a \in \{0,1\}^n$ and $W \in \{I,X,Z\}^n$, we use $\sigma_W(a)$ to denote the operator $\otimes_{i\in[n]}\sigma_{W_i}^{a_i}$ on $(\mathbb{C}^2)^{\otimes n}$ where $\sigma_I^0 = \sigma_X^0 = \sigma_Z^0 = \sigma_I$.

All quantum strategies for nonlocal games are assumed to be projective in this chapter. We often use $\mathcal{S} = \big(\tau_A, \tau_B, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B\big)$ to denote a quantum strategy. Here τ_A is a map from Alice's question set $\mathcal{I}_A$ to operators on $\mathcal{H}_A$, sending $x \in \mathcal{I}_A$ to the observable of Alice that corresponds to x.

Recall that a quantum error-correcting code (QECC) $\mathcal{C} = [[n,k]]$ is a map $\mathrm{Enc} : (\mathbb{C}^2)^{\otimes k} \to (\mathbb{C}^2)^{\otimes n}$, which encodes a k-qubit state $|\psi\rangle$ into an n-qubit state $\mathrm{Enc}(|\psi\rangle)$ where $n \geqslant k$. The code is said to have distance d if the original state can be recovered from the encoded state that has transformed under any quantum operation which acts on at most $(d-1)/2$ qubits. Given an $[[m,1]]$ QECC with map Enc, we abuse notation and also write Enc for the corresponding $[[mn,n]]$ encoding that is obtained by applying Enc to each of the qubits in an n-qubit system.

We use $\underline{A}_n^k$ to denote the set of k distinct numbers between 1 and n through this section. Then $\underline{A}^k := \bigcup_{n \geqslant k} \underline{A}_n^k$ is the set of k distinct numbers. Given a k-qubit logical gate U and an element $\underline{a} = (a_1, \ldots, a_k) \in \underline{A}^k$, let $U(\underline{a})$ denote the gate U applied to qubits $a_1, \cdots a_k$.

Below we recall the definition of simulatable codes, which was first introduced by Grilo, Slofstra, and Yuen [GSY19].

Definition 6.1.6. *Given a k-qubit logical gate U and a quantum error-correcting code $\mathcal{C} = [[m, 1]]$, let (σ_U, σ'_U) be a pair of states, and let ℓ be a positive integer. For each $1 \leqslant i \leqslant \ell$, let $\mathcal{O}_i$ be a mapping from elements $\underline{a} = (a_1, \cdots, a_k)$ in $\underline{A}^k$ to unitaries $\mathcal{O}_i(\underline{a})$ acting only on*

(i) the physical qubits of codewords in $\mathcal{C}$ that corresponds to logical qubits $a_1, \cdots, a_k$, and

(ii) the register that holds σ_U.

We say the tuple $(\sigma_U, \sigma'_U, \ell, \mathcal{O}_1, \cdots, \mathcal{O}_\ell)$ is an encoding of U in code $\mathcal{C}$ if

$$(\mathcal{O}_\ell(\underline{a}) \ldots \mathcal{O}_1(\underline{a}))(Enc(\rho) \otimes \sigma_U)(\mathcal{O}_\ell(\underline{a}) \ldots \mathcal{O}_1(\underline{a}))^* = Enc\big(U(\underline{a})\rho U(\underline{a})^*\big) \otimes \sigma'_U \qquad (6.1.3)$$

for all $n \geqslant k$, elements $\underline{a} \in \underline{A}_n^k$, and n-qubit states ρ. If in addition, the unitaries $\mathcal{O}_1(\underline{a}), \cdots, \mathcal{O}_\ell(\underline{a})$ are gates in some set $\mathcal{U}$ for all $\underline{A} \in \underline{A}^k$, then we say the encoding $(\sigma_U, \sigma'_U, l, \mathcal{O}_1, \cdots, \mathcal{O}_\ell)$ uses physical gates in $\mathcal{U}$.

Given a circuit of logical gates $V = U_1 \ldots U_k$ we refer to an encoding of V as the corresponding circuit of physical gates obtained by applying an encoding of each gate U_i.

Definition 6.1.7. *An encoding $(\sigma_U, \sigma'_U, \mathcal{O}_1, \ldots, \mathcal{O}_\ell)$ of a k-qubit logical gate U in a QECC $\mathcal{C}$ is called s-simulatable if for all $0 \leqslant t \leqslant \ell$, n-qubit states ρ, and subsets S of the physical qubits of $Enc(\rho) \otimes \sigma_U$ with $|S| \leqslant s$, the partial trace*

$$\mathrm{Tr}_{\overline{S}}\Big(\mathcal{O}_t(\underline{a}) \ldots \mathcal{O}_1(\underline{a}))(Enc(\rho) \otimes \sigma_U)(\mathcal{O}_t(\underline{a}) \ldots \mathcal{O}_1(\underline{a}))^*\Big)$$

is a $2^{|S|} \times 2^{|S|}$ matrix whose entries are rational and can be computed in polynomial time from t, $\underline{a}$ and S. In particular, this matrix is independent of ρ if $\mathcal{C}$ can correct arbitrary errors on s qubits.

Theorem 6.1.8 (Theorem 6 in [GSY19]). *Let $\mathcal{U} = \{H, \Lambda(X), \Lambda^2(X)\}$. For every $s \in \mathbb{N}$, there exists a constant $n \in \mathbb{N}$ and a $[[n, 1]]$ QECC $\mathcal{C}$ such that any logical gate in $\mathcal{U}$ has an s-simulatable encoding in $\mathcal{C}$ using physical gates in $\mathcal{U}$.*

6.2 Low-weight Pauli braiding test and its robustness

6.2.1 The test

In this section, we introduce a non-local game that can self-test for Alice making measurements with n-qubit "braids" of Pauli σ_X and σ_Z of weight at most 6, against n EPR pairs. That is, Alice performs a measurement of the form $\otimes_i \sigma_{W_i}$, where each $W_i \in \{X, Z, I\}$ and for all but 6 indices we have $W_i = I$. As we discuss in Section 6.1.2 we also want this game to be able to be won perfectly when Alice is restricted to only perform measurements on at most 6 qubits. Consequently, we cannot use the typical Pauli Braiding Test. To this end, we introduce a low-weight version of the Pauli Braiding test. We introduce this game for weight 6 but the rigidity arguments in the following section equally hold for the analogous game with any constant weight on the strings. This game is constructed from two subgames which we call the low-weight linearity test and the low-weight anti-commutation test.

Low-weight linearity test

For any $a \in \{0,1\}^n$ and $W \in \{X, Z\}^n$, we use $W(a)$ to denote the sequence $W_1^{a_1} W_2^{a_2} \cdots W_n^{a_n}$ where $X^0 = Z^0 = I$. Let $\mathcal{I}_A := \{W(a) : W \in \{X, Z\}^n, a \in \{0,1\}^n \text{ such that } |a| \leqslant 6\}$ and let $\mathcal{I}_B := \{(W(a), W(a')) : W \in \{X, Z\}^n, a, a' \in \{0,1\}^n \text{ such that } |a|, |a'| \leqslant 6\}$ be the question sets for Alice and Bob respectively. We first describe the n-qubit low-weight linearity test in Figure 6.2.

For this game we let μ denote the implied probability distribution on possible questions $\mathcal{I}_A \times \mathcal{I}_B$. We see that for any $x \in \mathcal{I}_A$ and $y \in \mathcal{I}_B$, either $\mu(x, y) = 0$ or $\frac{1}{\mu(x,y)} = O(n^6)$.

1. The verifier selects uniformly at random $W \in \{X, Z\}^n$ and strings $a, a' \in \{0,1\}^n$ satisfying $|a|, |a'| \leqslant 6$ (*i.e.* a, a' both have at most 6 non-zero entries).

2. The verifier sends $(W(a), W(a'))$ to Bob. If $a + a'$ has weight at most 6 then the verifier selects $W' \in \{W(a), W(a'), W(a + a')\}$ uniformly at random to send to Alice. Otherwise, the verifier uniformly at random sends $W' \in \{W(a), W(a')\}$ to Alice.

3. The verifier receives two bits (b_1, b_2) from Bob and one bit c from Alice.

4. If Alice receives $W(a)$ then the verifier requires $b_1 = c$. If Alice receives $W(a')$ then the verifier requires $b_2 = c$. If Alice receives $W(a + a')$ then the verifier requires $b_1 + b_2 = c$.

Figure 6.2: Low-weight linearity test.

Suppose $S = (\tau^A, \tau^B, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B)$ is a quantum strategy for this game. On each input $x \in \mathcal{I}_A$, Alice performs a two-outcome PVM $\{E_0^x, E_1^x\}$ where $E_0^x - E_1^x = \tau^A(x)$. Similarly, on each input $y = (W(a), W(a')) \in \mathcal{I}_B$ Bob performs a four-outcome PVM $\{F_{0,0}^y, F_{1,0}^y, F_{0,1}^y, F_{1,1}^y\}$, and we define the following observables:

$$\begin{aligned}
\tau_y^B(W(a)) &:= F_{0,0}^y + F_{0,1}^y - F_{1,0}^y - F_{1,1}^y, \\
\tau_y^B(W(a')) &:= F_{0,0}^y + F_{1,0}^y - F_{0,1}^y - F_{1,1}^y, \text{ and} \\
\tau_y^B(W(a + a')) &:= F_{0,0}^y + F_{1,1}^y - F_{0,1}^y - F_{1,0}^y.
\end{aligned}$$

We take a moment to explain some subtleties of the above notation. Instead of specifying a single observable $\tau^B(W(a))$ for all possible $W(a)$ we include a reference to each particular question pair $y = (W(a), W(a'))$. This is because it is possible for the same $W(a)$ to be included in different question pairs for different choices of $W(a')$. In particular, we can not assume that Bob's measurements will be the same for $W(a)$ across these different possible choices. For Alice, things are more straightforward and we can define a unique observable

$\tau^A(W(a))$ for each $W(a)$. Note that one can readily check that for each $y = (W(a), W(a'))$ we have

$$\tau_y^B(W(a+a')) = \tau_y^B(W(a))\tau_y^B(W(a')) = \tau_y^B(W(a'))\tau_y^B(W(a)). \tag{6.2.1}$$

Lemma 6.2.1. *Suppose $S = (\tau^A, \tau^B, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B)$ is a strategy for low-weight linearity test with winning probability $1-\epsilon$. Let $\rho_A := \mathrm{Tr}_{\mathcal{H}_B}(|\psi\rangle\langle\psi|)$. Then the following bounds hold.*

1. *For every $y = (W(a), W(a')) \in \mathcal{I}_B$,*

   (a) $\langle\psi|\, \tau^A(W(a)) \otimes \tau_y^B(W(a))\, |\psi\rangle \geqslant 1 - O(n^6)\epsilon$,

   (b) $\langle\psi|\, \tau^A(W(a')) \otimes \tau_y^B(W(a'))\, |\psi\rangle \geqslant 1 - O(n^6)\epsilon$, *and*

   (c) *if in addition, $W(a+a') \in \mathcal{I}_A$, then $\langle\psi|\, \tau^A(W(a+a')) \otimes \tau_y^B(W(a+a')) \geqslant 1 - O(n^6)\epsilon$.*

2. *For every $W \in \{X, Z\}^n$ and $a, a' \in \{0,1\}^n$ with $|a|, |a'|, |a+a'| \leqslant 6$,*

   (a) $\|\tau^A(W(a))\tau^A(W(a')) - \tau^A(W(a+a'))\|_{\rho_A}^2 \leqslant O(n^6)\epsilon$,

   (b) $\|\tau^A(W(a'))\tau^A(W(a)) - \tau^A(W(a+a'))\|_{\rho_A}^2 \leqslant O(n^6)\epsilon$, *and*

   (c) $\|\tau^A(W(a))\tau^A(W(a')) - \tau^A(W(a'))\tau^A(W(a))\|_{\rho_A}^2 \leqslant O(n^6)\epsilon$

Proof. Suppose $S = (\tau^A, \tau^B, |\psi\rangle)$ wins this game with probability $1-\epsilon$. If we condition on a round in which Bob receives question $y = (W(a), W(a'))$ and Alice receives $x = W(a)$ then the probability they lose on this question pair is bounded above by $(1/\mu(x,y))\epsilon \leqslant O(n^6)\epsilon$. Indeed otherwise they will lose the overall game with a probability greater than ϵ. Hence for any $x = W(a) \in \mathcal{I}_A$ and $y = (W(a), W(a')) \in \mathcal{I}_B$, we have

$$\begin{aligned}\langle\psi|\, \tau^A(W(a)) \otimes \tau_y^B(W(a))\, |\psi\rangle &= \langle\psi|\, (E_0^x - E_1^x) \otimes (F_{0,0}^y + F_{0,1}^y - F_{1,0}^y - F_{1,1}^y)\, |\psi\rangle \\ &= \langle\psi|\, (E_0^x \otimes F_{0,0}^y + E_0^x \otimes F_{0,1}^y + E_1^x \otimes F_{1,0}^y + E_1^x \otimes F_{1,1}^y)\, |\psi\rangle\end{aligned}$$

$$
\begin{aligned}
&- \langle\psi| \left(E_0^x \otimes F_{1,0}^y + E_0^x \otimes F_{1,1}^y + E_1^x \otimes F_{0,0}^y + E_1^x \otimes F_{0,1}^y\right) |\psi\rangle \\
=&Pr(\text{win}|x,y) - Pr(\text{lose}|x,y) \\
=&1 - 2Pr(\text{lose}|x,y) \geqslant 1 - O(n^6)\epsilon
\end{aligned}
$$

A similar analysis holds in the case that Bob receives question $y = (W(a), W(a'))$ and Alice instead receives question $x = W(a')$. In particular we get

$$\langle\psi| \tau^A(W(a')) \otimes \tau_y^B(W(a')) |\psi\rangle \geqslant 1 - O(n^6)\epsilon.$$

Next we consider the instances in which Bob receives question $y = (W(a), W(a'))$ and Alice receives question $x = W(a+a')$ where $|a+a'| \leqslant 6$. In this case the winning condition requires $b_1 + b_2 = c$, so we have

$$
\begin{aligned}
&\langle\psi| \tau^A(W(a+a')) \otimes \tau_y^B(W(a+a')) |\psi\rangle \\
&\qquad =\langle\psi| \left(E_0^x - E_1^x\right) \otimes \left(F_{0,0}^y + F_{1,1}^y - F_{0,1}^y - F_{1,0}^y\right) |\psi\rangle \\
&\qquad =\langle\psi| \left(E_0^x \otimes F_{0,0}^y + E_0^x \otimes F_{1,1}^y + E_1^x \otimes F_{1,0}^y + E_1^x \otimes F_{0,1}^y\right) |\psi\rangle \\
&\qquad\quad - \langle\psi| \left(E_0^x \otimes F_{1,0}^y + E_0^x \otimes F_{0,1}^y + E_1^x \otimes F_{0,0}^y + E_1^x \otimes F_{1,1}^y\right) |\psi\rangle \\
&\qquad =Pr(\text{win}|x,y) - Pr(\text{lose}|x,y) \\
&\qquad =1 - 2Pr(\text{lose}|x,y) \geqslant 1 - O(n^6)\epsilon.
\end{aligned}
$$

To see the inequalities in the second part hold for fixed $W(a)$ and $W(a')$ where $|a+a'| \leqslant 6$, we take $x = W(a+a'), y = (W(a), W(a'))$ to be the corresponding inputs for Alice and Bob. Let $\rho := |\psi\rangle\langle\psi|$. By the above work, we have

$$
\begin{aligned}
\|\tau^A(W(a)) \otimes \mathbb{1} - \mathbb{1} \otimes \tau_y^B(W(a))\|_\rho^2 &\leqslant O(n^6)\epsilon, \\
\|\tau^A(W(a')) \otimes \mathbb{1} - \mathbb{1} \otimes \tau_y^B(W(a'))\|_\rho^2 &\leqslant O(n^6)\epsilon, \text{ and} \\
\|\tau^A(W(a+a')) \otimes \mathbb{1} - \mathbb{1} \otimes \tau_y^B(W(a+a'))\|_\rho^2 &\leqslant O(n^6)\epsilon.
\end{aligned}
$$

Note that $\tau_y^B(W(a+a')) = \tau_y^B(W(a'))\tau_y^B(W(a))$ and that $\tau^A(W(a))$ and $\tau_y^B(W(a'))$ are unitary operators. We have

$$\|\tau^A(W(a))\tau^A(W(a')) - \tau^A(W(a+a'))\|_{\rho_A}$$

$$
\begin{aligned}
=&\|\Big(\tau^A(W(a))\tau^A(W(a')) - \tau^A(W(a+a'))\Big) \otimes \mathbb{1}\|_\rho \\
\leqslant&\|\tau^A(W(a))\tau^A(W(a')) \otimes \mathbb{1} - \tau^A(W(a)) \otimes \tau_y^B(W(a'))\|_\rho \\
&+ \|\tau^A(W(a)) \otimes \tau_y^B(W(a')) - \mathbb{1} \otimes \tau_y^B(W(a'))\tau_y^B(W(a))\|_\rho \\
&+ \|\mathbb{1} \otimes \tau_y^B(W(a+a')) - \tau^A(W(a+a')) \otimes \mathbb{1}\|_\rho \leqslant O(n^3)\sqrt{\epsilon}.
\end{aligned}
$$

Hence 2(a) holds, 2(b) holds for the same reason, while 2(c) follows from 2(a) and 2(b). □

Low-weight anti-commutation test

Next we introduce a natural version of the anti-commutation test built from the well-known magic square game. Recall that in the magic square game, Alice and Bob are trying to convince the verifier that they have a solution to a system of equations over $\mathbb{Z}_2$. There are 9 variables $v_1, \ldots, v_9$ in a 3×3-array whose rows are labeled r_1, r_2, r_3 and columns are labeled c_1, c_2, c_3. Each row or column corresponds to an equation: variables along the rows or columns in $\{r_1, r_2, r_3, c_1, c_2\}$ sum to 0; variables along the column c_3 sum to 1. In each round, Bob receives one of the 6 possible equations and he must respond with a satisfying assignment to the given equation. Alice is then asked to provide a consistent assignment to one of the variables contained in the equation Bob received. The following table describes an operator solution for this system of equations:

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

Table 6.1: Operator solution for magic square game

The canonical perfect quantum strategy for this game is one in which

- the players share two EPR pairs,
- given a variable v_i, Alice performs A_i on her registers, and

- given a row or column consisting of three variables v_j, v_l, and v_ℓ, Bob perform $A_j A_k A_\ell$ on his registers.

It is well-known that the magic square game is a robust self-test with robustness $O(\epsilon^{1/4})$. To incorporate this game in our anti-commutation test, we ask the players to play the Magic Square game on a specified 2-qubit register of their shared n-qubit state. Importantly, for all but one question v_9 Alice will not be able to tell if she is playing the low-weight linearity test or anti-commutation test, and thus we can combine the rigidity constraints from each game. Recall that the system of equations in the magic square game has an operator solution $\{A_1, \cdots, A_9\}$ defined in Section 6.2.1. We describe the low-weight anti-commutation test in Figure 6.3.

1. The verifier samples uniformly at random a string $a \in \{0,1\}^n$ with exactly two non-zero entries $i < j$. The verifier also samples a row or column $q \in \{r_1, r_2, r_3, c_1, c_2, c_3\}$, and a variable v_k contained in q as in the Magic Square game.

2. Bob receives the question (q, a).

3. If $k \neq 9$ then Alice receives $W(a) = I^{i-1} W_i I^{j-i} W_j I^{n-j} \in \mathcal{I}_A$ with $\sigma_{W_i} \otimes \sigma_{W_j} = A_k$. If $k = 9$ then Alice receives question (v_9, a).

4. The players win if and only if Bob responds with a satisfying assignment to q and Alice provides an assignment to variable v_k that is consistent with Bob's.

Figure 6.3: Low-weight anti-commutation test.

In the above game, for each string $a \in \{0,1\}^n$ with $|a| = 2$ we define the following set of observables for Alice $\{O_1(a), \ldots, O_9(a)\}$. If the players are winning the anti-commutation test with probability $1 - \epsilon$ then the above observables must determine the operators of a quantum strategy for Magic Square that wins with probability at least $1 - O(n^2)\epsilon$. The

robustness of magic square implies:

Lemma 6.2.2. *If the players are winning low-weight anti-commutation test with probability $1-\epsilon$, then for any $a \in \{0,1\}^n$ with $|a| = 2$ we have*

$$\|O_1(a)O_5(a) + O_5(a)O_1(a)\|_\sigma^2 \leqslant O(n)\sqrt{\epsilon}, \text{ and}$$
$$\|O_4(a)O_2(a) + O_2(a)O_4(a)\|_\sigma^2 \leqslant O(n)\sqrt{\epsilon}.$$

Formal statements

Combining the low-weight linearity test and low-weight anti-commutation test from the previous sections, we now construct the low-weight Pauli braiding test and state its rigidity result.

Definition 6.2.3. *The low-weight Pauli braiding test (LWPBT) is played by executing with probability $1/2$ either the low-weight anti-commutation test or the low-weight linearity test.*

If a quantum strategy $S = (\tau^A, \tau^B, |\psi\rangle)$ can win LWPBT with probability $1-\epsilon$, then it must be winning both the low-weight linearity test and low-weight anti-commutation test with probability at least $1-2\epsilon$. For every $W \in \{X, Z\}$ and $i \in [n]$, we use $\tau_W^A(e_i)$ to denote $\tau^A(I^{i-1}WI^{n-i})$. For any bit string $a = 0^{j-2}110^{n-j}$ with $2 \leqslant j \leqslant n$, since Alice cannot tell a question $I^{j-1}WI^{n-j}$ is from the low-weight linearity test or low-weight anti-commutation test, we must have $O_1(a) = \tau_X^A(e_j)$ and $O_5(a) = \tau_Z^A(e_j)$. Similarly, for any bit string $a = 0^{j-1}110^{n-j-1}$ with $1 \leqslant j \leqslant n-1$ we must have $O_2(a) = \tau_X^A(e_j)$ and $O_4(a) = \tau_Z^A(e_j)$. Then the following theorem follows directly from Lemma 6.2.1 and Lemma 6.2.2.

Theorem 6.2.4. *Suppose $S = (\tau^A, \tau^B, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B)$ is a strategy for LWPBT with wining probability $1-\epsilon$. Let $\rho_A := \mathrm{Tr}_{\mathcal{H}_B}(|\psi\rangle\langle\psi|)$.*

1. *For every $y = (W(a), W(a')) \in I_B$, we have the following bounds on consistency.*

   (a) $\langle\psi| \tau^A(W(a)) \otimes \tau_y^B(W(a)) |\psi\rangle \geqslant 1 - O(n^6)\epsilon,$

(b) $\langle\psi|\,\tau^A(W(a'))\otimes\tau_y^B(W(a'))\,|\psi\rangle \geqslant 1-O(n^6)\epsilon$, *and*

(c) if in addition $|a+a'|\leqslant 6$, *then* $\langle\psi|\,\tau^A(W(a+a'))\otimes\tau_y^B(W(a+a'))\geqslant 1-O(n^6)\epsilon$.

2. *For every* $W\in\{X,Z\}^n$ *and* $a,a'\in\{0,1\}^n$ *with* $|a|,|a'|,|a+a'|\leqslant 6$, *we have the following linearity bounds and commutation bound.*

(a) $\|\tau^A(W(a))\tau^A(W(a'))-\tau^A(W(a+a'))\|_{\rho_A}^2\leqslant O(n^6)\epsilon$,

(b) $\|\tau^A(W(a'))\tau^A(W(a))-\tau^A(W(a+a'))\|_{\rho_A}^2\leqslant O(n^6)\epsilon$, *and*

(c) $\|\tau^A(W(a))\tau^A(W(a'))-\tau^A(W(a'))\tau^A(W(a))\|_{\rho_A}^2\leqslant O(n^6)\epsilon$

3. *For any* $i,j\in[n]$ *we have the following commutation/anti-commutation bound.*

(a) $\|\tau_X^A(e_i)\tau_Z^A(e_j)-(-1)^{\delta_{ij}}\tau_Z^A(e_j)\tau_X^A(e_i)\|_{\rho_A}^2\leqslant O(n)\sqrt{\epsilon}$.

6.2.2 Proof of robustness

We now aim to prove the rigidity of the low-weight Pauli Braiding test. To start, we fix an $n\in\mathbb{N}$, an $\epsilon>0$, and a quantum strategy $S:=(\tau^A,\tau^B,|\psi\rangle\in\mathcal{H}_A\otimes\mathcal{H}_B)$ for the n-qubit LWPBT with winning probability $1-\epsilon$ through this section (except for Theorem 6.2.12).

Let $H(n)$ be the n-qubit Weyl-Heisenberg group generated by indeterminates $J,X_i,Z_i,i\in[n]$, subject to the relations

(R0) J is central, and $J^2=X_i^2=Z_i^2=1$ for all $1\leqslant i\leqslant n$,

(R1) $[X_i,Z_i]=J$ for all or all $1\leqslant i\leqslant n$, and

(R2) $[X_i,X_j]=[Z_i,Z_j]=[X_i,Z_j]=1$ for all $i\neq j$.

Intuitively, this group models n-qubit Pauli measurements. It has an irreducible representation $\sigma:H(n)\to\mathcal{U}((\mathbb{C}^2)^{\otimes n})$ sending $J\mapsto-\mathbb{1}$, $X_i\mapsto\sigma_X(e_i)$, and $Z_i\mapsto\sigma_Z(e_i)$ for all

$i \in [n]$. In this section, the symbol σ will be used exclusively to refer to this irreducible representation. The following two lemmas are well-known.

Lemma 6.2.5. $\mathrm{Irr}(H(n)) = \{\sigma\} \cup \{\chi_i : 1 \leqslant i \leqslant 2^{2n}\}$ *where every* $\chi_i : H(n) \to \mathbb{C}$ *is a one dimensional representation sending* $J \mapsto 1$.

Lemma 6.2.6. $H(n)$ *has a normal form* $\mathcal{N}(w) = J^{\alpha} X_{i_1} \cdots X_{i_k} Z_{j_1} \cdots Z_{j_l}$ *where* $\alpha \in \{0, 1\}$, $1 \leqslant i_1 < \cdots < i_k \leqslant n$, *and* $1 \leqslant j_1 < \cdots < j_l \leqslant n$.

For any $W \in \{X, Z\}$ and $i \in [n]$, we use $\tau_W^A(e_i)$ and $\tau_W^B(e_i)$ to denote $\tau^A(I^{i-1}WI^{n-i})$ and $\tau_y^B(I^{i-1}WI^{n-i})$ respectively, where $y = (I^{i-1}WI^{n-i}, I^n)$. Define functions $f_P : H(n) \to \mathcal{U}(\mathcal{H}_P)$, $P \in \{A, B\}$ via sending

$$J^{\alpha} X_{i_1} \cdots X_{i_k} Z_{j_1} \cdots Z_{j_l} \mapsto (-1)^{\alpha} \tau_X^P(e_{i_1}) \cdots \tau_X^P(e_{i_k}) \tau_Z^P(e_{j_1}) \cdots \tau_Z^P(e_{j_l}),$$

so in particular, $f_P(1) = \mathbb{1}_{\mathcal{H}_P}$ and $f_P(J) = -\mathbb{1}_{\mathcal{H}_P}$. We also define functions $\widetilde{f}_A, \widetilde{f}_B : H(n) \to \mathcal{U}(\mathcal{H}_A \otimes \mathcal{H}_B)$ via $\widetilde{f}_A(g) := f_A(g) \otimes \mathbb{1}_{\mathcal{H}_B}$ and $\widetilde{f}_B(g) := \mathbb{1}_{\mathcal{H}_A} \otimes f_B(g)$. Through this section, we use ρ, ρ_A and ρ_B to denote $|\psi\rangle\langle\psi|$, $\mathrm{Tr}_{\mathcal{H}_B}(\rho)$ and $\mathrm{Tr}_{\mathcal{H}_A}(\rho)$ respectively.

Proposition 6.2.7. *Let* $\delta := O(n^6)\sqrt{\epsilon}$. *Every* $f \in \{\widetilde{f}_A, \widetilde{f}_B\}$ *satisfies the following conditions.*

(1) f *respects all the relations in R0.*

(2) $\|f(X_i)f(Z_i) + f(Z_i)f(X_i)\|_\rho^2 \leqslant \delta$ *for all* $1 \leqslant i \leqslant n$.

(3) $\|f(X_i)f(X_j) - f(X_j)f(X_i)\|_\rho^2$, $\|f(Z_i)f(Z_j) - f(Z_j)f(Z_i)\|_\rho^2$, *and* $\|f(X_i)f(Z_j) - f(Z_j)f(X_i)\|_\rho^2$ *are bounded by* δ *whenever* $i \neq j$.

(4) For every W_i *where* $W \in \{X, Z\}, i \in [n]$, *there exists a unitary* $\widehat{W}_i$ *commuting with all* $\{f(X_j), f(Z_j), j \in [n]\}$ *such that* $\|f(W_i) - \widehat{W}_i\|_\rho^2 \leqslant \delta$.

(5) For any $s \geqslant 1$ *and every monomial*[3] $v = v_1 \cdots v_s$ *over* $\{f(X_i), f(Z_i), i \in [n]\}$ *of degree* s, *there exists a unitary* $\hat{v}$ *commuting with all* $\{f(X_i), f(Z_i), i \in [n]\}$ *such that* $\|v - \hat{v}\|_\rho \leqslant s\sqrt{\delta}$.

[3]Here we allow the coefficient of a monomial to be 1 or -1.

Proof. We first examine that $\widetilde{f}_A$ satisfies (1), (2), (3), and (4). Since $\|W \otimes \mathbb{1}_{\mathcal{H}_B}\|_\rho = \|W\|_{\rho_A}$ for all $W \in \mathcal{B}(\mathcal{H}_A)$, it follows from Theorem 6.2.4 that $\widetilde{f}_A$ satisfies part (1), (2), and (3). To establish part (4), observe that every $\widetilde{f}_B(W_i)$ commutes with $\widetilde{f}_A(X_j), \widetilde{f}_A(Z_j)$ for all $j \in [n]$, and

$$\|\widetilde{f}_A(W_i) - \widetilde{f}_B(W_i)\|_\rho^2 = 2 - 2\langle\psi|\, \tau_W^A(e_i) \otimes \tau_W^B(e_i)\, |\psi\rangle \leqslant O(n^6)\sqrt{\epsilon} \tag{6.2.2}$$

by Theorem 6.2.4. Hence part (4) follows by taking $\hat{W}_i = \widetilde{f}_B(W_i)$.

Next we examine that $\widetilde{f}_B$ satisfies (1), (2), (3) and (4). Part (1) is obvious. Since

$$\begin{aligned}\widetilde{f}_B(X_i)\widetilde{f}_B(Z_i) + \widetilde{f}_B(Z_i)\widetilde{f}_B(X_i) = {} & \widetilde{f}_B(X_i)\big(\widetilde{f}_B(Z_i) - \widetilde{f}_A(Z_i)\big) + \widetilde{f}_B(Z_i)\big(\widetilde{f}_B(X_i) - \widetilde{f}_A(X_i)\big) \\ & + \widetilde{f}_A(Z_i)\big(\widetilde{f}_B(X_i) - \widetilde{f}_A(X_i)\big) + \widetilde{f}_A(X_i)\big(\widetilde{f}_B(Z_i) - f_A(Z_i)\big) \\ & + \widetilde{f}_A(Z_i)\widetilde{f}_A(X_i) + \widetilde{f}_A(X_i)\widetilde{f}_A(Z_i),\end{aligned}$$

and each term on the right hand side has ρ-norm $\leqslant O(n^6)\sqrt{\epsilon}$ by Theorem 6.2.4, it follows that $\|\widetilde{f}_B(X_i)\widetilde{f}_B(Z_i) + \widetilde{f}_B(Z_i)\widetilde{f}_B(X_i)\|_\rho^2 \leqslant O(n^6)\sqrt{\epsilon}$. Therefore, part (2) holds for $\widetilde{f}_B$. With a similar argument we obtain that part (3) holds. Part (4) follows from Equation (6.2.2) by taking $\widehat{W}_i = \widetilde{f}_A(W_i)$.

Now we prove part (5) by induction on the monomial degree $s \geqslant 1$. The base case $s = 1$ follows straight from part (4). Suppose part (5) holds for all monomials over $\{f(X_i), f(Z_i), i \in [n]\}$ of degree s. For any monomial $v = v_1 \cdots v_s v_{s+1}$ over $\{f(X_i), f(Z_i), i \in [n]\}$ of degree $s+1$, let $v' := v_1 \cdots v_s$. By the induction hypothesis, there are unitaries $\hat{v}'$ and $\hat{v}_{s+1}$ commuting with all $\{f(X_i), f(Z_i), i \in [n]\}$ such that $\|v' - \hat{v}'\|_\rho \leqslant s\sqrt{\delta}$ and $\|v_{s+1} - \hat{v}_{s+1}\|_\rho \leqslant \sqrt{\delta}$. In particular, $\hat{v}_{s+1}$ commutes with v', so $v = v'(v_{s+1} - \hat{v}_{s+1}) + \hat{v}_{s+1}(v' - \hat{v}') + \hat{v}_{s+1}\hat{v}'$. Since ρ-norm is left unitarily invariant and $\hat{v}', \hat{v}_{s+1}$ are unitaries commuting with all $\{f(X_i), f(Z_i), i \in [n]\}$, it follows that $\hat{v}_{s+1}\hat{v}' =: \hat{v}$ is a unitary commuting with all all $\{f(X_i), f(Z_i), i \in [n]\}$ and satisfies

$$\|v - \hat{v}\|_\rho \leqslant \|v_{s+1} - \hat{v}_{s+1}\|_\rho + \|v' - \hat{v}'\|_\rho \leqslant (s+1)\sqrt{\delta}.$$

We conclude that part (5) holds for all monomials over $\{f(X_i), f(Z_i), i \in [n]\}$. □

Proposition 6.2.8. *Let $\delta := O(n^6)\sqrt{\epsilon}$. Then every $f \in \{\widetilde{f}_A, \widetilde{f}_B\}$ is an $\big(O(n^6)\delta, \rho\big)$-homomorphism of $H(n)$.*

Proof. Let $R := \{f(X_i)f(X_j) - f(X_j)f(X_i), f(Z_i)f(Z_j) - f(Z_j)f(Z_i), f(X_i)f(Z_j) - f(Z_j)f(X_i) : i \neq j\} \cup \{f(X_i)f(Z_i) + f(Z_i)f(X_i) : i \in [n]\}$. Then by Proposition 6.2.7 part (2) and (3), $\|r\|_\rho \leqslant \sqrt{\delta}$ for all $r \in R$. Since $f(X_i)$ and $f(Z_i)$ are unitaries, it follows that $\|r\|_{op} \leqslant 2$ for all $r \in R$.

By the definition of $\widetilde{f}_A$ and $\widetilde{f}_B$ and the normal form theorem for $H(n)$, for any $g, h \in H(n)$, we see that $f(g)f(h)$ and $f(gh)$ are monomials over $\{f(X_i), f(Z_i), i \in [n]\}$ of degrees less than $4n$, and $f(g)f(h) - f(gh) = \sum_{i=1}^{k} u_i r_i v_i$ where $k \leqslant 4n^2$, $r_1, \cdots r_k \in R$, $u_1, \cdots u_k, v_1, \cdots, v_k$ are monomials over $\{f(X_i), f(Z_i), i \in [n]\}$, and every v_i has degree less than $2n$. The last condition implies that for every $i \in [k]$, there is a unitary $\hat{v}_i$ commuting with all $\{f(X_i), f(Z_i), i \in [n]\}$ such that $\|v_i - \hat{v}_i\|_\rho \leqslant 2n\sqrt{\delta}$ by Proposition 6.2.7 part (5). Then for each $i \in [k]$ we have

$$\begin{aligned}\|u_i r_i v_i\|_\rho = \|r_i(v_i - \hat{v}_i + \hat{v}_i)\|_\rho &\leqslant \|r_i(v_i - \hat{v}_i)\|_\rho + \|\hat{v}_i r_i\|_\rho \\ &\leqslant \|r_i\|_{op} \cdot \|v_i - \hat{v}_i\|_\rho + \|r_i\|_\rho \leqslant (4n+1)\sqrt{\delta}.\end{aligned}$$

Hence $\|f(g)f(h) - f(gh)\|_\rho \leqslant \sum_{i=1}^{k} \|u_i r_i v_i\|_\rho \leqslant O(n^3)\sqrt{\delta}$. We conclude that $\|f(g)f(h) - f(gh)\|_\rho^2 \leqslant O(n^6)\delta$ for all $g, h \in H(n)$. □

Since $\|f_P(g)f_P(h) - f_P(gh)\|_{\rho_P}^2 = \|\widetilde{f}_P(g)\widetilde{f}_P(h) - \widetilde{f}_P(gh)\|_\rho^2$ for every $P \in \{A, B\}$ and all $g, h \in H(n)$, we have:

Corollary 6.2.9. *The function f_A (resp. f_B) is a $(O(n^{12})\sqrt{\epsilon}, \rho_A)$-homomorphism (resp. $(O(n^{12})\sqrt{\epsilon}, \rho_B)$-homomorphism) of $H(n)$.*

Now we can apply Theorem 5.1.4 to f_A and f_B.

Proposition 6.2.10. *There are Hilbert spaces $\mathcal{H}_A^{aux}$, $\mathcal{H}_B^{aux}$ and isometries $V_A : \mathcal{H}_A \to \mathbb{C}^{2^n} \otimes \mathcal{H}_A^{aux}$, $V_B : \mathcal{H}_B \to \mathbb{C}^{2^n} \otimes \mathcal{H}_B^{aux}$ such that $\|V_A f_A(g) - \big(\sigma(g) \otimes \mathbb{1}_{\mathcal{K}_A}\big)V_A\|_{\rho_A}^2 \leqslant O(n^{12})\sqrt{\epsilon}$ and $\|V_B f_B(g) - \big(\sigma(g) \otimes \mathbb{1}_{\mathcal{K}_B}\big)V_B\|_{\rho_B}^2 \leqslant O(n^{12})\sqrt{\epsilon}$ for all $g \in H(n)$.*

Proof. Let $\delta = O(n^{12})\sqrt{\epsilon}$. Corollary 6.2.9 implies f_A is a (δ, ρ_A)-homomorphism of $H(n)$. For any one-dimensional irreducible representation $\xi \in \mathrm{Irr}\big(H(n)\big)$,

$$\begin{aligned}\widehat{f}_A(\xi) &= \sum_{g\in H(n)} f_A(g)\otimes\overline{\xi(g)} = \frac{1}{2}\left(\sum_{g\in H(n)}\xi(g)f_A(g) + \sum_{g\in H(n)}\xi(Jg)f_A(Jg)\right)\\ &= \frac{1}{2}\left(\sum_{g\in H(n)}\xi(g)f_A(g) - \sum_{g\in H(n)}\xi(g)f_A(g)\right) = 0.\end{aligned}$$

Then by Theorem 5.1.4, there is a Hilbert space $\mathcal{K}$, an isometry $V : \mathcal{H}_A \to \mathcal{K}$, and a representation $\phi : H(n) \to \mathcal{U}(\mathcal{K})$ such that $\|f_A(g) - V^*\phi(g)V\|_\rho^2 \leqslant \delta$ for all $g \in H(n)$, and ϕ has a unique irreducible constituent σ. The latter condition means that $\mathcal{K} \cong \mathbb{C}^{2^n}\otimes\mathcal{H}_A^{aux}$ for some Hilbert space $\mathcal{H}_A^{aux}$ and there is a unitary $U : \mathcal{K} \to \mathbb{C}^{2^n}\otimes\mathcal{H}_A^{aux}$ such that $U\phi(g)U^* = \sigma(g)\otimes\mathbb{1}_{\mathcal{H}_A^{aux}}$ for all $g \in H(n)$. Since ρ_A-norm is left unitarily invariant, it follows that

$$\|f(g) - V^*\phi(g)V\|_{\rho_A} = \|f(g) - (UV)^*\big(\sigma(g)\otimes\mathbb{1}_{\mathcal{H}_A^{aux}}\big)UV\|_{\rho_A}$$

for all $g \in H(n)$. We conclude that $V_A := UV : \mathcal{H}_A \to \mathbb{C}^{2^n}\otimes\mathcal{H}_A^{aux}$ is an isometry such that $\|f_A(g) - V_A\big(\sigma(g)\otimes Id_{\mathcal{H}_A^{aux}}\big)V_A\|_{\rho_A}^2 \leqslant \delta$. The argument for f_B follows similarly. □

The above theorem illustrates that in a near-perfect strategy for LWPBT, the players must perform measurements that are close to the measurements in the canonical perfect strategy. Let π be the associated representation of the canonical perfect strategy for LWPBT, and let Φ_{LWPBT} be the game polynomial of LWPBT. Then

$$\begin{aligned}\pi(\Phi_{LWPBT}) &= \frac{1}{4n}\sum_{a,b\in\{0,1\},i\in[n]}\sigma_X(e_i)^a\sigma_Z(e_i)^b\otimes\sigma_X(e_i)^a\sigma_Z(e_i)^b\\ &= \frac{1}{n}\sum_{i\in[n]}\mathbb{1}_{\mathbb{C}^4}^{\otimes(i-1)}\otimes|\Phi_{\mathrm{EPR}}\rangle\langle\Phi_{\mathrm{EPR}}|\otimes\mathbb{1}_{\mathbb{C}^4}^{\otimes(n-i)}.\end{aligned}$$

Hence $|\Phi_{\Phi_{\mathrm{EPR}}}^{\otimes n}\rangle$ is the unique eigenstate of the 1-eigenspace of $\pi(\Phi_{LWPBT})$ and the spectral gap of $\pi(\Phi_{LWPBT})$ is $\frac{1}{n}$. The following proposition follows straightforwardly from Proposition 4.2.13.

Proposition 6.2.11. *There are Hilbert spaces $\mathcal{H}_A^{aux}$ and $\mathcal{H}_B^{aux}$, isometries $V_A : \mathcal{H}_A \to \mathbb{C}^{2n} \otimes \mathcal{H}_A^{aux}, V_B : \mathcal{H}_B \to \mathbb{C}^{2n} \otimes \mathcal{H}_B^{aux}$, and a unit vector $|aux\rangle \in \mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}$ such that*

$$\|(V_A \otimes V_B)\big(f_A(g) \otimes \mathbb{1}_{\mathcal{H}_B} |\psi\rangle\big) - \big(\sigma(g) \otimes \mathbb{1}_{\mathbb{C}^{2^n}} |\Phi_{EPR}^{\otimes n}\rangle\big) \otimes |aux\rangle\| \leqslant O(n^7)\epsilon^{1/4} \tag{6.2.3}$$

for all $g \in H(n)$.

Recall that for any $W \in \{X, Z\}^n$ and $a \in \{0,1\}^n$, we use $\sigma_W(a)$ to denote tensor product of Pauli operators $\otimes_{i=1}^n \sigma_{W_i}^{a_i}$. In the canonical perfect strategy for LWPBT, Alice performs $\sigma_W(a)$ on question $W(a) \in \mathcal{I}_A$. Since $|a| \leqslant 6$ for all $W(a) \in \mathcal{I}_A$, as an immediate consequence of Proposition 6.2.11 and Theorem 6.2.4 we have:

Theorem 6.2.12. *There exists a constant $C_{\text{lw}} > 0$ such that the following holds. For any $\epsilon > 0$, $n \in \mathbb{N}$, and strategy $\mathcal{S} = (\tau^A, \tau^B, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B)$ for the n-qubit LWPBT with winning probability $1 - \epsilon$, there are isometries $V_A : \mathcal{H}_A \to (\mathbb{C}^2)^{\otimes n} \otimes \mathcal{H}_A^{aux}, V_B : \mathcal{H}_B \to (\mathbb{C}^2)^{\otimes n} \otimes \mathcal{H}_B^{aux}$ and a unit vector $|aux\rangle \in \mathcal{H}_A^{aux} \otimes \mathcal{H}_B^{aux}$ such that*

$$\|(V_A \otimes V_B)\big(\tau^A(W(a)) \otimes Id_{\mathcal{H}_B} |\psi\rangle\big) - \big(\sigma_W(a) \otimes Id_{\mathbb{C}^{2^n}} |\Phi_{EPR}^{\otimes n}\rangle\big) \otimes |aux\rangle\| \leqslant C_{\text{lw}} n^7 \epsilon^{1/4}$$

for all $W(a) \in \mathcal{I}_A$.

6.3 Energy test and Hamiltonian game

In this section, we show that for some local Hamiltonian H, one can construct a nonlocal game $\mathcal{G}(H)$ whose winning probability is closely related to the ground state energy $\lambda_0(H)$ of H. Our game is based on the Hamiltonian game introduced by Grilo [Gri19], but some subtle reconfigurations are made for the purpose of the zero-knowledge property. In particular, instead of using Pauli braiding test as in [Gri19], we employ the low-weight Pauli braiding test against dishonest quantum provers and then perform parallel repetition to achieve a constant completeness-soundness gap. To incorporate LWPBT in our modified Hamiltonian test, we consider Hamiltonians with specific structures:

Definition 6.3.1. *We say a Hamiltonian H is of XZ-type if it can be decomposed as $H = \frac{1}{m}\sum_{\ell=1}^{m} \gamma_\ell H_\ell$ where each $\gamma_\ell \in [-1, 1]$ and each term H_ℓ is a tensor product of operators σ_X, σ_Z or σ_I.*

Next, we define the relevant energy test which is analogous to the energy test used in [Gri19].

Definition 6.3.2 (Energy test)**.** *Given an n-qubit 6-local Hamiltonian $H = \frac{1}{m}\sum_{\ell=1}^{m} \gamma_\ell H_\ell$ of XZ-type we define the following energy test:*

1. *The verifier picks a term H_ℓ for $\ell \in [m]$ taken uniformly at random, and selects uniformly at random from the pairs $\{(W, r) \in \{X, Z\}^n \times \{0, 1\}^n : \sigma_W(r) = H_\ell\}$.*

2. *The verifier sends $W(r)$ to Alice, and tells Bob that the players are playing the energy test.*

3. *Alice responds with a single value $c \in \{-1, 1\}$.*

4. *Bob responds with $2n$ bits $a_1, \ldots a_n, b_1, \ldots b_n$.*

5. *The verifier next computes bit string d as follows. Take $d_i = (-1)^{a_i}$ if $r_i = 1$ and $W_i = X$, take $d_i = (-1)^{b_i}$ if $r_i = 1$ and $W_i = Z$, and take $d_i = 0$ in all other cases.*

6. *The verifier accepts if $c \cdot \prod_i d_i \neq sign(\gamma_l)$, and rejects with probability $|\gamma_l|$ otherwise.*

Combining the LWPBT and the above energy test we define our modified Hamiltonian test:

Definition 6.3.3 (Hamiltonian test)**.** *Let $H = \frac{1}{m}\sum_{\ell=1}^{m} \gamma_\ell H_\ell$ be a k-local Hamiltonian of XZ-type and let $p \in (0, 1)$. We define the following game $\mathcal{G}(H, p)$: with probability $(1 - p)$ the players play LWPBT introduced in Section Section 6.2, and with probability p the players play energy test described in Definition 6.3.2.*

We refer to a strategy $\mathcal{S}$ for $\mathcal{G}(H,p)$ as a *semi-honest strategy* if the players employ the canonical perfect strategy when playing LWPBT. Hence in a semi-honest strategy Alice and Bob hold n EPR pairs and Alice must perform $\sigma_W(r)$ on question $W(r)$ since she cannot distinguish questions from LWPBT or energy test. We also define the *honest strategy* $\mathcal{S}_h$ for $\mathcal{G}(H,p)$ in which the players employ the canonical perfect strategy when playing LWPBT, and in the energy test, Bob honestly teleports the ground state of H to Alice and provides the verifier with the teleportation keys.

Below we analyze the players' ability to win the overall game $\mathcal{G}(H,p)$ assuming the players are using a semi-honest strategy.

Lemma 6.3.4 (Lower bound on semi-honest strategies)**.** *Suppose $H = \frac{1}{m}\sum_{l=1}^{m}\gamma_l H_l$ is an n-qubit 6-local XZ Hamiltonian, and Alice and Bob are performing a semi-honest strategy $\mathcal{S}$ for $\mathcal{G}(H,p)$. Then*

$$\omega(\mathcal{S}) \leqslant \omega(\mathcal{S}_h) = 1 - p\left(\frac{1}{2m}\sum_{l}|\gamma_l| + \frac{1}{2}\lambda_0(H)\right).$$

Proof. Suppose the players are employing a semi-honest strategy $\mathcal{S} = (\tau^A, \tau^B, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B)$ for $\mathcal{G}(H,p)$. Let $\tau := \mathrm{Tr}_{\mathcal{H}_B}(|\psi\rangle\langle\psi|)$. Since the players win the LWPBT perfectly, they can only lose the overall game if they are playing an instance of the energy test. Let $a, b \in \{0,1\}^n$ be the answers Bob provides in the energy test, and let $\rho := \sigma_X^b\sigma_Z^a\tau\sigma_Z^a\sigma_X^b$.

Suppose in a round of the energy test, the verifier picks an $\ell \in [m]$ and selects a $W(r)$ for Alice. As discussed above, since Alice cannot distinguish questions from LWPBT and the energy test, she must perform $\sigma_W(r) = H_\ell$ on her registers. Hence $\mathbb{E}(c\cdot\prod_i d_i) = \mathrm{Tr}(H_\ell\sigma_X^b\sigma_Z^a\tau\sigma_Z^a\sigma_X^b) = \mathrm{Tr}(H_\ell\rho)$. Let p_ℓ be the probability of $c\prod_i d_i = sign(\gamma_\ell)$. Then $\mathbb{E}(c\prod_i d_i) = p_\ell sign(\gamma_\ell) - (1-p_\ell)sign(\gamma_\ell)$, or in other words, $\gamma_\ell\mathbb{E}(c\prod_i d_i) = (2p_\ell - 1)|\gamma_\ell|$. This implies the verifier rejects with probability

$$p_\ell|\gamma_\ell| = \frac{|\gamma_\ell| + \gamma_\ell\mathbb{E}(c\prod_i d_i)}{2} = \frac{|\gamma_\ell| + \gamma_\ell\mathrm{Tr}(H_\ell\rho)}{2}.$$

Thus by averaging over $\ell \in [m]$ we see that the players lose the energy test with probability

$$\frac{1}{m}\sum_{\ell\in[m]}\frac{|\gamma_\ell| + \gamma_\ell \mathrm{Tr}(H_\ell\rho)}{2} = \frac{1}{2m}\sum_{\ell\in[m]}|\gamma_\ell| + \frac{1}{2}\mathrm{Tr}(H\rho).$$

This probability is minimized if and only if ρ is indeed the density matrix of the ground state of H and in such case, the probability of winning the overall game is at most

$$1 - p\big(\frac{1}{2m}\sum_{\ell\in[m]}|\gamma_\ell| + \frac{1}{2}\lambda_0(H)\big).$$

This probability can be achieved if Bob teleports over the ground state and supplies the verifier with the verification keys in the energy test. □

Lemma 6.3.5. *(Upper bound on dishonest strategies) Let $H = \frac{1}{m}\sum_{\ell=1}^{m}\gamma_\ell H_\ell$ be a 6-local, n-qubit Hamiltonian of XZ-type. For any $\eta \in (0,1)$, let $p = \frac{4n^{-6}\eta^{3/4}}{(C_{\mathrm{lw}}+1)3^{3/4}}$ where C_{lw} is the constant given in Theorem 6.2.12. Then*

$$\omega^*\big(\mathcal{G}(H,p)\big) \leqslant \omega(\mathcal{S}_h) + \eta,$$

where $\omega(\mathcal{S}_h) = 1 - p\big(\frac{1}{2m}\sum_{\ell\in[m]}|\gamma_\ell| + \frac{1}{2}\lambda_0(H)\big)$ as in Lemma 6.3.5.

Proof. Suppose the provers are employing a strategy $\mathcal{S} = (\tau^A, \tau^B, |\psi\rangle)$ for $\mathcal{G}(H,p)$ that wins LWPBT with probability $1-\epsilon$ and wins the energy test with probability $\delta + 1 - \frac{\sum_\ell|\gamma_\ell|}{2m} - \frac{\lambda_0(H)}{2}$. Theorem 6.2.12 implies $\delta \leqslant C_{\mathrm{lw}}n^7\epsilon^{1/4}$. Then for $p := \frac{4n^{-7}\eta^{3/4}}{(C_{\mathrm{lw}}+1)3^{3/4}}$ with $\eta \in (0,1)$, we have $\eta + \epsilon = \eta/3 + \eta/3 + \eta/3 + \epsilon \geqslant 4(\frac{\eta^3\epsilon}{3^3})^{1/4} = p(C_{\mathrm{lw}}+1)n^7\epsilon^{1/4}$. It follows that

$$p\delta - (1-p)\epsilon \leqslant pCn^6\epsilon^{1/4} + p\epsilon - \epsilon \leqslant pC_{\mathrm{lw}}n^7\epsilon^{1/4} + pn^7\epsilon^{1/4} - \epsilon = p(C_{\mathrm{lw}}+1)n^7\epsilon^{1/4} - \epsilon \leqslant \eta.$$

Hence the overall winning probability is given by

$$\omega(\mathcal{S}) = (1-p)(1-\epsilon) + p(\delta + 1 - \frac{\sum_\ell|\gamma_\ell|}{2m} - \frac{\lambda_0(H)}{2}) = \omega(\mathcal{S}_h) + p\delta - (1-p)\epsilon \leqslant \omega(\mathcal{S}_h) + \eta.$$

□

In the rest of this paper, given an n-qubit, 6-local Hamiltonian H of XZ-type and parameters α and β with $\beta-\alpha \geqslant 1/poly(n)$, we use $\mathcal{G}(H)$ to denote the game $\mathcal{G}(H,p)$ with $p = \frac{32n^{-7}(\beta-\alpha)^{24}}{27(C_{\mathrm{lw}}+1)^4}$.

Theorem 6.3.6. *Given an n-qubit, 6-local Hamiltonian $H = \frac{1}{m}\sum_{\ell=1}^{m}\gamma_\ell H_\ell$ and parameters α, β with $\beta-\alpha \geqslant 1/poly(n)$, let ω_α (resp. ω_β) denote the maximum winning probability for $\mathcal{G}(H)$ when $\lambda_0(H) \leqslant \alpha$ (resp. $\lambda_0(H) \geqslant \beta$). Then $\omega_\alpha - \omega_\beta \geqslant 1/poly(n)$.*

Proof. Let $\eta := \frac{16(\beta-\alpha)^{36}}{27(C_{\mathrm{lw}}+1)^4}$, and let $p := \frac{4n^{-7}\eta^{3/4}}{(C_{\mathrm{lw}}+1)3^{3/4}}$. Then $p = \frac{32n^{-7}(\beta-\alpha)^{27}}{27(C_{\mathrm{lw}}+1)^4}$, and hence $\mathcal{G}(H) = \mathcal{G}(H,p)$. By Lemma 6.3.4 and Lemma 6.3.5 we have $\omega(\mathcal{S}_h) \leqslant \omega^*\big(\mathcal{G}(H,p)\big) \leqslant \omega(\mathcal{S}_h)+\eta$. This implies $\omega_\alpha \geqslant 1-p(\frac{1}{2m}\sum_\ell|\gamma_\ell| + \frac{1}{2}\alpha)$ and $\omega_\beta \leqslant 1-p(\frac{1}{2m}\sum_\ell|\gamma_\ell| + \frac{1}{2}\beta)+\eta$. Since $n^7(\beta-\alpha)^8 \leqslant O(n^{-1})$, it follows that

$$\omega_\alpha - \omega_\beta \geqslant \frac{1}{2}p(\beta-\alpha) - \eta = \frac{16n^{-6}(\beta-\alpha)^{28}}{27(C_{\mathrm{lw}}+1)^4}(1-n^7(\beta-\alpha)^8) \geqslant \frac{16n^{-6}(\beta-\alpha)^{28}}{27(C_{\mathrm{lw}}+1)^4} \geqslant \frac{1}{poly(n)}.$$

□

Our approach to gap amplification follows that of [GSY19] which uses parallel repetition for the anchored version of games with perfect completeness. The key difference is that in our case the underlying games do not satisfy perfect completeness. Instead we apply a threshold parallel repetition theorem due to Yuen to the anchored version of our games.

For every $n \in \mathbb{N}$, let $\mathcal{G}(H), w_\alpha$ and w_β be as in Theorem 6.3.6. By [Yue16, Theorem 41], there exists a $poly(n)$-computable transformation, called *anchoring*, that transforms $\mathcal{G}(H)$ to a two-player game $\mathcal{G}(H)_\perp$ with winning probability $1-\frac{1-w^*(\mathcal{G}(H))}{2}$. So $w^*(\mathcal{G}(H)_\perp) = \begin{cases} 1-\epsilon_\alpha/2 & \text{if } \lambda_0(H) \leqslant \alpha \\ 1-\epsilon_\beta/2 & \text{if } \lambda_0(H) \geqslant \beta \end{cases}$, where $\epsilon_\alpha := 1-w_\alpha$ and $\epsilon_\beta := 1-w_\beta$. Then by [Yue16, Theorem 42], there is a universal constant $C>0$ such that for all integer $m \geqslant 1$, and $\gamma \geqslant 0$, the probability that in the game $\mathcal{G}(H)_\perp^m$ the players can win more than $\big(w^*(\mathcal{G}(H)_\perp)+\gamma\big)m$ games is at most $(1-\gamma^9/2)^{Cm}$. Take $\gamma := \frac{\epsilon_\alpha-\epsilon_\beta}{4}$ and $m = \max\{4\gamma^{-2}, 2C\gamma^{-9}\}$. Let $\widehat{\mathcal{G}}(H) := \mathcal{G}(H)_\perp^m$ be the m parallel repeated anchoring version of $\mathcal{G}(H)$. We show that this nonlocal game has a constant completeness-soundness gap.

Theorem 6.3.7. *Let $\widehat{\omega}_\alpha$ (resp. $\widehat{\omega}_\beta$) be the maximum winning probability for $\widehat{\mathcal{G}}(H)$ when $\lambda_0(H) \leqslant \alpha$ (resp. $\lambda_0(H) \geqslant \beta$). Then $\widehat{\omega}_\alpha - \widehat{\omega}_\beta \geqslant 1/4$.*

Proof. If $\lambda_0(H) \geqslant \beta$, then $\widehat{\omega}_\beta \leqslant (1 - \frac{\gamma^9}{2})^{Cm} \leqslant (1 - \frac{\gamma^9}{2})^{2/\gamma^9} < e^{-1} < 1/2$. Now suppose $\lambda_0(H) \leqslant \alpha$. An optimal strategy S for $\mathcal{G}(H)_\perp$ has winning probability $1 - \frac{\epsilon_\alpha}{2}$. Let X be the random variable for the number of games the strategy S^m wins. Then $X \sim \text{Binomial}(m, 1 - \frac{\epsilon_\alpha}{2})$, so $\mathbb{E}X = m(1-\frac{\epsilon_\alpha}{2})$ and $\text{Var}X = m\frac{\epsilon_\alpha}{2}(1-\frac{\epsilon_\alpha}{2})$. Since $(1-\frac{\epsilon_\alpha}{2})-(1-\frac{\epsilon_\beta}{2}+\gamma) = \frac{\epsilon_\beta-\epsilon_\alpha}{2}-\gamma = \gamma$, we obtain that

$$\begin{aligned} Pr(X \leqslant (1 - \tfrac{\epsilon_\beta}{2} + \gamma)m) &= Pr((1 - \tfrac{\epsilon_\alpha}{2})m - X \geqslant \gamma m) \\ &\leqslant Pr(|X - \mathbb{E}X| \geqslant \gamma m) \\ &\leqslant \frac{m(1 - \frac{\epsilon_\alpha}{2})\frac{\epsilon_\alpha}{2}}{(\gamma m)^2} = \frac{1}{m\gamma^2} \leqslant 1/4. \end{aligned}$$

This implies $\widehat{\omega}_\alpha \geqslant w(S^m) = 1 - Pr(X \leqslant (1 - \frac{\epsilon_\beta}{2} + \gamma)m) \geqslant 3/4$, so the theorem follows. □

6.4 Zero-knowledge proof system

In this section, we show that the family of games described in Definition 6.3.3 provides a statistical zero-knowledge MIP*[2, 1] protocol for QMA with inverse polynomial completeness/soundness gap. First we introduce our protocol.

6.4.1 Simulation of history states for XZ-Hamiltonians

Before we introduce our MIP* protocol and proceed to our result on zero-knowledge, we reformulate a result, originally introduced by Broadbent and Grilo [BG22] (Lemma 3.5), so that it is more amenable to device-independent techniques.

Theorem 6.4.1 (Simulation of history states)**.** *For any language $L = (L_{yes}, L_{no})$ in* QMA *and $s \in \mathbb{N}$, there is a family of verification circuits $V_x^{(s)} = U_T \dots U_1$ for L that acts on*

a witness of size $p(|x|)$ and on $q(|x|)$ ancillary qubits such that there exists a polynomial-time deterministic algorithm $Sim_{V^{(s)}}$ that takes as input an instance $x \in L$ and a subset $S \subseteq [T+p+q]$ with $|S| \leqslant 3s+2$, then outputs a classical description of an $|S|$-qubit density matrix $\rho(x,S)$ with the following properties:

1. *If $x \in L_{yes}$, then there exists a $p(|x|)$-qubit witness ψ^s such that $V_x^{(s)}$ accept with probability at least $1-negl(n)$ on ψ^s and $\|\rho(x,S) - \mathrm{Tr}_{\overline{S}}(\rho)\|_{tr} \leqslant negl(|x|)$, where*

$$\rho = \frac{1}{T+1} \sum_{t,t' \in [T+1]} |unary(t)\rangle\langle unary(t)| \otimes U_t \dots U_1(\psi^s \otimes |0\rangle\langle 0|^{\otimes q})U_1^* \dots U_{t'}^*$$

   is the history state of $V_x^{(s)}$ on witness ψ^s.

2. *Let H_i be one of the terms from the circuit-to-local Hamiltonian construction from $V_x^{(s)}$, and let S_i be the set of qubits on which H_i acts non-trivially. Then $\mathrm{Tr}(H_i \rho(x,S_i)) = 0$ for all $x \in L$.*

3. *The Hamiltonian H from the circuit-to-local Hamiltonian construction is a 6-local Hamiltonian of XZ type.*

Proof. The first two points were proven by Broadbent and Grilo using simulatable codes constructed from a different set of physical gates [BG22]. In brief, Broadbent and Grilo provide a constructive approach which for each $x \in L$ provides a transformation from the original verification circuit V to a simulatable verification circuit $V_x^{(s)}$ that has 4 main stages:

(i) The verifier receives an encoded witness and checks if the provided witness is properly encoded under the relevant code $\mathcal{C}$,

(ii) creates auxiliary resource states $|0\rangle, |T\rangle$ and encodes them under $\mathcal{C}$,

(iii) performs an encoded version of the original verification circuit V on the encoded witness using either transversal Clifford gates or suitable encodings of T-gates, which use $|T\rangle$, and

(iv) decodes the output of the computation.

For each constant s the CECC $\mathcal{C}$ is taken to be $\log(3s+5)$-fold concatenated Steane code.

Theorem 6.1.8 is obtained by using the same code $\mathcal{C}$ and applying the 3-qubit Toffoli gate using resource state $|\text{Toffoli}\rangle$, which can be constructed from $|000\rangle$ using H and $\Lambda^2(X)$. The proof of our result then follows by appropriately changing the resource generation stage (ii) to create encodings of auxiliary states $|0\rangle$ and $|\text{Toffoli}\rangle$. Then stage (iii) is altered to instead apply an encoding of the original circuit using encodings of the gate set $\{H, \Lambda(X), \Lambda^2(X)\}$.

To see how this change of gate set gives us the third result, note that for any gate G we have $\Lambda(G) = \frac{1}{2}(I+Z)\otimes I + \frac{1}{2}(I-Z)\otimes G$. Using this decomposition we can readily check that gates $\Lambda(X)$ and $\Lambda^2(X)$ can both be expressed as a real linear combination of tensor products of X, Z, and I. The same holds for $H = \frac{1}{\sqrt{2}}(X+Z)$. Consequently, all physical gates used in stages (ii) and (iii) will consist of gates that can be expressed as real linear combinations of tensors of X and Z. The same is true for physical gates used in stages $i)$ and $iv)$. We will also have that all of these gates are of order 2. Finally, following the same approach due to Ji (Lemma 22 [Ji16]), we get H is 6-local and of XZ type. □

Below we only need to invoke Theorem 6.4.1 for the case of $s = 2$ in order to our zero-knowledge protocol. We use V_x to denote $V_x^{(2)}$ throughout the rest of this section.

6.4.2 A two prover zero-knowledge proof system for QMA

Let $L = (L_{yes}, L_{no})$ be a language in QMA. Figure 6.4 describes a two-prover one-round interactive proof system for L with a constant polynomial completeness-soundness gap.

To put it more concretely, for any $x \in L$, applying Theorem 6.4.1, with $s = 2$, provides a $poly(|x|)$-size verification circuit V_x, and the circuit-to-Hamiltonian construction creates a $poly(|x|)$-qubit 6-local Hamiltonian H_x of XZ-type. We can then construct a non-local game $\widehat{\mathcal{G}}_x$ as in Section 6.3. The constant completeness-soundness gap follows from

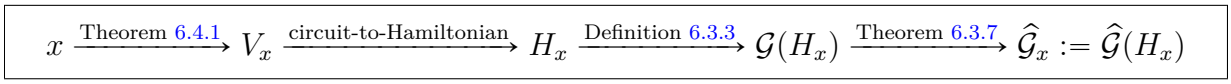


Figure 6.4: x is an instance in $L \in \mathsf{QMA}$. V_x is a $poly(|x|)$-size quantum circuit. H_x is a $poly(|x|)$-qubit 6-local Hamiltonian of XZ-type. $\widehat{\mathcal{G}}_x$ is a nonlocal game with $poly(|x|)$-bit questions and $poly(|x|)$-bit answers.

Theorem 6.3.7. The map from instances $x \in L$ to nonlocal games $\widehat{\mathcal{G}}_x$ is efficient since each step described in Figure 6.4 is efficient.

To prove the above interactive proof system for L has the statistical zero-knowledge property, we first establish that any malicious verifier $\widehat{V}$ and $x \in L_{yes}$, there exists a PPT simulator that can sample from $View(\widehat{V}(x), \mathcal{S}_h)$, where $\mathcal{S}_h$ is the honest strategy for $\mathcal{G}_x$ defined in Section 6.3.

Lemma 6.4.2. *Suppose $x \in L_{yes}$ for some language $L = (L_{yes}, L_{no})$ in QMA. Let $\mathcal{G}_x$ be the corresponding nonlocal game described in Figure 6.4, and let $\mathcal{S}_h$ be the honest strategy for $\mathcal{G}_x$ defined in Section 6.3. For any malicious verifier $\widehat{V}$ there exists a PPT algorithm $Sim_{\widehat{V}}$ with output distribution negligibly close to $View(\widehat{V}(x), \mathcal{S}_h)$,*

Proof. Let H_x be the corresponding Hamiltonian, and suppose H_x acts on n qubits ($n = poly(|x|)$). Recall that, in $\mathcal{S}_h$, Alice and Bob measure on a shared n-EPR pair $|\Phi_{\text{EPR}}^{\otimes n}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. Bob has an addition n-qubit register $\mathcal{H}_{B'}$ holding a copy of the ground state ρ of H_x. Let $\mathcal{H}_{A,i}, \mathcal{H}_{B,i}$ and $\mathcal{H}_{B',i}$ be the i-th qubit of Alice or Bob on their respective registers.

A malicious verifier $\widehat{V}$ samples its first question q_1 using some distribution on the set of all possible questions for Alice or Bob. Given a response r_1 the second question q_2 is conditionally sampled using distribution. Since $\widehat{V}$ is PPT the simulator $Sim_{\widehat{V}}$ can also sample from these distributions given the same randomness. We consider the cases below for conditionally generating the responses.

If neither question q_1 nor q_2 are requests for energy test then in the honest strategy both players will make one or more Pauli measurements on their shared n-EPR pairs, and hence the simulator can efficiently produce responses. Here the order of the players will

not matter as the simulator can first randomly generate the response r_1 of the first player and compute the appropriate response r_2 of the second conditional on the previous entries in the transcript.

Suppose q_1 is a request for an energy test sent to Bob. In the honest strategy, Bob performs n Bell measurements on $\mathcal{H}_B \otimes \mathcal{H}_{B'}$. The simulator can produce a response r_1 conditional on Bob receiving a request for energy test by sampling $2n$ uniformly random bits $(\alpha, \beta) = (\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_n)$. In the honest strategy Alice should now have $\rho_{\alpha,\beta} := \sigma_Z^\beta \sigma_X^\alpha \rho \sigma_X^\alpha \sigma_Z^\beta$ on her register $\mathcal{H}_A$, where σ_W^r denotes $\otimes_{i\in[n]} \sigma_W^{r_i}$ for $W \in \{X, Z\}$ and $r \in \{0,1\}^n$.

It follows that q_2 must be a measurement request for Alice. This can be either of the form $\sigma_W(a)$ for some $W \in \{X, Z, I\}^n$ and $a \in \{0,1\}^n$ with $|a| \leqslant 6$, or $\sigma_{XZ} \otimes \sigma_{ZX}(a)$ with $|a| = 2$. If S is the set of qubits on which Alice's observable acts non-trivially then by Theorem 6.4.1 there exists a polynomial time algorithm which can output a description of a density matrix $\rho(x, S)$ satisfying

$$\|\mathrm{Tr}_{\overline{S}}(\rho) - \rho(x, S)\|_{tr} \leqslant negl(n). \tag{6.4.1}$$

$Sim_{\hat{V}}$ can then append r_2 to the transcript using an approximation for Alice's honest measurement result on the qubits in S of $\rho_{\alpha,\beta}$. This approximation can then be calculated using $\rho(x, S)$ since

$$\mathrm{Tr}_{\overline{S}}(\sigma_Z^\beta \sigma_X^\alpha \rho \sigma_X^\alpha \sigma_Z^\beta) = \big(\bigotimes_{i\in S} \sigma_Z^{b_i} \sigma_X^{a_i}\big) \mathrm{Tr}_{\overline{S}}(\rho) \big(\bigotimes_{i\in S} \sigma_Z^{b_i} \sigma_X^{ai}\big).$$

Lastly, we consider the case that Alice is first given a measurement request q_1 and after receiving response r_1 the verifier sends an energy test request to Bob for q_2. In order to generate a response for Alice the simulator will first generate a uniformly random response r_1. We take Φ_{q_1,r_1} denote the post measurement state on $\mathcal{H}_A \otimes \mathcal{H}_B$ obtained by measuring the shared EPR pairs according to q_1 and obtaining outcome r_1. In the honest strategy, the overall shared state will be

$$\tau_{q_1,r_1} := \Phi_{q_1,r_1} \otimes \rho \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'},$$

and Bob will perform independent Bell measurements on the registers $\mathcal{H}_B \otimes \mathcal{H}_{B'}$. Again we take S to denote the set of qubits on which Alice measured given question q_1. Then we

have

$$\mathrm{Tr}_{\overline{S}}(\tau_{q_1,r_1}) = \mathrm{Tr}_{\overline{S}}(\Phi_{q_1,r_1}) \otimes \mathrm{Tr}_{\overline{S}}(\rho).$$

It follows from Equation (6.4.1) that

$$\|\mathrm{Tr}_{\overline{S}}(\tau_{q_1,r_1}) - \mathrm{Tr}_{\overline{S}}(\Phi_{q_1,r_1}) \otimes \rho(x,S)\|_{tr} \leqslant \mathrm{negl}(n).$$

Thus the simulator can generate the conditional response $(\alpha, \beta) = (\alpha_i, \beta_i)_i$ as follows. First compute reduced density matrix $\rho(x, S)$ from Theorem 6.4.1. For $i \in S$ sample (α_i, β_i) according to the probability of each possible Bell measurement result on $\mathrm{Tr}_{\overline{S}}(\Phi_{q_1,r_1}) \otimes \rho(x, S)$. For the remaining $i \notin S$ the simulator can sample uniformly random pairs (α_i, β_i).

In all of the above cases, the output of the simulator will be guaranteed negligibly close and thus the output of $Sim_{\widehat{V}}$ is negligibly close to $View(x, \mathcal{S})$. □

All that remains is to argue that the interactive protocol described in Figure 6.4 based on the scaled-up game $\widehat{\mathcal{G}}_x$ is statistically zero-knowledge.

Theorem 6.4.3. *The protocol described in Figure 6.4 is statistical zero-knowledge and has a constant completeness-soundness gap.*

Proof. The constant completeness-soundness gap follows directly from Theorem 6.3.7. To show the statistical zero-knowledge, we first consider the anchoring procedure for the game $\mathcal{G}_x$. We can specify an honest strategy $\mathcal{S}_{h,\perp}$ for the anchored version of $\mathcal{G}_x$ by fixing a choice of output for either player who receives question $\perp$ in the honest strategy. Then, given any malicious verifier $\widehat{V}(x)$, the simulator given in Theorem 6.4.3 can be trivially modified to sample from a distribution which is negligibly close to $View(\widehat{V}(x), \mathcal{S}_{h,\perp})$.

In the case of the threshold parallel repeated game $\widehat{\mathcal{G}}_x$, the honest strategy $\mathcal{S}^m_{h,\perp}$ is taken to be the m-fold product of the honest strategy $\mathcal{S}_{h,\perp}$. Then, as commented in [GSY19], since the protocol only queries each player once, a new simulator can be obtained by sampling according to the m-fold product of the simulator used in the above lemma. □

6.5 Off-the-shelf model

In this section, we formally define the OTS model (Section 6.5.1). In Section 6.5.2, we state our main conceptual theorems, which make use of all the technical contributions in the main part of this work.

6.5.1 Formal description of the model

Here we provide a formal description of the OTS model. This model is defined as a refinement of MIP^*, where the completeness condition is weakened, allowing only one of the provers to be "all-powerful", while the other has limited functionality determined independently of the problem instance.

Off-the-shelf device. We first formalize the definition of a family of off-the-shelf devices. A *verification device* $D = (|\psi\rangle, \{P_a^1\}_a, \ldots, \{P_a^q\}_a)$ consists of a state $|\psi\rangle$ on Hilbert spaces $\mathcal{K}_A \otimes \mathcal{K}_B$ and a collection of POVMs $\{P_a^1\}_a, \ldots, \{P_a^q\}_a$ on $\mathcal{K}_A$. We say that a quantum strategy $\mathcal{S} = (\mathcal{H}_A, \mathcal{H}_B, \{E_a^x\}, \{F_b^y\}, |\phi\rangle)$ can be *implemented* using D, if three conditions hold:

(i) $\mathcal{H}_A = \mathcal{K}_A$ and $\mathcal{H}_B = \mathcal{K}_B \otimes \mathcal{K}_{B'}$ for some Hilbert space $\mathcal{K}_{B'}$.

(ii) The set of measurements in $\mathcal{S}$ which act on $\mathcal{H}_A$ are contained in D.

(iii) The shared state $|\phi\rangle$ in $\mathcal{S}$ can be decomposed as $|\phi\rangle = |\psi\rangle \otimes |\phi'\rangle$ where $|\psi\rangle$ is the state in D and $|\phi'\rangle$ is some auxiliary state held on a Hilbert space $\mathcal{K}_{B'}$.

Note that if a quantum strategy $\mathcal{S}$ can be implemented using a verification device D, then the overall system is decomposed as $\mathcal{H}_A \otimes \mathcal{H}_B = \mathcal{K}_A \otimes \mathcal{K}_B \otimes \mathcal{K}_{B'}$. Informally, we view this decomposition as consisting of an entangled state $|\psi\rangle$ shared between the device and a single prover, together with an auxiliary state $|\phi'\rangle$ accessible only to the prover.

Given a collection of verification devices $\{D_n\}_{n\in\mathbb{N}}$, where each D_n consists of a state $|\psi_n\rangle$ and a sequence of POVMs, we say $\{D_n\}_{n\in\mathbb{N}}$ is an *efficient family of off-the-shelf devices* if there exists a polynomial-time uniform family of quantum circuits $\{Q_n\}_{n\in\mathbb{N}}$ satisfying the following: Q_n generates the state $|\psi_n\rangle$ from an all 0 state, and on input i measures $|\psi_n\rangle$ using the i-th POVM from D_n.

Definition 6.5.1. *A promise language $L = (L_{yes}, L_{no})$ has an off-the-shelf (OTS) proof system if there exists an efficient family of off-the-shelf devices $\{D_n\}_{n\in\mathbb{N}}$, and a polynomial-time computable function that takes an instance x to the description of a non-local game $\mathcal{G}_x$ satisfying the following:*

1. ***Completeness using off-the-shelf devices.*** *For any $x \in L_{yes}$ with $|x| \leqslant n$, there exists a quantum strategy $\mathcal{S}_x$, which can be implemented using D_n, obtaining $\omega(\mathcal{G}_x, \mathcal{S}_x) \geqslant c$.*

2. ***Soundness.*** *For any $x \in L_{no}$ we have $\omega^*(\mathcal{G}_x) < s$.*

We use OTS *to denote the class of all languages L which admits an OTS proof system with a constant completeness-soundness gap.*

Any OTS proof system is described as a special instance of a 2-player, 1-round MIP^* proof system with additional constraints regarding the completeness condition and we say that an OTS proof system is statistically zero-knowledge if it is statistically zero-knowledge as an MIP^* proof system (see Definition 2.3.4 for details).

6.5.2 Applications to ZK and delegated computation

In this section, we show that any language in QMA admits a statistical zero-knowledge OTS proof system. We also consider how the OTS model can be scaled down to provide a protocol for verifiable delegated quantum computation.

Theorem 6.5.2. *For every language L in* QMA*, there exists a statistical zero-knowledge OTS proof system for L with constant completeness and soundness gap.*

Proof. We will be working with the proof system sending an instance x to game $\widehat{\mathcal{G}}_x$, as described in Figure 6.4. Using the rigidity results in Section 6.2, we have already shown completeness and soundness of properties of the individual game $\widehat{\mathcal{G}}_x$ in Section 6.3. The ZK property of this game has also been shown in Section 6.4. All that remains to show is that this protocol further satisfies the extra restrictions of completeness using off-the-shelf devices outlined in Definition 6.5.1. That is, we need to show that there exists an efficient family of off-the-shelf devices $\{D_n\}$ which can implement the honest strategy $\mathcal{S}_x$ for all yes instances x.

For each $L \in \mathsf{QMA}$, there exists a polynomial f such that, for all $x \in L$ of size $|x| = n$ the corresponding Hamiltonian H_x is supported on at most $f(n)$ qubits. Next suppose $x \in L_{yes}$ with $|x| \leqslant n$. In the honest strategy for the game $\mathcal{G}_x$, Alice and Bob share at most $f(n)$-EPR pairs, additionally, Bob privately holds a ground state ρ for H_x. The measurements required by Alice always correspond to σ_X or σ_Z on up to 6 qubits of the shared EPR pairs, or $\sigma_X\sigma_Z \otimes \sigma_Z\sigma_X$ on two qubits. In the honest strategy $\mathcal{S}_x$ for the m-fold parallel repeated anchoring game $\widehat{\mathcal{G}}_x$, the players share $mf(n)$-EPR pairs and Alice's measures in σ_X or σ_Z on up to $6m$ qubits or measures with $\sigma_X\sigma_Z \otimes \sigma_Z\sigma_X$ on $2m$ qubits. Since $m = poly(n)$, we then satisfy the completeness condition required by specifying an efficient family of off-the-shelf devices $\{D_n\}$, where for each n the verification device D_n contains $mf(n)$-EPR pairs and all of the above required Pauli measurements on up to $6m$ qubits. □

In our application towards delegated quantum computation, we consider a novel type of interactive protocol, where in addition to exchanging classical messages, the server can send an untrusted verification device, as defined in Section 6.5.1, to the client (see Section 6.1). In Figure 6.5, we consider the case where in the first "message", called a set-up stage, the prover sends an untrusted verification device, which is followed by classical communication.

Putting these observations together with Theorem 6.5.2, we obtain the following result on delegated quantum computation.

Theorem 6.5.3. *For every language L in BQP, there is a statistical-zero-knowledge delegation protocol as outlined in Figure 6.5 for L with constant completeness and soundness*

1. **Set-up:** The client sends a set-up parameter $k \in \mathbb{N}$ to the server who provides a verification device D_k from an efficient family of off-the-shelf devices $\{D_n\}_n$.

2. **Choice of computation:** The client sends a classical description of circuit Q, satisfying $|Q| \leqslant k$ to the server.

3. **Verifiable delegation:** The client plays a 1-round game $\widehat{\mathcal{G}}_Q$, using the server and device D_k as players. The client accepts if and only if the game is won.

Figure 6.5: A delegation protocol between a polynomial-time classical client and polynomial-time quantum server, who provides an untrusted verification device during set-up.

gap.

Theorem 6.5.3 holds largely due to the fact that it can be viewed as a particular application of Theorem 6.5.2 in the setting of a BQP-complete problem. The only additional technical requirement occurs in step 3, in which an honest polynomial-time quantum prover is required to be able to saturate the optimal winning probability of the corresponding game. We provide the following sketch.

Proof. (Sketch) We can view the BQP-complete problem from Definition 2.2.1 as a language in QMA. This allows us to apply the efficient mapping outlined in Figure 6.4 to obtain a corresponding game $\widehat{\mathcal{G}}_Q$. In this case, the ground state of the underlying Hamiltonian can be prepared by a polynomial-time quantum prover. Thus, as in the proof of Theorem 6.5.2, we can define the required polynomial-time uniform family of off-the-shelf devices $\{D_n\}_{n\in\mathbb{N}}$ by taking D_n to contain suitably many EPR pairs, as well as the required Pauli measurements. Since furthermore the required ground state can always be prepared by a polynomial-time quantum prover, an honest server can obtain the required completeness in Step 3 by generating this state and teleporting it to the verification device when required. We also have that the above delegation protocol inherits the ZK property via the results of Theorem 6.5.2. □

Chapter 7

Decision problems in operator algebras

7.1 Motivation and overview

Let $\mathcal{A}$ be the free $*$-algebra with at least two generators. As discussed in Section 1.3, there is an effective way to determine whether a given $*$-polynomial (with rational coefficients) in $\mathcal{A}$ is positive in all representations by searching through sums of squares decomposition. The purpose of the chapter is to show that no such procedure exists for $\mathcal{A} \otimes \mathcal{A}$: determine whether an element of $\mathcal{A} \otimes \mathcal{A}$ is positive is undecidable.

Theorem 7.1.1. *Let $\mathcal{A}_{\mathbb{Q}}$ be one of the algebras $\mathbb{Q}^*\langle x_1, \ldots, x_n \rangle$ or $\mathbb{Q}\mathcal{F}_n$ for $n \geqslant 2$, or $\mathbb{Q}\mathbb{Z}_m^{*n}$ for $n \geqslant 3$, $m \geqslant 2$ or $n \geqslant 2$, $m \geqslant 3$, and let $\mathcal{A} = \mathcal{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C}$ be the complexification. Then the decision problem*

$$\text{Given } \alpha \in \mathcal{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{A}_{\mathbb{Q}}, \text{ is } \alpha \text{ positive as an element of } \mathcal{A} \otimes_{\mathbb{C}} \mathcal{A}? \tag{Pos}$$

is coRE-hard.

Specifically, we show that there is a computable mapping from Turing machines M to self-adjoint elements $\alpha_M \in \mathcal{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{A}_{\mathbb{Q}}$, such that α_M is positive if and only if M does not

halt. The bounds on n and m in Theorem 7.1.1 are tight, as the algebras $\mathbb{Q}^*\langle x\rangle \otimes \mathbb{Q}^*\langle x\rangle = \mathbb{Q}[x_1, x_2]$, $\mathbb{Q}\mathcal{F}_1 \otimes \mathbb{Q}\mathcal{F}_1 = \mathbb{Q}\mathbb{Z} \times \mathbb{Z}$, and $\mathbb{Q}\mathbb{Z}_m \times \mathbb{Q}\mathbb{Z}_m$ are commutative, and positivity is also decidable for $\mathbb{Q}\mathbb{Z}_2^{*2} \times \mathbb{Z}_2^{*2}$ (see Example 7.6.8). As an immediate corollary of Theorem 7.1.1, we get:

Corollary 7.1.2. *Let $\mathcal{A}_{\mathbb{Q}}$ be one of the algebras $\mathbb{Q}^*\langle x_1, \ldots, x_n\rangle$ or $\mathbb{Q}\mathcal{F}_n$ for $n \geqslant 2$, or $\mathbb{Q}\mathbb{Z}_m^{*n}$ for $n \geqslant 3$, $m \geqslant 2$ or $n \geqslant 2$, $m \geqslant 3$, and let $\mathcal{A}$ be the complexification. Then there are elements of $\mathcal{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{A}_{\mathbb{Q}}$ which are positive, but are not sums of hermitian squares in $\mathcal{A} \otimes_{\mathbb{C}} \mathcal{A}$, so $\mathcal{A} \otimes_{\mathbb{C}} \mathcal{A}$ does not have the SOS property.*

Proof. If every element of $\mathcal{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{A}_{\mathbb{Q}}$ is a sum of squares in $\mathcal{A} \otimes_{\mathbb{C}} \mathcal{A}$, then the problem of deciding whether elements of $\mathcal{A} \otimes \mathcal{A}$ are positive is contained in RE by searching through SOS decompositions. Since coRE is not contained in RE, this is not possible. □

For the algebras $\mathbb{Q}\mathcal{F}_n$ and $\mathbb{Q}\mathbb{Z}_m^{*n}$, $m \geqslant 3$, the hypothesis $n \geqslant 2$ in Corollary 7.1.2 is necessary, since finite-dimensional C^*-algebras like $\mathbb{C}\mathbb{Z}_m \times \mathbb{Z}_m$ always have the SOS property, and $\mathbb{C}\mathbb{Z} \times \mathbb{Z}$ has the SOS property by a result of Scheiderer [Sch06]. We do not know if $\mathbb{C}\mathbb{Z}_2^{*2} \times \mathbb{Z}_2^{*2}$ has the SOS property. For $\mathcal{A}_{\mathbb{Q}} = \mathbb{Q}^*\langle x_1, \ldots, x_n\rangle$, the corollary already follows (for all $n \geqslant 1$) from the fact that $\mathbb{C}[x, y]$ does not have the SOS property; indeed, if $p(x, y)$ is a positive polynomial in $\mathbb{C}[x, y]$ which is not a sum of squares, then $p(x_1 \otimes 1, 1 \otimes x_1)$ is positive in $\mathcal{A} \otimes \mathcal{A}$, but does not have a sum of squares decomposition. The Motzkin polynomials provide explicit examples of positive polynomials in $\mathbb{Q}[x, y]$ which are not sums of squares, although of course they are sums of squares of rational functions by Artin's theorem. Corollary 7.1.2 does not seem to have been known for $\mathcal{A}_{\mathbb{Q}} = \mathbb{Q}\mathcal{F}_n$ and $\mathbb{Q}\mathbb{Z}_m^{*n}$; however, Theorem 7.1.1 is stronger, in that SOS decompositions can be replaced in Corollary 7.1.2 with any other certificate of positivity. For instance, for $\mathcal{A}_{\mathbb{Q}} = \mathbb{Q}^*\langle x_1, \ldots, x_n\rangle$ with $n \geqslant 2$, there are positive elements of $\mathcal{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{A}_{\mathbb{Q}}$ which are not sums of squares of noncommutative rational functions in the sense of [KSV23]. The proof of Theorem 7.1.1 is given in Section 7.6. We actually prove a more general statement (Theorem 7.6.1), which applies to other algebras including the algebra of bounded contractions.

The proof of Theorem 7.6.1 is by reduction to tracial positivity. An element α of a $*$-algebra $\mathcal{A}$ is said to be *trace-positive* if $\tau(\alpha) \geqslant 0$ for all (bounded) tracial states τ on $\mathcal{A}$. We show that tracial positivity is undecidable for free $*$-polynomials and group algebras:

Theorem 7.1.3. *Let $\mathcal{A}_{\mathbb{Q}}$ be one of the algebras $\mathbb{Q}^*\langle x_1, \ldots, x_N\rangle$, $\mathbb{Q}\mathcal{F}_N$, or $\mathbb{Q}\mathbb{Z}_m^{*N}$ for $m \geqslant 2$. If N is large enough, then the decision problem*

$$\text{Given } \alpha \in \mathcal{A}_{\mathbb{Q}}, \text{ is } \alpha \text{ trace-positive as an element of } \mathcal{A}? \tag{TrPos}$$

is coRE-hard.

Klep and Schweighofer [KS08a] prove an analog of Helton and McCullough's positivstellensatz for the algebra of bounded contractions: an element α is trace-positive if and only if $\alpha + \epsilon$ is a sum of hermitian squares and commutators for all $\epsilon > 0$. This is extended to free group algebras by Juschenko and Popovych [JP11], to archimedean algebras by Ozawa [Oza13], and to $\mathbb{Q}^*\langle x_1, \ldots, x_n\rangle$ by Klep, Scheiderer, and Volčič [KSV23]. Quarez [Qua15] (see also [KSV23, Example 3.2]) gives examples of trace-positive polynomials in $\mathbb{Q}^*\langle x_1, x_2\rangle$ which are not sums of hermitian squares and commutators, but which are sums of squares and commutators of noncommutative rational functions. As in Corollary 7.1.2, Theorem 7.1.3 immediately implies that all the algebras listed in the theorem contain trace-positive elements which are not sums of squares and commutators of noncommutative rational functions. Unlike Theorem 7.1.1, we do not know the smallest bound N such that Theorem 7.1.3 holds.

Part of the motivation for Theorem 7.1.1 comes from Kirchberg's reformulation of the Connes embedding problem, sometimes called Kirchberg's conjecture [Kir93], and the recent MIP*=RE theorem of Ji, Natarajan, Vidick, Wright, and Yuen [JNV+20], which resolves this conjecture. Kirchberg's conjecture asks whether the max and min tensor norms on $\mathbb{C}\mathcal{F}_n \otimes \mathcal{F}_n = \mathbb{C}\mathcal{F}_n \times \mathcal{F}_n$ agree for $n \geqslant 2$ [Kir93]. As Ozawa observes [Oza04, Oza13], if $\mathcal{A}$ is archimedean and RFD, then the max and min tensor norms on $\mathcal{A} \otimes \mathcal{A}$ agree if and only if $\mathcal{A} \otimes \mathcal{A}$ is RFD, so Kirchberg's conjecture is equivalent to whether $\mathbb{C}\mathcal{F}_n \otimes \mathbb{C}\mathcal{F}_n = \mathbb{C}\mathcal{F}_n \times \mathcal{F}_n$ is RFD. Kirchberg's conjecture is still equivalent to the Connes embedding problem if $\mathcal{F}_n$ is replaced by $\mathbb{Z}_m^{*n}$ for $n \geqslant 3$, $m \geqslant 2$ or $n \geqslant 2$, $m \geqslant 3$ [Oza13, Fri12]. The algebras $\mathbb{C}\mathbb{Z}_m^{*n} \otimes$

$\mathbb{C}\mathbb{Z}_m^{*n}$ are of particular interest in quantum information, since they correspond to bipartite (meaning composed of two spatially separated subsystems) measurement scenarios with n measurement settings and m measurement outcomes per subsystem, and they are closely connected with the complexity class MIP* of multiprover interactive proof systems with entangled provers.

The main result of [JNV+20] is that MIP* is equal to RE, the class of recursively enumerable languages. In algebraic language, this implies that there is a computable mapping from Turing machines M to elements $\alpha_M \in \overline{\mathbb{Q}}\mathbb{Z}_m^{*n} \times \mathbb{Z}_m^{*n}$ (where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$, and m and n also depend on M), such that if M halts then α_M is not positive in finite-dimensional representations of $\mathbb{C}\mathbb{Z}_m^{*n} \times \mathbb{Z}_m^{*n}$, and if M does not halt, then $\alpha_M - 1$ is positive in finite-dimensional representations of $\mathbb{C}\mathbb{Z}_m^{*n} \times \mathbb{Z}_m^{*n}$. This shows that the promise problem

> Given $n, m \geqslant 1$ and $\alpha \in \overline{\mathbb{Q}}\mathbb{Z}_m^{*n} \times \mathbb{Z}_m^{*n}$, determine if either $\alpha - 1$ is positive in finite-dimensional representations, or α is not positive in some finite-dimensional representation, promised that one of the two is the case. (GapFDPos)

is coRE-hard, so it is undecidable to determine if an element of $\mathbb{C}\mathbb{Z}_m^{*n} \times \mathbb{Z}_m^{*n}$ is strictly positive in finite-dimensional representations. If $\mathbb{C}\mathbb{Z}_m^{*n} \times \mathbb{Z}_m^{*n}$ were RFD, then (GapFDPos) would be equivalent to the promise problem

> Given $n, m \geqslant 1$ and $\alpha \in \overline{\mathbb{Q}}\mathbb{Z}_m^{*n} \times \mathbb{Z}_m^{*n}$, determine if either $\alpha - 1$ is positive, or α is not positive, promised that one of the two is the case. (GapPos)

Note that $\alpha - 1$ is positive if and only if α is strictly positive with spectrum contained in $[1, +\infty)$, so (GapPos) is a "gapped" version of the decision problem (Pos) considered in Theorem 7.1.1 (albeit with $\mathbb{Q}$ replaced by $\overline{\mathbb{Q}}$, and n and m allowed to vary). By Helton and McCullough's positivstellensatz, if $\alpha - 1$ is positive then α has an SOS decomposition proving positivity, so unlike (Pos), the problem (GapPos) is contained in RE. Since RE does not contain coRE, (GapPos) cannot be coRE-hard, and hence the MIP*=RE theorem implies that $\mathbb{C}\mathbb{Z}_m^{*n} \times \mathbb{Z}_m^{*n}$ is not RFD for large enough n and m.

There is a natural complement to the $\mathrm{MIP}^* = \mathrm{RE}$ theorem called the $\mathrm{MIP}^{\mathrm{co}} = \mathrm{coRE}$ conjecture, which if true would imply (GapPos) is RE-complete, and hence that (Pos) is RE-hard for $\mathcal{A} = \mathbb{C}\mathbb{Z}_m^{*n}$ (assuming again that $\mathbb{Q}$ is replaced by $\overline{\mathbb{Q}}$, and n and m are allowed to vary). If $\mathcal{A} \otimes \mathcal{A}$ is RFD, then (Pos) is contained in coRE, so showing that (Pos) is RE-hard for $\mathcal{A} = \mathbb{C}\mathbb{Z}_m^{*n}$ (with or without varying n and m) would give another disproof of the Connes embedding problem. Proving that (GapPos) is RE-complete would also imply that it is undecidable to determine if $\alpha \in \mathbb{C}\mathbb{Z}_m^{*n} \times \mathbb{Z}_m^{*n}$ is a sum of squares. On the other hand, because (GapPos) is contained in RE, hardness results for (GapPos) cannot be used to prove Corollary 7.1.2, and Theorem 7.1.1 is not true if (Pos) is replaced by (GapPos). Hence Theorem 7.1.1 and the $\mathrm{MIP}^{\mathrm{co}} = \mathrm{coRE}$ conjecture seem to be complementary. In any case, the proof methods we used here are different from the methods used in the proof of $\mathrm{MIP}^* = \mathrm{RE}$, and our techniques do not appear to be applicable to the $\mathrm{MIP}^{\mathrm{co}} = \mathrm{coRE}$ conjecture.

As mentioned above, the only upper bound we have on (Pos) is Π_2^0. If (Pos) contains both RE and coRE, then it seems possible that it is equal to Π_2^0, and we conjecture that this is the case for all the algebras in Theorem 7.1.1.

Conjecture 7.1.4. *Let $\mathcal{A}_{\mathbb{Q}}$ be one of the algebras $\mathbb{Q}^*\langle x_1, \ldots, x_n\rangle$ or $\mathbb{Q}\mathcal{F}_n$ for $n \geqslant 2$, or $\mathbb{Q}\mathbb{Z}_m^{*n}$ for $n \geqslant 3$, $m \geqslant 2$ or $n \geqslant 2$, $m \geqslant 3$, and let $\mathcal{A}$ be the complexification. Then the decision problem (Pos) from Theorem 7.1.1 is Π_2^0-complete.*

Tracial positivity has also been studied in connection with the Connes embedding problem [Had01, KS08a, BDKS14, JP11, Oza13], and the above connection with $\mathrm{MIP}^* = \mathrm{RE}$ and $\mathrm{MIP}^{\mathrm{co}} = \mathrm{coRE}$ could be described equally as well in terms of tracial positivity and MIP protocols with synchronous strategies (see e.g. [HMPS19, KPS18, MNY22, NZ23]). For tracial positivity, we make the following conjecture.

Conjecture 7.1.5. *Let $\mathcal{A}_{\mathbb{Q}}$ be one of the algebras $\mathbb{Q}^*\langle x_1, \ldots, x_N\rangle$, $\mathbb{Q}\mathcal{F}_N$, or $\mathbb{Q}\mathbb{Z}_m^{*N}$ for $m \geqslant 2$, and let $\mathcal{A}$ be the complexification. If N is large enough, then the decision problem (TrPos) from Theorem 7.1.3 is Π_2^0-complete.*

If Conjecture 7.1.5 is true, an additional problem is to find, for each algebra listed above, the smallest bound on N such that the decision problem (TrPos) is Π_2^0-complete.

7.2 Preliminaries

We use some more advanced concepts from group theory. Suppose S is a finite set of generators for a group G, and let $\mathcal{L}$ be the set of words over $S \cup S^{-1}$ which are trivial in G. The word problem for G is the problem of determining whether a word over $S \cup S^{-1}$ belongs to $\mathcal{L}$. Accordingly, we say that the word problem for G with respect to S is solvable in non-deterministic time $T : \mathbb{N} \to \mathbb{N}$ (resp. is in NP) if $\mathcal{L}$ can be recognized in time T (resp. in polynomial time).

If G has generating set S (not necessarily finite), a normal form for G with respect to S is a function η from words over $S \cup S^{-1}$ to words over $S \cup S^{-1}$, such that $\eta(x) = x$ in G for all words x, and two words x and y are equal in G if and only if $\eta(x) = \eta(y)$. Equivalently, a normal form can be specified as a function η from G to words over $S \cup S^{-1}$, such that $\eta(g) = g$ in G for all $g \in G$.

We denote the free product of a family of groups $\{G_i\}_{i \in I}$ by $*_{i \in I} G_i$, and the product by $\prod_{i \in I} G_i$. If $\{G_i\}_{i \in I}$ is a family of groups, K is a group, and $\phi_i : K \to G_i$ are injective homomorphisms, then the amalgamated free product of the family over K is

$$ {}_K *_i G_i := \langle *_{i \in I} G_i : \phi_i(k) = \phi_j(k) \text{ for all } k \in K, i, j \in I \rangle.$$

If $\phi_i(K)$ is in the centre of G_i for all $i \in I$, then the central product of this family over K is defined to be

$$ {}_K\prod\nolimits_i G_i := \langle \prod_i G_i : \phi_i(k) = \phi_j(k) \text{ for all } k \in K, i, j \in I \rangle.$$

In both cases, if we identify K with $\phi_i(K)$, then the image of K inside ${}_K *_i G_i$ and ${}_K\prod_i G_i$ is independent of what i we pick. Note that given a generating set S for K, we only need the relations $\phi_i(k) = \phi_j(k)$ for all $k \in S$ in the above presentations.

For each $i \in I$, let $A_i \subset G_i$ be a set of right coset representatives for $\phi_i(K)$, where we pick the identity element $\mathbb{1}$ as the representative of $\phi_i(K)$ itself. The normal form theorem for amalgamated free products states that every element $g \in {}_K *_i G_i$ can be written uniquely as $g = k g_1 \cdots g_m$, where $k \in K$, and $g_j \in A_{i_j} \backslash \{1\}$ for some sequence

$i_1, \ldots, i_m \in I$ with $i_j \neq i_{j+1}$ for all $1 \leqslant j < m$. While the normal form theorem for amalgamated free products does not give us a normal form of g in the above sense, if η is a normal form for K with respect to generating set S, and η_i is a normal form for G_i with respect to generating set S_i, $i \in I$, then $g \mapsto \eta(k)\eta_{i_1}(g_1)\cdots\eta_{i_m}(g_m)$ is a normal form for ${}_K *_i G_i$ with respect to generating set $S \sqcup \coprod_{i\in I} S_i$ (where $\coprod$ is the disjoint union). Similarly, if we pick an ordering for I, the normal form theorem for central products states that every element $g \in {}_K\prod_i G_i$ can be written uniquely as $kg_1 \cdots g_m$, where $k \in K$, and $g_i \in A_{i_j}\backslash\{1\}$ for some increasing sequence $i_1 < i_2 < \ldots < i_m$ in I. Again, if η is a normal form for K and η_i is a normal form for G_i, $i \in I$, then $g \mapsto \eta(k)\eta_{i_1}(g_1)\cdots\eta_{i_m}(g_m)$ is a normal form for ${}_K\prod_i G_i$. In both cases, the normal form theorem implies that the natural inclusions $G_j \hookrightarrow {}_K *_i G_i$ and $G_j \hookrightarrow {}_K\prod_i G_i$ are injections for all j, so G_j can be regarded as a subgroup of the amalgamated free product or central product. One application of amalgamated free products that we will use is the following lemma:

Lemma 7.2.1. *Let $G = \langle S : R\rangle$. For any $y \in S$, G is a subgroup of*

$$H := \langle G, s, t : y = st, s^2 = t^2 = 1\rangle$$

via the natural inclusion.

Proof. Suppose y has order $k \in \mathbb{N} \cup \{+\infty\}$. Then H is the amalgamated free product of G with the dihedral group

$$D_k = \langle s, t : s^2 = t^2 = (st)^k = 1\rangle$$

of order $2k$ over the subgroups $\langle y\rangle \cong \mathbb{Z}_k \cong \langle s, t\rangle$. □

Another construction we'll use are HNN extensions. Suppose that G is a group, H and K are subgroups of G, and $\phi : H \to K$ is an isomorphism. Then the HNN extension of G by ϕ is

$$\langle G, t : tht^{-1} = \phi(h) \text{ for all } h \in H\rangle.$$

It is well-known that the order of the generator t is infinite, and that, similar to the amalgamated free product and central product, G is a subgroup of the HNN extension

via the natural inclusion. More generally, given a sequence of subgroups $H_1, \ldots, H_m$ and $K_1, \ldots, K_m$ of a group G, along with isomorphisms $\phi_i : H_i \to K_i$, $1 \leqslant i \leqslant m$, G will be subgroup of the iterated HNN extension

$$\langle G, t_1, \ldots, t_m : t_i h t_i^{-1} = \phi_i(h) \text{ for all } 1 \leqslant i \leqslant m \text{ and } h \in H_i \rangle.$$

Britton's lemma allows us to determine the trivial words in an iterated HNN extension.

Lemma 7.2.2 (Britton's lemma, [Rot73])**.** *Let $H_1, \ldots, H_m$ and $K_1, \ldots, K_m$ be subgroups of a group G, and suppose $\phi_i : H_i \to K_i$ is an isomorphism for $i = 1 \ldots, m$. Let*

$$L = \langle G, t_1, \ldots, t_m : t_i h t_i^{-1} = \phi_i(h) \text{ for all } 1 \leqslant i \leqslant m \text{ and } h \in H_i \rangle$$

be the iterated HNN extension, and suppose

$$w = g_0 t_{i_1}^{e_1} g_1 t_{i_2}^{e_2} \cdots t_{i_n}^{e_n} g_n \in L$$

where $g_0, \ldots, g_n \in G$, $e_1, \ldots, e_n \in \{\pm 1\}$, and $1 \leqslant i_1, \ldots, i_n \leqslant m$. If $w = \mathbb{1}$ in L, then at least one of the following holds:

(a) $n = 0$ and $g_0 = \mathbb{1}$ in G,

(b) there is $1 \leqslant j < n$ such that $e_j = 1 = -e_{j+1}$, $i_j = i_{j+1}$, and $g_i \in H_{i_j}$, or

(c) there is $1 \leqslant j < n$ such that $e_j = -1 = -e_{j+1}$, $i_j = i_{j+1}$, and $g_i \in K_{i_j}$.

Let $G = \langle S : R \rangle$ be a finitely presented group. A function $f : \mathbb{N} \to \mathbb{N}$ is an isoperimetric function for G if for all words $w = s_1 \cdots s_n$ of length $n \geqslant 1$ over $S \cup S^{-1}$, if $w = \mathbb{1}$ in G then there are elements $u_1, \ldots, u_k \in \mathcal{F}_S$ and $r_1, \ldots, r_k \in R \cup R^{-1}$ with $k \leqslant f(n)$ and

$$w = u_1 r_1 u_1^{-1} \cdot u_2 r_2 u_2^{-1} \cdots u_k r_k u_k^{-1}.$$

Lemma 7.2.3 ([Ger93])**.** *Let $G = \langle S : R \rangle$ be a finitely presented group with an isoperimetric function f, and let $l := \max\{|r| : r \in R\}$ be the length of the longest relation in*

R. If a word $w \in \mathcal{F}_S$ of length n is equal to 1 in G, then there are $z_1, \cdots, z_k \in \mathcal{F}_S$ and $r_1, \cdots, r_k \in R \cup R^{-1}$ with $k \leqslant f(n)$ and $|z_i| \leqslant kl + l + n$ for all $1 \leqslant i \leqslant k$ such that

$$w = z_1 r_1 z_1^{-1} z_2 r_2 z_2^{-1} \cdots z_k r_k z_k^{-1}.$$

in $\mathcal{F}_S$.

We use the following theorem of Birget, Ol'shanskii, Rips, and Sapir:

Theorem 7.2.4 ([BORS02])**.** *Let G be a group with finite generating set S. If the word problem for G with respective to S is solvable in non-deterministic time $T(n)$, where T^4 is superadditive, then G can be embedded into a finitely presented group H with isoperimetric function $n^2 T(n^2)^4$.*

Here a function $T : \mathbb{N} \to \mathbb{N}$ is superadditive if $T(m+n) \geqslant T(m) + T(n)$ for all m, n. It follows immediately from this theorem that if the word problem for G is in NP, then G can be embedded in a finitely presented group H with a polynomial isoperimetric function.

7.3 Approximate states

We introduce some terminology for approximate states.

Definition 7.3.1. *Let $\mathcal{A}$ be a finitely generated $*$-algebra. Suppose $\epsilon \geqslant 0$ and $\mathcal{R} \subseteq \mathcal{A}$. An $(\epsilon, \mathcal{R})$-*state on $\mathcal{A}$ *is a state φ on $\mathcal{A}$ such that $\varphi(r^* r) \leqslant \epsilon$ for all $r \in \mathcal{R} \cup \mathcal{R}^*$. If, in addition, φ is tracial, then we say that φ is a* tracial $(\epsilon, \mathcal{R})$-state on $\mathcal{A}$.

If $(\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H}), \xi)$ is the GNS representation of a state φ on $\mathcal{A}$, then $\|x\|_\xi := \|x \cdot \xi\|$ is a semi-norm on $\mathcal{B}(\mathcal{H})$ such that $\|a\|_\varphi = \|\pi(a)\|_\xi$ for all $a \in \mathcal{A}$. If φ is an $(\epsilon, \mathcal{R})$-state on $\mathcal{A}$ as in Definition 7.3.1, then $\|\pi(r)\|_\xi \leqslant \sqrt{\epsilon}$ for all $r \in \mathcal{R}$, so we can think of π as a $\sqrt{\epsilon}$-approximate representation for $\mathbb{C}^* \langle \mathcal{A} : \mathcal{R} \rangle$ with respect to $\|\cdot\|_\xi$.

Definition 7.3.2. *Let $\mathcal{A}$ be a $*$-algebra with generating set $\mathcal{X}$. Let $\mathcal{R} \subseteq \mathbb{C}^* \langle \mathcal{X} \rangle$ be a set of $*$-polynomials over $\mathcal{X}$. For any $*$-polynomial $f \in \mathbb{C}^* \langle \mathcal{X} \rangle$ that is trivial in $\mathcal{A} / \langle \mathcal{R} \rangle$, we say that $\sum_{i=1}^n \lambda_i u_i r_i v_i$ is an $\mathcal{R}$-decomposition for f in $\mathcal{A}$ if*

1. u_i, v_i *are* $*$*-monomials in* $\mathbb{C}^*\langle\mathcal{X}\rangle$ *for all* $1 \leqslant i \leqslant n$,

2. $r_i \in \mathcal{R} \cup \mathcal{R}^*$ *for all* $1 \leqslant i \leqslant n$,

3. $\lambda_i \in \mathbb{C}$ *for all* $1 \leqslant i \leqslant n$, *and*

4. $f = \sum_{i=1}^n \lambda_i u_i r_i v_i$ *in* $\mathcal{A}$.

The size of an $\mathcal{R}$*-decomposition* $\sum_{i=1}^n \lambda_i u_i r_i v_i$ *is* $\sum_{i=1}^n |\lambda_i|(1 + \|r_i\|_{\mathcal{A}} \deg(v_i))$, *where* $\|\cdot\|_{\mathcal{A}}$ *is the operator norm in* $\mathcal{A}$.

Here a $*$-monomial in $\mathbb{C}^*\langle\mathcal{X}\rangle$ is a product $a_1 a_2 \cdots a_k$ where $k \geqslant 0$ and $a_1, \ldots, a_k \in \mathcal{X} \cup \mathcal{X}^*$ (the integer k is called the degree). We let $\|\cdot\|_1$ and $\|\cdot\|_{1,1}$ denote the 1-norm and first Sobolev 1-seminorm on $\mathbb{C}^*\langle\mathcal{X}\rangle$ with respect to the basis of $*$-monomials. In other words, if $f = \sum_{i=1}^n \lambda_i u_i \in \mathbb{C}^*\langle\mathcal{X}\rangle$ for distinct $*$-monomials $u_1, \ldots, u_n$, then $\|f\|_1 := \sum_{i=1}^n |\lambda_i|$ and $\|f\|_{1,1} := \sum_{i=1}^n |\lambda_i| \deg(u_i)$. Note that $\|\cdot\|_1$ is submultiplicative, and that $\|f^*\|_1 = \|f\|_1$, $\|f^*\|_{1,1} = \|f\|_{1,1}$ for all $f \in \mathbb{C}^*\langle\mathcal{X}\rangle$. The following elementary lemma is useful for computing sizes of $\mathcal{R}$-decompositions.

Lemma 7.3.3. *Let* $\mathcal{A}$ *be a* $*$*-algebra with generating set* $\mathcal{X}$, *and let* $\mathcal{R} \subseteq \mathbb{C}^*\langle\mathcal{X}\rangle$ *be a set of* $*$*-polynomials over* $\mathcal{X}$. *Then:*

(a) *If* $f = \sum_{i=1}^n u_i r_i v_i$ *for* $*$*-polynomials* $u_1, \ldots, u_n, v_1 \ldots, v_n \in \mathbb{C}^*\langle X\rangle$ *and* $r_1, \ldots, r_n \in \mathcal{R} \cup \mathcal{R}^*$, *then* f *has an* $\mathcal{R}$*-decomposition of size at most*

$$\sum_{i=1}^n \|u_i\|_1 \|v_i\|_1 + \|u_i\|_1 \|r_i\|_{\mathcal{A}} \|v_i\|_{1,1}.$$

(b) *If* $f - g$ *has an* $\mathcal{R}$*-decomposition of size* $\leqslant \Lambda_1$, *and* $g - h$ *has an* $\mathcal{R}$*-decomposition of size* $\leqslant \Lambda_2$, *then* $f - h$ *has an* $\mathcal{R}$*-decomposition of size* $\leqslant \Lambda_1 + \Lambda_2$.

(c) *If* g *has an* $\mathcal{R}$*-decomposition of size* $\leqslant \Lambda$, *then* fg *has an* $\mathcal{R}$*-decomposition of size* $\leqslant \|f\|_1 \Lambda$ *for all* $f \in \mathbb{C}^*\langle X\rangle$.

For instance, suppose we can demonstrate that $g = h$ in $\mathcal{A}/\langle\mathcal{R}\rangle$ by finding $f_1, \ldots, f_n$, $u_1, \ldots, u_n$, $v_1, \ldots, v_n \in \mathbb{C}^*\langle\mathcal{X}\rangle$ and $r_1, \ldots, r_n \in \mathcal{R} \cup \mathcal{R}^*$ such that $f_{i+1} - f_i = u_i r_i v_i$ for all $0 \leqslant i \leqslant n$, where $f_0 = g$ and $f_{n+1} = h$. Then we know that $g - h$ has an $\mathcal{R}$-decomposition of size at most $\sum_{i=1}^n \|u_i\|_1 \|v_i\|_1 + \|u_i\|_1 \|r_i\|_{\mathcal{A}} \|v_i\|_{1,1}$.

If $\mathcal{X}$ is a set of unitary generators for $\mathcal{A}$, then all $*$-monomials in $\mathbb{C}^*\langle\mathcal{X}\rangle$ are unitary in $\mathcal{A}$. As a result, an $\mathcal{R}$-decomposition of f can be used to bound the state-dependent norm of f with respect to any tracial $(\epsilon, \mathcal{R})$-state:

Proposition 7.3.4. *Suppose $\mathcal{A}$ is a $*$-algebra generated by a finite set of unitaries $\mathcal{X}$. Let $\mathcal{R} \subset \mathbb{C}^*\langle\mathcal{X}\rangle$ be a set of $*$-polynomials over $\mathcal{X}$, and let τ be a tracial $(\epsilon, \mathcal{R})$-state on $\mathcal{A}$. If $f \in \mathbb{C}^*\langle\mathcal{X}\rangle$ is trivial in $\mathcal{A}/\langle\mathcal{R}\rangle$ with an $\mathcal{R}$-decomposition $\sum_{i=1}^n \lambda_i u_i r_i v_i$, then $\|f\|_\tau \leqslant (\sum_{i=1}^n |\lambda_i|)\sqrt{\epsilon}$.*

Note that $\sum_{i=1}^n |\lambda_i|$ is less than or equal to the size of $\sum_{i=1}^n \lambda_i u_i r_i v_i$.

Proof. Since $\|\cdot\|_\tau$ is unitarily invariant,

$$\|f\|_\tau \leqslant \sum_{i=1}^n |\lambda_i| \|u_i r_i v_i\|_\tau = \sum_{i=1}^n |\lambda_i| \|r_i\|_\tau \leqslant (\sum_{i=1}^n |\lambda_i|)\sqrt{\epsilon}.$$

□

The proof of Proposition 7.3.4 does not work if τ is not tracial. However, we can still bound $\|f\|_\tau$ using the size of an $\mathcal{R}$-decomposition if τ is the restriction of a state on $\mathcal{A} \otimes \mathcal{A}$ satisfying a synchronicity condition:

Definition 7.3.5. *Suppose $\mathcal{A}$ is a $*$-algebra. A state φ on $\mathcal{A} \otimes \mathcal{A}$ is $(\epsilon, \mathcal{X})$-synchronous for some $\epsilon \geqslant 0$ and $\mathcal{X} \subseteq \mathcal{A}$ if*

$$\|x \otimes 1 - 1 \otimes x\|_\varphi \leqslant \sqrt{\epsilon} \tag{7.3.1}$$

for all $x \in \mathcal{X}$.

When working with $(\epsilon, \mathcal{X})$-synchronous states, it is convenient to let $\omega_{\mathcal{X}}$ denote the linear map $\mathbb{C}^*\langle\mathcal{X}\rangle \to \mathbb{C}^*\langle\mathcal{X}\rangle$ sending $x_1x_2\cdots x_n \mapsto x_nx_{n-1}\cdots x_1$ for all $n \in \mathbb{N}$ and $x_1, \ldots, x_n \in \mathcal{X} \cup \mathcal{X}^*$. This map satisfies $\omega_{\mathcal{X}}(a^*) = \omega_{\mathcal{X}}(a)^*$ and $\omega_{\mathcal{X}}(ab) = \omega_{\mathcal{X}}(b)\omega_{\mathcal{X}}(a)$ for all $a, b \in \mathbb{C}^*\langle\mathcal{X}\rangle$, and hence $\omega_{\mathcal{X}}$ is a $*$-isomomorphism $\mathbb{C}^*\langle\mathcal{X}\rangle \to \mathbb{C}^*\langle\mathcal{X}\rangle^{\mathrm{op}}$, where $\mathbb{C}^*\langle\mathcal{X}\rangle^{\mathrm{op}}$ is the opposite algebra of $\mathbb{C}^*\langle\mathcal{X}\rangle$.

Lemma 7.3.6. *Let $\mathcal{A}$ be a $*$-algebra generated by a finite set of unitaries $\mathcal{X}$. If φ is an $(\epsilon, \mathcal{X})$-synchronous state on $\mathcal{A} \otimes \mathcal{A}$, then*

$$\|u \otimes \mathbb{1} - \mathbb{1} \otimes \omega_{\mathcal{X}}(u)\|_\varphi \leqslant \|u\|_{1,1}\sqrt{\epsilon} \tag{7.3.2}$$

for all $u \in \mathbb{C}^*\langle\mathcal{X}\rangle$.

Proof. For every $x \in \mathcal{X}$, since x is unitary and $\|\cdot\|_\varphi$ is left unitarily invariant,

$$\|x^* \otimes \mathbb{1} - \mathbb{1} \otimes x^*\|_\varphi = \|(x \otimes x)(x^* \otimes \mathbb{1} - \mathbb{1} \otimes x^*)\|_\varphi = \|x \otimes \mathbb{1} - \mathbb{1} \otimes x\|_\varphi \leqslant \sqrt{\epsilon}.$$

Thus Equation (7.3.1) holds for all $x \in \mathcal{X} \cup \mathcal{X}^*$. Suppose $u = x_1 \cdots x_n$ is a monomial in $\mathbb{C}^*\langle\mathcal{X}\rangle$ of degree $n \geqslant 1$. Let $x_0 = x_{n+1} = \mathbb{1}$. Then

$$\begin{aligned}\|u \otimes \mathbb{1} - \mathbb{1} \otimes \omega_{\mathcal{X}}(u)\|_\varphi &= \|\sum_{k=1}^{n}(x_0x_1\cdots x_{k-1} \otimes x_{n+1}x_n\cdots x_{k+1})(x_k \otimes \mathbb{1} - \mathbb{1} \otimes x_k)\|_\varphi \\ &\leqslant \sum_{k=1}^{n}\|x_k \otimes \mathbb{1} - \mathbb{1} \otimes x_k\|_\varphi \leqslant n\sqrt{\epsilon}.\end{aligned}$$

By the subadditivity of $\|\cdot\|_\varphi$, Equation (7.3.2) holds for all $u \in \mathbb{C}^*\langle\mathcal{X}\rangle$. □

The following lemmas show that some of the properties of tracial states hold approximately for $(\epsilon, \mathcal{X})$-synchronous states.

Lemma 7.3.7. *Let $\mathcal{A}$ be a $*$-algebra generated by a finite set of unitaries $\mathcal{X}$, and let φ be an $(\epsilon, \mathcal{X})$-synchronous state on $\mathcal{A} \otimes \mathcal{A}$. If u is a monomial in $\mathbb{C}^*\langle\mathcal{X}\rangle$ and $a \in \mathcal{A}$, then $|\|u^*au \otimes 1\|_\varphi - \|a \otimes 1\|_\varphi| \leqslant \|a\|_{\mathcal{A}} \deg(u)\sqrt{\epsilon}$.*

Proof. Since u is a monomial in $\mathbb{C}^*\langle\mathcal{X}\rangle$, u and $\omega_{\mathcal{X}}(u)$ are unitary in $\mathcal{A}$. By Lemma 7.3.6, $\|u\otimes\mathbb{1}-\mathbb{1}\otimes\omega_{\mathcal{X}}(u)\|_\varphi \leqslant \deg(u)\sqrt{\epsilon}$. Thus

$$\begin{aligned}\|u^*au\otimes\mathbb{1}\|_\varphi &\leqslant \|(u^*a\otimes\mathbb{1})(u\otimes\mathbb{1}-\mathbb{1}\otimes\omega_{\mathcal{X}}(u))\|_\varphi + \|u^*a\otimes\omega_{\mathcal{X}}(u)\|_\varphi\\ &= \|(a\otimes\mathbb{1})(u\otimes\mathbb{1}-\mathbb{1}\otimes\omega_{\mathcal{X}}(u))\|_\varphi + \|a\otimes\mathbb{1}\|_\varphi\\ &\leqslant \|a\|_{\mathcal{A}}\deg(u)\sqrt{\epsilon} + \|a\otimes\mathbb{1}\|_\varphi.\end{aligned}$$

Replacing u with u^* and a with u^*au in this calculation, we see that

$$\|a\otimes 1\|_\varphi \leqslant \|a\|_{\mathcal{A}}\deg(u)\sqrt{\epsilon} + \|u^*au\otimes 1\|_\varphi,$$

and hence $\big|\|u^*au\otimes 1\|_\varphi - \|a\otimes 1\|_\varphi\big| \leqslant \|a\|_{\mathcal{A}}\deg(u)\sqrt{\epsilon}$. □

Lemma 7.3.8. *Let $\mathcal{A}$ be a $*$-algebra generated by a finite set of unitaries $\mathcal{X}$, and let φ be an $(\epsilon,\mathcal{X})$-synchronous state on $\mathcal{A}\otimes\mathcal{A}$. If u is a monomial in $\mathbb{C}^*\langle\mathcal{X}\rangle$ and $a\in\mathbb{C}^*\langle\mathcal{X}\rangle$ is a hermitian square in $\mathcal{A}$, then*

$$\Re\big(\varphi(u^*aua\otimes\mathbb{1})\big) \geqslant -\|u^*au\|_{1,1}\|a\otimes\mathbb{1}\|_\varphi\sqrt{\epsilon}.$$

Proof. Observe that

$$\varphi(u^*aua\otimes\mathbb{1}) = \varphi\big(a\otimes\omega_{\mathcal{X}}(u^*au)\big) + \varphi\Big(\big(u^*au\otimes\mathbb{1}-\mathbb{1}\otimes\omega_{\mathcal{X}}(u^*au)\big)\big(a\otimes\mathbb{1}\big)\Big).$$

Since $a=b^*b$ in $\mathcal{A}$ for some $b\in\mathbb{C}^*\langle\mathcal{X}\rangle$, $a\otimes\omega_{\mathcal{X}}(u^*au) = \big(b\otimes\omega_{\mathcal{X}}(u^*b^*)\big)^*\big(b\otimes\omega_{\mathcal{X}}(u^*b^*)\big)$ is a hermitian square in $\mathcal{A}$. Hence $\varphi\big(a\otimes\omega_{\mathcal{X}}(u^*au)\big)\geqslant 0$. By the Cauchy–Schwarz inequality and Lemma 7.3.6,

$$\begin{aligned}\Big|\varphi\Big(\big(u^*au\otimes\mathbb{1}-\mathbb{1}\otimes\omega_{\mathcal{X}}(u^*au)\big)\big(a\otimes\mathbb{1}\big)\Big)\Big| &\leqslant \|u^*au\otimes\mathbb{1}-\mathbb{1}\otimes\omega_{\mathcal{X}}(u^*au)\|_\varphi\cdot\|a\otimes\mathbb{1}\|_\varphi\\ &\leqslant \|u^*au\|_{1,1}\|a\otimes\mathbb{1}\|_\varphi\sqrt{\epsilon}.\end{aligned}$$

Since $\Re(\alpha)\geqslant -|\alpha|$ for every complex number α, the lemma follows. □

Lemma 7.3.9. *Let $\mathcal{A}$ be a $*$-algebra generated by a finite set of unitaries $\mathcal{X}$, and let $\iota:\mathcal{A}\to\mathcal{A}\otimes\mathcal{A}:a\mapsto a\otimes 1$ be the left inclusion. Suppose $\mathcal{R}\subseteq\mathbb{C}^*\langle\mathcal{X}\rangle$ is a set of $*$-polynomials over $\mathcal{X}$, and let φ be an $(\epsilon,\mathcal{X})$-synchronous state on $\mathcal{A}\otimes\mathcal{A}$ such that $\tau:=\varphi\circ\iota$ is an $(\epsilon,\mathcal{R})$-state on $\mathcal{A}$. If $f\in\mathcal{A}$ has an $\mathcal{R}$-decomposition of size Λ, then $\|f\|_\tau\leqslant\Lambda\sqrt{\epsilon}$.*

Proof. Let $\sum_{i=1}^{n} \lambda_i u_i r_i v_i$ be an $\mathcal{R}$-decomposition for f in $\mathcal{A}$ of size Λ. For every $1 \leqslant i \leqslant n$, by Lemma 7.3.6 there is a monomial $\widehat{v}_i$ in $\mathbb{C}^*\langle \mathcal{X} \rangle$ such that $\|v_i \otimes \mathbb{1} - \mathbb{1} \otimes \widehat{v}_i\|_\varphi \leqslant deg(v_i)\sqrt{\epsilon}$. Since $\varphi \circ \iota$ is an $(\epsilon, \mathcal{R})$-state on $\mathcal{A}$ and $\mathbb{1} \otimes \widehat{v}$ is unitary, it follows that $\|r_i \otimes \widehat{v}_i\|_\varphi = \|r_i\|_{\varphi \circ \iota} \leqslant \sqrt{\epsilon}$ for all $1 \leqslant i \leqslant n$. Then

$$\begin{aligned}
\|f \otimes \mathbb{1}\|_\varphi = \|\sum_{i=1}^{n} \lambda_i u_i r_i v_i \otimes \mathbb{1}\|_\varphi &\leqslant \sum_{i=1}^{n} |\lambda_i| \|r_i v_i \otimes \mathbb{1}\|_\varphi \\
&\leqslant \sum_{i=1}^{n} |\lambda_i| \big(\|(r_i \otimes \mathbb{1})(v_i \otimes \mathbb{1} - \mathbb{1} \otimes \widehat{v}_i)\|_\varphi + \|r_i \otimes \widehat{v}_i\|_\varphi \big) \\
&\leqslant \sum_{i=1}^{n} |\lambda_i| \big(\|r_i\|_{\mathcal{A}} \deg(v_i) \sqrt{\epsilon} + \sqrt{\epsilon} \big) = \Lambda \sqrt{\epsilon},
\end{aligned}$$

so $\|f\|_\tau = \|f \otimes \mathbb{1}\|_\varphi \leqslant \Lambda \sqrt{\epsilon}$. □

7.3.1 Dealing with infinite operator norm

The results presented so far in this section are useful for algebras $\mathcal{A}$ with $\|a\|_{\mathcal{A}} < \infty$ for all $a \in \mathcal{A}$. However, for the free algebras $\mathcal{A} = \mathbb{C}^*\langle x_1, \cdots, x_n \rangle$ the operator norm $\|a\|_{\mathcal{A}} = \infty$ for all $a \in \mathcal{A}$ which are not scalar multiples of identity, making the size of an $\mathcal{R}$-decomposition infinite as well. To handle this situation, we show in this section that for any element f in the free algebra $\mathcal{A}$, there is a set of relations $\mathcal{W}(f)$ such that if τ is a tracial $(\epsilon, \mathcal{W}(f))$-state on $\mathcal{A}$, then there is a tracial state on $\mathbb{C}\mathbb{Z}_2^{*n}$ which is close to τ on f.

Lemma 7.3.10. *For any $A \in \mathcal{B}(\mathcal{H})$, the operator $\widetilde{A} := sgn\big(\frac{A+A^*}{2}\big)$ is a unitary involution in $C^*\langle A \rangle''$. If in addition, ξ is a vector in $\mathcal{H}$ satisfying (i) $\|(A^2 - I_{\mathcal{H}})\xi\| \leqslant \epsilon$, (ii) $\|((A^*)^2 - I_{\mathcal{H}})\xi\| \leqslant \epsilon$, (iii) $\|(AA^* - I_{\mathcal{H}})\xi\| \leqslant \epsilon$, (iv) $\|(A^*A - I_{\mathcal{H}})\xi\| \leqslant \epsilon$, and (v) $\|(A - A^*)\xi\| \leqslant \epsilon$ for some $\epsilon \geqslant 0$, then $\|(A - \widetilde{A})\xi\| \leqslant 2\epsilon$ and $\|(A^* - \widetilde{A})\xi\| \leqslant 2\epsilon$.*

Here sgn denotes the function $\mathbb{R} \to \{-1, 1\}$ sending elements in $[0, +\infty)$ to 1 and elements in $(-\infty, 0)$ to -1.

Proof. The spectrum of $\frac{A+A^*}{2}$ is in $\mathbb{R}$, so by Borel functional calculus, $\widetilde{A} := \text{sgn}(\frac{A+A^*}{2})$ is a unitary involution and is in $C^*\langle A \rangle''$. Since sgn and $|\cdot|$ are measurable functions on $\mathbb{R}$

satisfying $(1+|a|)(\mathrm{sgn}(a)-a) = \mathrm{sgn}(a)(1-a^2)$ for all $a \in \mathbb{R}$, we obtain that

$$\begin{aligned}\|(\widetilde{A} - \tfrac{A+A^*}{2})\xi\| &= \|(\mathrm{sgn}(\tfrac{A+A^*}{2}) - \tfrac{A+A^*}{2})\xi\| \leqslant \|(\mathrm{Id}_{\mathcal{H}} + |\tfrac{A+A^*}{2}|)(\mathrm{sgn}(\tfrac{A+A^*}{2}) - \tfrac{A+A^*}{2})\xi\| \\ &= \|\mathrm{sgn}(\tfrac{A+A^*}{2})(\mathrm{Id}_{\mathcal{H}} - (\tfrac{A+A^*}{2})^2)\xi\| = \|(\mathrm{Id}_{\mathcal{H}} - (\tfrac{A+A^*}{2})^2)\xi\| \\ &= \|(\mathrm{Id}_{\mathcal{H}} - \tfrac{A^2+(A^*)^2+AA^*+A^*A}{4})\xi\| \leqslant \epsilon,\end{aligned}$$

where the last inequality follows from the conditions $(i)-(iv)$. By condition (v), $\|(A - \frac{A+A^*}{2})\xi\| = \|\frac{A-A^*}{2}\xi\| \leqslant \frac{\epsilon}{2}$, so $\|(\widetilde{A}-A)\xi\| \leqslant \|(\widetilde{A} - \frac{A+A^*}{2})\xi\| + \|(A - \frac{A+A^*}{2})\xi\| \leqslant \frac{3}{2}\epsilon \leqslant 2\epsilon$. Similarly we have $\|(\widetilde{A} - A^*)\xi\| \leqslant 2\epsilon$. □

Lemma 7.3.11. *Let $\mathcal{X}$ be a finite set. There is a computable mapping $\mathcal{W}$ from $\mathbb{Q}^*\langle\mathcal{X}\rangle$ to finite subsets of $\mathbb{Q}^*\langle\mathcal{X}\rangle$ such that*

(a) $\mathcal{W}(f) \subseteq \ker q$ for all $f \in \mathbb{Q}^*\langle\mathcal{X}\rangle$ where $q : \mathbb{C}^*\langle\mathcal{X}\rangle \to \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ is the quotient map, and

(b) for any tracial state τ on $\mathbb{C}^*\langle\mathcal{X}\rangle$, there is a tracial state $\widehat{\tau}$ on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ such that for all $f \in \mathbb{Q}^*\langle\mathcal{X}\rangle$ and $\epsilon \geqslant 0$, if τ is a tracial $(\epsilon, \mathcal{W}(f))$-state, then

$$\big|\|f\|_{\widehat{\tau}} - \|f\|_{\tau}\big| \leqslant 2\|f\|_{1,1}\sqrt{\epsilon}.$$

Proof. If $u = x_1 \cdots x_n \in \mathbb{C}^*\langle\mathcal{X}\rangle$ is a monomial of degree $n \geqslant 0$, then define

$$\begin{aligned}\mathcal{W}(u) := &\{(x_i x_i^* - \mathbb{1})x_{i+1}\cdots x_n : 1 \leqslant i \leqslant n\} \cup \{(x_i^* x_i - \mathbb{1})x_{i+1}\cdots x_n : 1 \leqslant i \leqslant n\} \\ &\cup \big\{(x_i^2 - \mathbb{1})x_{i+1}\cdots x_n : 1 \leqslant i \leqslant n\big\} \cup \big\{((x_i^*)^2 - \mathbb{1})x_{i+1}\cdots x_n : 1 \leqslant i \leqslant n\big\} \\ &\cup \{(x_i - x_i^*)x_{i+1}\cdots x_n : 1 \leqslant i \leqslant n\}\end{aligned}$$

(so in particular, $\mathcal{W}(1) = \varnothing$). If $f \in \mathbb{Q}^*\langle\mathcal{X}\rangle$ has support $u_1, \ldots, u_\ell$, or in other words $f = \sum_{i=1}^{\ell} \lambda_i u_i \in \mathbb{Q}^*\langle\mathcal{X}\rangle$ for distinct $*$-monomials $u_1, \ldots, u_\ell$ and non-zero coefficients $\lambda_1, \ldots, \lambda_\ell$, we define $\mathcal{W}(f) := \bigcup_{i=1}^{\ell} \mathcal{W}(u_i)$. Clearly $\mathcal{W}$ is computable. If u is a monomial, then $q(s^*s) = 0$ for all $s \in \mathcal{W}(u)$, so the same is true for $\mathcal{W}(f)$.

Let $\big(\pi : \mathbb{C}^*\langle\mathcal{X}\rangle \to \mathcal{B}(\mathcal{H}), v\big)$ be the GNS representation of τ. Note that $T \mapsto \langle v, Tv\rangle$ extends to a tracial state on $\pi(\mathbb{C}^*\langle\mathcal{X}\rangle)''$. For every $x \in \mathcal{X}$, let $\widehat{\pi}(x) := \mathrm{sgn}\big(\frac{\pi(x)+\pi(x)^*}{2}\big)$. By

Lemma 7.3.10, $\widehat{\pi}(x)$ is a unitary involution in $C^*\langle\pi(x)\rangle''$ for every $x \in \mathcal{X}$, so $\widehat{\pi}$ induces a $*$-representation of $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ on $\mathcal{H}$ and $\widehat{\tau}(a) := \langle v, \widehat{\pi}(a)v\rangle$ defines a tracial state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$.

Suppose $u = x_1 \cdots x_n$ is a monomial. If $\tau(s^*s) \leqslant \epsilon$ for all $s \in \mathcal{W}(u)$, then $\|\pi(s)v\| \leqslant \sqrt{\epsilon}$ for all $s \in \mathcal{W}(u)$, and hence by Lemma 7.3.10,

$$\|\big(\widehat{\pi}(x_i) - \pi(x_i)\big)\pi(x_{i+1}\cdots x_n)v\| \leqslant 2\sqrt{\epsilon}$$

for all $1 \leqslant i \leqslant n$. It follows that

$$\begin{aligned}\|\big(\widehat{\pi}(u) - \pi(u)\big)v\| &\leqslant \sum_{i=1}^{n}\|\widehat{\pi}(x_1\cdots x_{i-1})\big(\widehat{\pi}(x_i) - \pi(x_i)\big)\pi(x_{i+1}\cdots x_n)v\| \\ &= \sum_{i=1}^{n}\|\big(\widehat{\pi}(x_i) - \pi(x_i)\big)\pi(x_{i+1}\cdots x_n)\psi\| \leqslant 2n\sqrt{\epsilon}.\end{aligned}$$

For a general element $f \in \mathbb{Q}^*\langle\mathcal{X}\rangle$, write $f = \sum_{i=1}^{\ell}\lambda_i u_i$ as above. If $\tau(s^*s) \leqslant \epsilon$ for all $s \in \mathcal{W}(f)$, then

$$\begin{aligned}\big|\|f\|_\tau - \|f\|_{\widehat{\tau}}\big| &= \big|\|\widehat{\pi}(f)v\| - \|\pi(f)v\|\big| \leqslant \|\big(\widehat{\pi}(f) - \pi(f)\big)v\| \\ &\leqslant \sum_{i=1}^{\ell}|\lambda_i|\cdot\|\big(\widehat{\pi}(u_i) - \pi(u_i)\big)v\| \leqslant \sum_{i=1}^{\ell}2|\lambda_i|\deg(u_i)\sqrt{\epsilon} = 2\|f\|_{1,1}\sqrt{\epsilon}.\end{aligned}$$

We conclude that $\mathcal{W}$ is a computable mapping satisfying (a) and (b). □

Note that the proof of Lemma 7.3.11 only requires $\tau(s^*s) \leqslant \epsilon$ for all $s \in \mathcal{W}(f)$. We use the stronger hypothesis that τ is an $(\epsilon, \mathcal{W}(f))$-state for convenience.

Lemma 7.3.12. *Let $\mathcal{X}$ be a finite set, and let $\mathcal{W}$ be the map from Lemma 7.3.11. Suppose φ is an $(\epsilon, \mathcal{X})$-synchronous state on $\mathbb{C}^*\langle\mathcal{X}\rangle \otimes \mathbb{C}^*\langle\mathcal{X}\rangle$ for some $\epsilon \geqslant 0$, and $\varphi(s^*s \otimes \mathbb{1}) \leqslant \epsilon, \varphi(\mathbb{1} \otimes s^*s) \leqslant \epsilon$ for all $s \in \bigcup_{x\in\mathcal{X}}\mathcal{W}(x)$. Then there is a $(25\epsilon, \mathcal{X})$-synchronous state $\widehat{\varphi}$ on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} \otimes \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ such that for all $f \in \mathbb{Q}^*\langle\mathcal{X}\rangle$, if $\varphi(s^*s \otimes \mathbb{1}) \leqslant \epsilon$ for all $s \in \mathcal{W}(f)$, then*

$$\big|\|f \otimes \mathbb{1}\|_{\widehat{\varphi}} - \|f \otimes \mathbb{1}\|_\varphi\big| \leqslant 2\|f\|_{1,1}\sqrt{\epsilon}.$$

Proof. Let $(\pi : \mathbb{C}^*\langle\mathcal{X}\rangle \otimes \mathbb{C}^*\langle\mathcal{X}\rangle \to \mathcal{B}(\mathcal{H}), \psi)$ be the GNS representation of φ. For every $x \in \mathcal{X}$, let $\widehat{\pi}(x \otimes \mathbb{1}) := \operatorname{sgn}\left(\frac{\pi(x\otimes\mathbb{1})+\pi(x\otimes\mathbb{1})^*}{2}\right)$ and $\widehat{\pi}(\mathbb{1} \otimes x) := \operatorname{sgn}\left(\frac{\pi(\mathbb{1}\otimes x)+\pi(\mathbb{1}\otimes x)^*}{2}\right)$. Then by Lemma 7.3.10, for every $x \in \mathcal{X}$, $\widehat{\pi}(x\otimes\mathbb{1})$ and $\widehat{\pi}(\mathbb{1}\otimes x)$ are unitary involutions in $C^*\langle\pi(x\otimes\mathbb{1})\rangle''$ and $C^*\langle\pi(\mathbb{1}\otimes x)\rangle''$ respectively. So for every $x, x' \in \mathcal{X}$, $[\pi(x\otimes\mathbb{1}), \pi(\mathbb{1}\otimes x')] = 0$ implies $[\widehat{\pi}(x\otimes\mathbb{1}), \widehat{\pi}(\mathbb{1}\otimes x')] = 0$, and hence $\widehat{\pi}$ induces a $*$-representation of $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} \otimes \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ on $\mathcal{H}$ and $\widehat{\varphi}(a) := \langle\psi, \widehat{\pi}(a)\psi\rangle$ defines a state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} \otimes \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$. By the assumption, $\varphi(s^*s\otimes\mathbb{1}) \leqslant \epsilon$ and $\varphi(\mathbb{1}\otimes s^*s) \leqslant \epsilon$ for all $s \in \bigcup_{x\in\mathcal{X}} \mathcal{W}(x)$. This implies $\|\pi(s\otimes\mathbb{1})\psi\| \leqslant \sqrt{\epsilon}$ and $\|\pi(\mathbb{1}\otimes s)\psi\| \leqslant \sqrt{\epsilon}$ for all $s \in \bigcup_{x\in\mathcal{X}} \mathcal{W}(x)$, and hence by Lemma 7.3.10, $\|\big(\widehat{\pi}(x\otimes\mathbb{1}) - \pi(x\otimes\mathbb{1})\big)\psi\| \leqslant 2\sqrt{\epsilon}$ and $\|\big(\widehat{\pi}(\mathbb{1}\otimes x) - \pi(\mathbb{1}\otimes x)\big)\psi\| \leqslant 2\sqrt{\epsilon}$ for all $x \in \mathcal{X}$. It follows that

$$\begin{aligned}\|\big(\widehat{\pi}(x\otimes\mathbb{1}) - \widehat{\pi}(\mathbb{1}\otimes x)\big)\psi\| \leqslant &\|\big(\widehat{\pi}(x\otimes\mathbb{1}) - \pi(x\otimes\mathbb{1})\big)\psi\| + \|\big(\pi(x\otimes\mathbb{1}) - \pi(\mathbb{1}\otimes x)\big)\psi\| \\ &+ \|\big(\widehat{\pi}(\mathbb{1}\otimes x) - \pi(\mathbb{1}\otimes x)\big)\psi\| \leqslant 2\sqrt{\epsilon} + \sqrt{\epsilon} + 2\sqrt{\epsilon} = 5\sqrt{\epsilon}.\end{aligned}$$

This means $\widehat{\varphi}$ is a $(25\epsilon, \mathcal{X})$-synchronous state $\widehat{\varphi}$ on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} \otimes \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$. The rest of the lemma follows from a similar argument to the proof of Lemma 7.3.11. □

7.4 Construction of a suitable family of algebras

We begin the proofs of Theorems 7.1.1 and 7.1.3, with the case $\mathcal{A} = \mathbb{Q}\mathbb{Z}_2^{*N}$. To explain the idea of the proof, suppose that $\mathcal{S} \subseteq \mathbb{N}$ is an RE set, and that we can find an integer N, a self-adjoint element $w \in \mathbb{Q}\mathbb{Z}_2^{*N}$, and a computable family of finitely presented algebras $\mathcal{A}_\mathcal{S}(m) = \mathbb{C}^*\langle\mathbb{C}\mathbb{Z}_2^{*N} : \mathcal{R}_m\rangle$ such that $\mathcal{A}_\mathcal{S}(m)$ has a tracial state τ with $\tau(w^2) > 0$ if and only if $m \in \mathcal{S}$. If $\alpha(m) := \sum_{r\in\mathcal{R}_m} r^*r - w^2$, then a tracial state τ on $\mathcal{A}_\mathcal{S}(m)$ with $\tau(w^2) > 0$ pulls back to a tracial state on $\mathbb{C}\mathbb{Z}_2^{*N}$ with $\tau(\alpha(m)) < 0$. Unfortunately this idea runs into a *stability problem*: it is not necessarily the case that every tracial state on $\mathbb{C}\mathbb{Z}_2^{*N}$ with $\tau(\alpha(m)) < 0$ comes from a tracial state on $\mathcal{A}_\mathcal{S}(m)$. Indeed, it might be possible to find a tracial state τ for which $\tau\left(\sum_{r\in\mathcal{R}_m} r^*r\right)$ is small, but $\tau(w^2)$ is large.

The main technical idea of this chapter is that we can overcome the stability problem with a carefully chosen algebra $\mathcal{A}_\mathcal{S}(m)$. Specifically, we start with the algebra generated by a family of positive contractions $\{\widetilde{P}_0, \widetilde{P}_1, \ldots\}$ and a family of unitary involutions

$\{\widetilde{X}_0, \widetilde{X}_1, \ldots\}$ satisfying the relations

$$\widetilde{P}_{n+1} = \widetilde{P}_n + \widetilde{X}_n \widetilde{P}_n \widetilde{X}_n \tag{7.4.1}$$

for all n such that $M_{\mathcal{S}}$ does not halt on input m after n steps, where $M_{\mathcal{S}}$ is a Turing machine recognizing $\mathcal{S}$. This algebra is not finitely presented, so the purpose of this section is to show that this algebra can be embedded in a finitely-presented algebra $\mathcal{A}_{\mathcal{S}}(m)$, in such a way that the size of relation (7.4.1) is polynomial in n. Relation (7.4.1) implies that $\tau(\widetilde{P}_n) = \frac{1}{2}\tau(\widetilde{P}_{n+1})$ for any tracial state τ on $\mathcal{A}_{\mathcal{S}}(m)$, and in the next section we use this fact to overcome the stability problem and finish the proofs of Theorems 7.1.1 and 7.1.3 (for the case $\mathcal{A} = \mathbb{Q}\mathbb{Z}_2^{*N}$) using the strategy outlined in the previous paragraph.

Theorem 7.4.1. *Let $\mathcal{S} \subset \mathbb{N}$ be an RE set, and let $M_{\mathcal{S}}$ be a Turing machine that recognizes $\mathcal{S}$. Then there is a finite set $\mathcal{X}$, two sequences $\{\widetilde{P}_0, \widetilde{P}_1, ...\}$ and $\{\widetilde{X}_0, \widetilde{X}_1, ...\}$ in $\mathbb{Q}^*\langle\mathcal{X}\rangle$, and a computable mapping $m \mapsto \mathcal{R}_m$ from $\mathbb{N}$ to finite subsets of $\mathbb{Q}\mathbb{Z}_2^{*\mathcal{X}}$, such that*

(a) for all $n \geqslant 0$, $\widetilde{P}_n$ is a hermitian square in $\mathbb{Q}\mathbb{Z}_2^{*\mathcal{X}}$ with $\|\widetilde{P}_n\|_1 = 1$ and $\|\widetilde{P}_n\|_{1,1} = 3(n+1)/2$, and $\widetilde{X}_n$ is a monomial in $\mathbb{Q}^*\langle\mathcal{X}\rangle$ of degree $4n+1$ such that $\widetilde{X}_n^2 = 1$ in $\mathbb{Q}\mathbb{Z}_2^{*\mathcal{X}}$,

(b) there are constants $C > 0, k \in \mathbb{N}$ such that for every $m \in \mathbb{N}$ and $n \geqslant 0$, if $M_{\mathcal{S}}$ hasn't halted after n steps on input m, then $\widetilde{P}_n + \widetilde{X}_n\widetilde{P}_n\widetilde{X}_n - \widetilde{P}_{n+1}$ is trivial in $\mathcal{A}_{\mathcal{S}}(m) := \mathbb{C}^*\langle\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} : \mathcal{R}_m\rangle$ and has an $\mathcal{R}_m$-decomposition in $\mathbb{C}\mathbb{Z}_2^{\mathcal{X}}$ of size $\leqslant C\big((n+1)m\big)^k$,

(c) if $m \in \mathcal{S}$, then there is a tracial state τ on $\mathcal{A}_{\mathcal{S}}(m)$ such that $\tau(\widetilde{P}_0^2) > 0$, and

(d) there is a positive integer D such that $\|r\|_{1,1} \leqslant Dm$ for all $r \in \mathcal{R}_m, m \in \mathbb{N}$.

In part (a), $\|\cdot\|_1$ and $\|\cdot\|_{1,1}$ denote the 1-norm and Sobolev seminorm on $\mathbb{C}^*\langle\mathcal{X}\rangle$ defined in the previous section. Since monomials in $\mathbb{C}^*\langle\mathcal{X}\rangle$ are unitary in $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$, $\|a\|_{\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}} \leqslant \|a\|_1$ for all $a \in \mathbb{C}^*\langle\mathcal{X}\rangle$. So part (a) implies that $\widetilde{P}_n$ is a contraction in $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$, i.e. $\|\widetilde{P}_n\|_{\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}} \leqslant 1$, and $\widetilde{X}_n$ is a unitary involution in $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ for all $n \geqslant 0$.

For the rest of this section, we fix an RE set $\mathcal{S} \subset \mathbb{N}$, and a deterministic Turing machine $M_{\mathcal{S}}$ that recognizes $\mathcal{S}$. Define $h : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ by

$$h(m) = \begin{cases} n & m \in \mathcal{S} \text{ and } M_{\mathcal{S}} \text{ halts at the } n\text{th step on the input } m \\ \infty & m \notin \mathcal{S} \end{cases},$$

so $h|_{\mathbb{N}}$ is the running time of $M_{\mathcal{S}}$. Recall that in our convention, all Turing machines take at least one step, so $h(m) \geqslant 1$ for all $m \in \mathbb{Z}$. To prove Theorem 7.4.1, we start in Section 7.4.1 by encoding the Turing machine $M_{\mathcal{S}}$ in certain group relations. We finish the proof by constructing $\mathcal{A}_{\mathcal{S}}(m)$ in Section 7.4.2.

7.4.1 Group stage of construction

In the first stage of constructing $\mathcal{A}_{\mathcal{S}}(m)$, we build up a group $G_{\mathcal{S}}$ out of amalgamations, central products, and HNN extensions. We show that $G_{\mathcal{S}}$ has a finite generating set, and that the word problem with respect to this generating set is decidable in polynomial time. This allows us to embed $G_{\mathcal{S}}$ in a finitely presented group H_S, which we use as the basis for defining the algebras $\mathcal{A}_{\mathcal{S}}(m)$.

For the construction of $G_{\mathcal{S}}$, let $[A, B] := ABA^{-1}B^{-1}$ denote the group commutator, and let $\mathbb{Z}_n$ be the additive cyclic group of order $n \in \mathbb{N} \cup \{+\infty\}$ (so in particular, $\mathbb{Z}_\infty = \mathbb{Z}$). To order the elements of $\mathbb{Z}_n$, we represent elements of $\mathbb{Z}_n$ by integers $-\lfloor \frac{n+2}{2} \rfloor < j < \lfloor \frac{n+1}{2} \rfloor$. For instance, for $\mathbb{Z}_4$ we use representatives $-2, -1, 0, 1$. This choice of representatives has the property that every congruence class is represented by an element that is minimal in absolute value, i.e. if k' is the representative of $[k]$, then $|k'| \leqslant |k|$. Also, note that this set of representatives contains -1 for every $n \geqslant 2$. When $n = +\infty$, elements of $\mathbb{Z}_n = \mathbb{Z}$ represent themselves.

For each $m \in \mathbb{Z}$ and $i \in \mathbb{Z}_{h(m)+1}$, let $K_{\mathcal{S}}(m, i)$ be the group generated by indeterminates J, x_{mi}, z_{mi}, subject to the relations:

- $J^2 = x_{mi}^2 = z_{mi}^2 = \mathbb{1}$,

- $[x_{mi}, J] = [z_{mi}, J] = 1$, and
- $[x_{mi}, z_{mi}] = J^a$, where $a = 1$ if $i+1 \neq 0$ in $\mathbb{Z}_{h(m)+1}$, and $a = 0$ otherwise.

If $i + 1 \neq 0$ in $\mathbb{Z}_{h(m)+1}$, then the map $x_{mi} \mapsto a$, $z_{mi} \mapsto b$, $J \mapsto abab$ gives an isomorphism from $K_S(m, i)$ to the rank 4 dihedral group

$$D_4 = \langle a, b : a^2 = b^2 = (ab)^4 = 1 \rangle,$$

while if $i + 1 = 0$ in $\mathbb{Z}_{h(m)+1}$ then all generators commute. Hence

$$K_{\mathcal{S}}(m, i) = \begin{cases} D_4 & i + 1 \neq 0 \text{ in } \mathbb{Z}_{h(m)+1} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 & i + 1 = 0 \text{ in } \mathbb{Z}_{h(m)+1} \end{cases}.$$

In particular, J is central and $\langle J \rangle = \mathbb{Z}_2$ in both cases. For $m \in \mathbb{Z}$, let

$$K_{\mathcal{S}}(m) := \prod_{\langle J \rangle} \prod_{i \in \mathbb{Z}_{h(m)+1}} K_{\mathcal{S}}(m, i)$$

be the central product of the groups $K_{\mathcal{S}}(m, i)$, $i \in \mathbb{Z}_{h(m)+1}$, over the central subgroup $\langle J \rangle = \mathbb{Z}_2$, and let

$$K_{\mathcal{S}} := {}_{\langle J \rangle} *_{m \in \mathbb{Z}} K_{\mathcal{S}}(m)$$

be the amalgamated free product of the groups $K_{\mathcal{S}}(m)$, $m \in \mathbb{Z}$, over $\langle J \rangle = \mathbb{Z}_2$. In other words, $K_{\mathcal{S}}$ is generated by indeterminates

$$\mathcal{X}_K := \{J, x_{mi}, z_{mi}, m \in \mathbb{Z}, i \in \mathbb{Z}_{h(m)+1}\},$$

subject to relations

(K0) $J^2 = x_{mi}^2 = z_{mi}^2 = 1$ for all $m \in \mathbb{Z}, i \in \mathbb{Z}_{h(m)+1}$,

(K1) $[x_{mi}, J] = [z_{mi}, J] = 1$ for all $m \in \mathbb{Z}$, $i \in \mathbb{Z}_{h(m)+1}$,

(K2) for all $m \in \mathbb{Z}, i \in \mathbb{Z}_{h(m)+1}$,

$$[x_{mi}, z_{mi}] = \begin{cases} J & i+1 \neq 0 \text{ in } \mathbb{Z}_{h(m)+1} \\ \mathbb{1} & i+1 = 0 \text{ in } \mathbb{Z}_{h(m)+1} \end{cases}, \text{ and}$$

(K3) for all $m \in \mathbb{Z}$ and $i \neq j \in \mathbb{Z}_{h(m)+1}$,

$$[x_{mi}, z_{mj}] = [x_{mi}, x_{mj}] = [z_{mi}, z_{mj}] = \mathbb{1}.$$

Note from relations (K1) that J is central in $K_{\mathcal{S}}$. For each $m \in \mathbb{Z}$ and $i \in \mathbb{Z}_{h(m)+1}$, the elements $\{1, x_{mi}, z_{mi}, x_{mi}z_{mi}\}$ form a set of right coset representatives for $\langle J \rangle$. By the normal form theorem for central products, every element $w \in K_{\mathcal{S}}(m)$, $m \in \mathbb{Z}$ can be written uniquely as

$$w = J^c x_{m,i_1}^{a_1} z_{m,i_1}^{b_1} x_{m,i_2}^{a_2} z_{m,i_2}^{b_2} \cdots x_{m,i_k}^{a_k} z_{m,i_k}^{b_k}, \tag{7.4.2}$$

where $k \geqslant 0$, $i_1 < i_2 < \ldots < i_k$ are representatives of elements from $\mathbb{Z}_{h(m)+1}$ as described above, $c \in \mathbb{Z}_2$, and $(a_j, b_j) \in \{(0,1),(1,0),(1,1)\} \subset \mathbb{Z}_2 \times \mathbb{Z}_2$ for all $1 \leqslant j \leqslant k$. The function $\eta_m(w) = J^c x_{m,i_1}^{a_1} z_{m,i_1}^{b_1} \cdots x_{m,i_k}^{a_k} z_{m,i_k}^{b_k}$ is a normal form for $K_{\mathcal{S}}(m)$. Note that we take the indices $i_1, \ldots, i_k$ to be from the chosen set of representatives for $\mathbb{Z}_{h(m)+1}$, rather than elements of $\mathbb{Z}_{h(m)+1}$, so $\eta(w)$ is a word over

$$\widetilde{\mathcal{X}}_K := \left\{ J, x_{mi}, z_{mi}, m \in \mathbb{Z}, -\lfloor \tfrac{h(m)+3}{2} \rfloor < i < \lfloor \tfrac{h(m)+2}{2} \rfloor \right\}$$

rather than $\mathcal{X}_K$. We use this convention so that the indices are ordered, and so we can encode words over the generators as binary strings. For convenience in what follows, we assume that words over $\widetilde{\mathcal{X}}_K \cup \widetilde{\mathcal{X}}_K^{-1}$ are encoded in a fairly typical way as a sequence of substrings representing symbols and indices, where symbols are encoded with a fixed number of bits, and indices are written in binary with a sign bit. For instance, we might encode $x_{m,i}^{-1}$ by the bit sequence for x^{-1} followed by the binary representations of m and i separated by delimiters, and $x_{m,i}^{-3} z_{m',i'}$ by this same sequence repeated three times (we do not represent exponents in binary) followed by the encoding of $z_{m',i'}$. The **bit-length** (as opposed to the usual length) of a word over $\widetilde{\mathcal{X}}_K \cup \widetilde{\mathcal{X}}_K^{-1}$ is the length of this binary encoding. The bit-length of a word w depends on the indices m and i of generators $x_{mi}^{\pm 1}$

and $z_{mi}^{\pm 1}$ appearing in w. In what follows, we need to pay special attention to how large i gets, so we define the **maximum index** of a word w over $\widetilde{\mathcal{X}}_K \cup \widetilde{\mathcal{X}}_K^{-1}$ to be

$$\max\{r \geqslant 0 : \text{one of } x_{m,\pm r}^{\pm 1}, z_{m,\pm r}^{\pm 1} \text{ appears in } w \text{ for some } m \in \mathbb{Z}\} \cup \{0\}.$$

Returning to normal forms, the subset

$$\mathcal{C}(m) := \big\{x_{m,i_1}^{a_1} z_{m,i_1}^{b_1} \cdots x_{m,i_k}^{a_k} z_{m,i_k}^{b_k} : k \geqslant 0, -\lfloor \tfrac{h(m)+3}{2} \rfloor < i_1 < \ldots < i_k < \lfloor \tfrac{h(m)+2}{2} \rfloor, \\ (a_j, b_j) \in \{(0,1),(1,0),(1,1)\}, 1 \leqslant j \leqslant k\big\}$$

is a set of right coset representatives for $\langle J \rangle$ in $K_{\mathcal{S}}(m)$. By the normal form theorem for amalgamated free products, every element $w \in K_{\mathcal{S}}$ can be written uniquely as

$$w = J^c w_1 \cdots w_\ell \tag{7.4.3}$$

where $\ell \geqslant 0$, $c \in \mathbb{Z}_2$, and $w_j \in \mathcal{C}(m_j)\backslash\{1\}$ for some integers $m_1, \ldots, m_\ell$ such that $m_j \neq m_{j+1}$ for all $1 \leqslant j \leqslant \ell - 1$. The function $\eta(w) = J^c w_1 \cdots w_\ell$ is a normal form for $K_{\mathcal{S}}$. This normal form can be computed efficiently:

Proposition 7.4.2. *Let η be the normal form for K_S described above. If w is given as a word over $\widetilde{X}_K \cup \widetilde{X}_K^{-1}$, then $\eta(w)$ is computable in polynomial time in the bit-length of w. If we write $\eta(w) = J^c w_1 \cdots w_\ell$ as in Eq. (7.4.3), then the length, bit-length, and maximum index of $w_1 \cdots w_\ell$ are at most the length, bit-length, and maximum index of w respectively.*

Proof. To compute $\eta(w)$, suppose first that w is a word over $\widetilde{\mathcal{X}}_K(m) \cup \widetilde{\mathcal{X}}_K(m)^{-1}$, where

$$\widetilde{\mathcal{X}}_K(m) := \left\{J, x_{mi}, z_{mi}, -\lfloor \tfrac{h(m)+3}{2} \rfloor < i < \lfloor \tfrac{h(m)+2}{2} \rfloor\right\}.$$

Note that if $-\lfloor \frac{h(m)+3}{2} \rfloor < i < \lfloor \frac{h(m)+2}{2} \rfloor$, then $i + 1 = 0$ in $\mathbb{Z}_{h(m)+1}$ if and only if $i = -1$. Using relations (K1)-(K3), we can reorder w so that it can be written as in Eq. (7.4.2) for some $c, a_1, b_1, \ldots, a_k, b_k \in \mathbb{Z}$ (rather than $\mathbb{Z}_2$). Using relations (K0), we can then reduce $c, a_1, b_1, \ldots, a_k, b_k$ mod 2 to put w in normal form $\eta_m(w) = J^c \overline{w}$, where $\overline{w} \in \mathcal{C}(m)$. Since a list of integers can be sorted in polynomial time, this process takes polynomial time in the

bit-length of w. Since every generator in $\overline{w}$ occurs in w, and no generator appears in $\overline{w}$ more than once, the length, bit-length, and maximum index of $\overline{w}$ are at most the length, bit-length, and maximum index of w respectively.

If w is a word over $\widetilde{\mathcal{X}}_K \cup \widetilde{\mathcal{X}}_K^{-1}$, then we can write $w = J^c w_1 \cdots w_\ell$, where $c \in \mathbb{Z}_2$, w_j is a word over $\widetilde{\mathcal{X}}_K(m_j) \cup \widetilde{\mathcal{X}}_K(m_j)^{-1}$ for $1 \leqslant i \leqslant \ell$, and $m_1, \ldots, m_\ell$ is some sequence of integers such that $m_j \neq m_{j+1}$ for $1 \leqslant j \leqslant \ell - 1$. Using the procedure in the last paragraph, we can put w_j in normal form $J^{c_j}\overline{w}_j$ for $K_{\mathcal{S}}(m_j)$, where $\overline{w}_j \in \mathcal{C}(m_j)$ and $c_j \in \mathbb{Z}_2$. The length of $\overline{w}_j$ is at most the length of w_j, so the length of $\overline{w}_1 \cdots \overline{w}_\ell$ is at most the length of $w_1 \cdots w_\ell$, and the same is true of bit-length and maximum index. Let $c' = c + \sum_j c_j$. If $\overline{w}_j \neq 1$ for all $1 \leqslant j \leqslant \ell$, then $\eta(w) = J^{c'}\overline{w}_1 \cdots \overline{w}_\ell$. Otherwise, if $\overline{w}_j = 1$ for some $1 \leqslant j \leqslant \ell$, then we can repeat this procedure with $w' = J^{c'}\overline{w}_1 \cdots \overline{w}_{j-1}\overline{w}_{j+1} \cdots \overline{w}_\ell$. Since ℓ decreases in each iteration of this algorithm, the overall running time will be polynomial in the bit-length of w. Also, since the length of $w_1 \cdots w_\ell$ does not increase in each iteration, the length of $\overline{w}_1 \cdots \overline{w}_\ell$ in the final iteration is at most the length of the initial input w, and the same is true of bit-length and maximum index. □

Remark 7.4.3. *Since, for instance, $\eta(z_{m0}x_{m0}) = Jx_{m0}z_{m0}$, the length and bit-length of $\eta(w)$ is not necessarily less than the length and bit-length of w. Proposition 7.4.2 does imply that the length of $\eta(w)$ is at most one more than the length of w. Since the generator J does not contribute to the maximum index, the maximum index of $\eta(w)$ is at most the maximum index of w.*

Remark 7.4.4. *The above algorithm for computing η assumes that the generators x_{mi} and z_{mi} in the input are given by specifying the representative of the index $i \in \mathbb{Z}_{h(m)+1}$. The algorithm does not work as stated without this assumption. For instance, on $w = x_{m,-3} \cdot x_{m,7}$ the algorithm will return w back again, but if $h(m) = 9$ then $x_{m,7} = x_{m,-3}$ in $K_{\mathcal{S}}$, and $\eta(w) = 1$. If $i \in \mathbb{Z}$, then the representative for i in $\mathbb{Z}_{h(m)+1}$ can be computed by running the Turing machine $M_{\mathcal{S}}$ on input m for $2|i| - 1$ steps. If $M_{\mathcal{S}}$ halts by this point then we know $h(m)$ and can replace i by its representative if necessary, while if it does not halt then $h(m) > 2|i| - 1$ and hence $-\lfloor\frac{h(m)+3}{2}\rfloor < i < \lfloor\frac{h(m)+2}{2}\rfloor$. The running time of this procedure is polynomial in the bit-length of m and the value of i, but not polynomial in the bit-length*

of i. We will use this procedure for computing the representative of i later.

For the final step of constructing $G_{\mathcal{S}}$, we take iterated HNN extensions over several subgroups of $K_{\mathcal{S}}$:

$$\begin{aligned} K_{\mathcal{S},x} &:= \langle J, x_{mi}, m \in \mathbb{Z}, i \in \mathbb{Z}_{h(m)+1} \rangle, \\ K_{\mathcal{S},z} &:= \langle J, z_{mi}, m \in \mathbb{Z}, i \in \mathbb{Z}_{h(m)+1} \rangle, \text{ and} \\ K_{\mathcal{S},0} &:= \langle J, x_{m,0}, z_{m,0}, m \in \mathbb{Z} \rangle. \end{aligned}$$

Lemma 7.4.5.

(a) An element $w \in K_{\mathcal{S}}$ is in $K_{\mathcal{S},x}$ if and only if its normal form $\eta(w)$ is a word over $\{J, x_{mi},\ m \in \mathbb{Z}, -\lfloor \frac{h(m)+3}{2} \rfloor < i < \lfloor \frac{h(m)+2}{2} \rfloor\}$. In addition, there is an automorphism $\phi_S : K_{\mathcal{S},x} \to K_{\mathcal{S},x}$ sending $J \mapsto J$ and $x_{mi} \mapsto x_{m,i+1}$ for all $m \in \mathbb{Z}, i \in \mathbb{Z}_{h(m)+1}$.

(b) An element $w \in K_{\mathcal{S}}$ is in $K_{\mathcal{S},z}$ if and only if its normal form $\eta(w)$ is a word over $\{J, z_{mi},\ m \in \mathbb{Z}, -\lfloor \frac{h(m)+3}{2} \rfloor < i < \lfloor \frac{h(m)+2}{2} \rfloor\}$. In addition, there is an automorphism $\phi_T : K_{\mathcal{S},z} \to K_{\mathcal{S},z}$ sending $J \mapsto J$ and $z_{mi} \mapsto z_{m,i+1}$ for all $m \in \mathbb{Z}, i \in \mathbb{Z}_{h(m)+1}$.

(c) An element $w \in K_{\mathcal{S}}$ is in $K_{\mathcal{S},0}$ if and only if its normal form $\eta(w)$ is a word over $\{J, x_{m,0}, z_{m,0}, m \in \mathbb{Z}, \}$. In addition, there is an automorphism $\phi_W : K_{\mathcal{S},0} \to K_{\mathcal{S},0}$ sending $J \mapsto J$, $x_{m,0} \mapsto x_{m+1,0}$, and $z_{m,0} \mapsto z_{m+1,0}$ for all $m \in \mathbb{Z}$.

Proof. For part (a), observe that the subgroup $K_{\mathcal{S},x}(m,i) := \langle J, x_{mi} \rangle \subseteq K_{\mathcal{S}}(m,i)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ for all $m \in \mathbb{Z}, i \in \mathbb{Z}_{h(m)+1}$. For $m \in \mathbb{Z}$, let $K_{\mathcal{S},x}(m) := \langle J, x_{mi} : i \in \mathbb{Z}_{h(m)+1} \rangle \subseteq K_{\mathcal{S}}(m)$, and consider the natural surjective homomorphism

$$\Phi_m : {\prod_{\langle J \rangle}}_{i \in \mathbb{Z}_{h(m)+1}} K_{\mathcal{S},x}(m,i) \to K_{\mathcal{S},x}(m).$$

By the normal form theorem for central products, every element w in the domain of Φ_m can be written uniquely as $w = J^c x_{m,i_1} x_{m,i_2} \cdots x_{m,i_k}$, where $k \geqslant 0$, $-\lfloor \frac{h(m)+3}{2} \rfloor < i_1 < \cdots < i_k < \lfloor \frac{h(m)+2}{2} \rfloor$, and $c \in \mathbb{Z}_2$. Comparing with the normal form η_m for $K_{\mathcal{S}}(m)$, we see that Φ_m sends normal forms to normal forms. It follows that Φ_m is an isomorphism, and that

if $w \in K_{\mathcal{S},x}(m)$, then the normal form $\eta_m(w)$ in $K_{\mathcal{S}}(m)$ is a word containing only J and x_{mi}'s.

A similar argument using the normal form theorem for amalgamated free products shows that

$$K_{\mathcal{S},x} = {}_{\langle J \rangle} *_{m \in \mathbb{Z}} K_{\mathcal{S},x}(m),$$

and the normal form $\eta(w)$ of an element $w \in K_{\mathcal{S},x}$ is a word over $\{J, x_{mi} : m \in \mathbb{Z}, -\lfloor \frac{h(m)+3}{2} \rfloor < i < \lfloor \frac{h(m)+2}{2} \rfloor\}$.

For the automorphism, observe that

$${}_{\langle J \rangle}\prod\nolimits_{i \in \mathbb{Z}_{h(m)+1}} K_{\mathcal{S},x}(m,i) \cong \mathbb{Z}_2 \times \mathbb{Z}_2^{\oplus h(m)+1},$$

where the first $\mathbb{Z}_2$ is generated by J, and $\mathbb{Z}_2^{\oplus h(m)+1}$ is generated by $\{x_{mi} : i \in \mathbb{Z}_{h(m)+1}\}$. Hence for every $m \in \mathbb{Z}$ there is an automorphism $\phi_S^{(m)} : K_{\mathcal{S},x}(m) \to K_{\mathcal{S},x}(m)$ sending $J \mapsto J$ and $x_{mi} \mapsto x_{m,i+1}$ for all $i \in \mathbb{Z}_{h(m)+1}$, and these extend to the desired automorphism $\phi_S : K_{\mathcal{S},x} \to K_{\mathcal{S},x}$.

The argument for part (b) is identical. For part (c), observe that $K_{\mathcal{S}}(m,0) \cong D_4$ for all $m \in \mathbb{Z}$ (since $h(m) \geqslant 1$), and that $K_{\mathcal{S},0} = {}_{\langle J \rangle} *_{m \in \mathbb{Z}} K_{\mathcal{S}}(m,0)$ by the normal form theorem for amalgamated free products again. Hence for every $m \in \mathbb{Z}$ there is an isomorphism $\phi_W^{(m)} : K_{\mathcal{S}}(m,0) \to K_{\mathcal{S}}(m+1,0)$ sending $J \mapsto J$, $x_{m,0} \mapsto x_{m+1,0}$, and $z_{m,0} \mapsto z_{m+1,0}$, and these extend to the desired automorphism $\phi_W : K_{\mathcal{S},0} \to K_{\mathcal{S},0}$. □

We can now define $G_{\mathcal{S}}$ as the iterated HNN extensions of $K_{\mathcal{S}}$ by the automorphisms ϕ_S, ϕ_T, and ϕ_W from Lemma 7.4.5, using variables S, T, and W respectively. This means that

$$\begin{aligned} G_{\mathcal{S}} = \langle K_{\mathcal{S}}, S, T, W : {} & SJS^{-1} = TJT^{-1} = WJW^{-1} = J, \\ & Sx_{mi}S^{-1} = x_{m,i+1}, Tz_{mi}T^{-1} = z_{m,i+1}, m \in \mathbb{Z}, i \in \mathbb{Z}_{h(m)+1}, \\ & Wx_{m,0}W^{-1} = x_{m+1,0}, Wz_{m,0}W^{-1} = z_{m+1,0}, m \in \mathbb{Z} \rangle. \end{aligned}$$

Unlike $K_{\mathcal{S}}$, this group is finitely generated:

Lemma 7.4.6. *$G_{\mathcal{S}}$ is generated by $\{J, S, T, W, x_{00}, z_{00}\}$.*

Proof. For any $m \in \mathbb{Z}, i \in \mathbb{Z}_{h(m)+1}$, we have $x_{mi} = S^i W^m x_{00} W^{-m} S^{-i}$ and $z_{mi} = T^i W^m z_{00} W^{-m} T^{-i}$ in $G_{\mathcal{S}}$. □

We use this generating set frequently going forward. Hence for notational convenience, we let $X := x_{00}$, $Z := z_{00}$, and $\mathcal{X}_G := \{J, S, T, W, X, Z\}$. Also, we let X_{mi} and Z_{mi} denote the words

$$X_{mi} := S^i W^m X W^{-m} S^{-i} \text{ and } Z_{mi} := T^i W^m Z W^{-m} T^{-i}, m, i \in \mathbb{Z}.$$

The words X_{mi} and Z_{mi} both have length $2|m| + 2|i| + 1$.

If we restate the presentation of $G_{\mathcal{S}}$ with respect to this generating set, we see that $G_{\mathcal{S}}$ is the group generated by $\mathcal{X}_G$, subject to the following relations:

(G0) $J^2 = X^2 = Z^2 = 1$.

(G1) $[S, J] = [T, J] = [W, J] = [X, J] = [Z, J] = \mathbb{1}$, i.e., J is a central element.

(G2) For every $m, i \in \mathbb{Z}$,

$$[X_{mi}, Z_{mi}] = \begin{cases} J & i + 1 \neq 0 \bmod h(m) + 1 \\ \mathbb{1} & i + 1 = 0 \bmod h(m) + 1 \end{cases}.$$

(G3) For all $m \in \mathbb{Z}$ and $i \neq j \bmod h(m) + 1$,

$$[X_{mi}, Z_{mj}] = [X_{mi}, X_{mj}] = [Z_{mi}, Z_{mj}] = \mathbb{1}.$$

(G4) For every $m \in \mathbb{N}$ with $h(m) < +\infty$,

$$X_{m,h(m)+1} = X_{m,0} \text{ and } Z_{m,h(m)+1} = Z_{m,0}.$$

In the next stage of our construction, we want to use Theorem 7.2.4 to embed $G_{\mathcal{S}}$ into a finitely presented group with polynomial isoperimetric function. For this, we need:

Proposition 7.4.7. *The word problem for $G_{\mathcal{S}}$ with respect to $\mathcal{X}_G$ is solvable in deterministic polynomial time.*

Proof. First consider the larger generating set $\widehat{\mathcal{X}}_G := \widetilde{\mathcal{X}}_K \cup \{S, T, W\}$ where

$$\widetilde{\mathcal{X}}_K = \left\{ J, x_{mi}, z_{mi}, m \in \mathbb{Z}, -\lfloor \tfrac{h(m)+3}{2} \rfloor < i < \lfloor \tfrac{h(m)+2}{2} \rfloor \right\}$$

as in Proposition 7.4.2. The word problem with respect to $\widehat{\mathcal{X}}_G$ is solvable using Britton's Lemma as follows:

(1) Given a word w over $\widehat{\mathcal{X}}_G \cup \widehat{\mathcal{X}}_G^{-1}$, write

$$w = g_0 t_1^{e_1} g_1 t_2^{e_2} \cdots t_n^{e_n} g_n,$$

where $e_1, \ldots, e_n \in \{\pm 1\}$, $t_1, \ldots, t_n \in \{S, T, W\}$, and $g_0, \ldots, g_n$ are words over $\widetilde{\mathcal{X}}_K \cup \widetilde{\mathcal{X}}_K^{-1}$.

(2) For every $0 \leqslant i \leqslant n$, compute the normal form $\eta(g_i)$ of g_i from Proposition 7.4.2.

(3) If $n = 0$, then $w = \mathbb{1}$ in $G_{\mathcal{S}}$ if and only if $\eta(g_0) = \mathbb{1}$, and we can stop.

(4) Otherwise, use Lemma 7.4.5 to check whether there is an index $1 \leqslant j < n$ such that $e_j = -e_{j+1}$, $t_j = t_{j+1} = S$, and $g_j \in K_{\mathcal{S},x}$. If such a j exists, then let $g_j' = J^c x_{m_1,i_1'} \cdots x_{m_k,i_k'}$ where $\eta(g_j) = J^c x_{m_1,i_1} \cdots x_{m_k,i_k}$ and $-\lfloor \frac{h(m_l)+3}{2} \rfloor < i_l' < \lfloor \frac{h(m_l)+2}{2} \rfloor$ is the representative of $[i_l + e_j] \in \mathbb{Z}_{h(m_l)+1}$ (computed as in Remark 7.4.4). Return to step (1) with

$$w = g_0 t_1^{e_1} \cdots t_{j-1}^{e_{j-1}} (g_{j-1} g_j' g_{j+1}) t_{j+2}^{e_{j+2}} g_{j+2} \cdots t_n^{e_n} g_n.$$

(5) If no such j exists, perform step (4) with $S, K_{\mathcal{S},x}$ replaced by $T, K_{\mathcal{S},z}$ and $W, K_{\mathcal{S},0}$, with g_j' adjusted to match the automorphisms ϕ_T and ϕ_W from Lemma 7.4.5 respectively.

(6) If no such j exists for S, T and W, then $w \neq \mathbb{1}$ in $G_{\mathcal{S}}$ by Britton's Lemma, and we can stop.

Define the bit-length and maximum index of a word w over $\widehat{\mathcal{X}}_G \cup \widehat{\mathcal{X}}_G^{-1}$ analogously to words over $\widetilde{\mathcal{X}}_K \cup \widetilde{\mathcal{X}}_K^{-1}$. Specifically, if if w is written as in step (1), then define the maximum index of w to be $\max_i I_i$, where I_i is the maximum index of g_i. Let N, B, and I be the length, bit-length, and maximum index of the initial input to the above algorithm. Since n decreases by two after each iteration, and n is bounded by N, the algorithm is guaranteed to halt after at most $\lceil N/2 \rceil$ iterations. In steps (4) and (5), the length of g'_j is equal to the length of $\eta(g_j)$, which is at most one more than the length of g_j. The generators t_j and t_{j+1} are removed from w in this step, and w does not change in any other step, so the length of w also decreases in each iteration. The maximum index can increase by one in steps (4) and (5) when the automorphisms ϕ_S and ϕ_T are applied, so the maximum index throughout is bounded by $I + \lceil N/2 \rceil$. Applying automorphisms ϕ_S, ϕ_T, and ϕ_W in steps (4) and (5) can also increase the bit-length of each generator by one (note that the bit-length of the representative of $[i] \in \mathbb{Z}_{h(m)+1}$ is at most the bit-length of i), so the overall bit length of w can go up by at most N in each step. Thus the bit-length of w is bounded by $B + N \cdot \lceil N/2 \rceil$ throughout.

By Proposition 7.4.2, each normal form $\eta(g_j)$ in step (2) can be computed in time polynomial in the bit-length of w, and we compute at most N normal forms in this step. In steps (4) and (5), each representative i'_ℓ can be computed in time polynomial in the bit-length and maximum index of w, and we have to compute at most N representatives. The other steps can be done in time polynomial in the bit-length of w, so we conclude that the entire algorithm takes time polynomial in N, B, and I.

Since I is not polynomial in N and B in general, the above algorithm doesn't run in polynomial time in N or B. However, if the initial input is a word in $\mathcal{X}_G \cup \mathcal{X}_G^{-1}$, then $I = 0$, and $B = CN$ where C is the number of bits needed to encode each element of $\mathcal{X}_G \cup \mathcal{X}_G^{-1}$. So the above algorithm takes time polynomial in N for words from $\mathcal{X}_G \cup \mathcal{X}_G^{-1}$. □

We can now embed $G_{\mathcal{S}}$ into a finitely-presented group:

Proposition 7.4.8. *There is a finitely-presented group $H_{\mathcal{S}} = \langle \mathcal{X}_H : \mathcal{R}_H \rangle$, a polynomial $d_{\mathcal{S}}$, and an embedding $\iota : \mathcal{F}_{\mathcal{X}_G} \hookrightarrow \mathcal{F}_{\mathcal{X}_H}$ such that*

(a) $z^2 \in \mathcal{R}_H$ *for all* $z \in \mathcal{X}_H$ *(so all the generators of* $H_{\mathcal{S}}$ *are involutions),*

(b) $\iota(J)$, $\iota(X)$, *and* $\iota(Z)$ *are elements of* $\mathcal{X}_H$, *while* $\iota(S)$, $\iota(T)$, *and* $\iota(W)$ *have length two in* $H_{\mathcal{S}}$, *and*

(c) *if* $w \in \mathcal{F}_{\mathcal{X}_G}$ *is a word which is trivial in* $G_{\mathcal{S}}$, *then there there exist* $r_1, \cdots, r_k \in \mathcal{R}_H \cup \mathcal{R}_H^{-1}$, $z_1, \cdots, z_k \in \mathcal{F}_{\mathcal{X}_H}$ *with* $k \leqslant d_{\mathcal{S}}(|\iota(w)|)$ *and* $|z_i| \leqslant d_{\mathcal{S}}(|\iota(w)|)$ *for all* $1 \leqslant i \leqslant k$ *satisfying*

$$\iota(w) = z_1 r_1 z_1^{-1} z_2 r_2 z_2^{-1} \cdots z_k r_k z_k^{-1}$$

in $\mathcal{F}_{\mathcal{X}_H}$.

Item (c) implies that ι embeds $G_{\mathcal{S}}$ into $H_{\mathcal{S}}$.

Proof. By Proposition 7.4.7 and Theorem 7.2.4, $G_{\mathcal{S}}$ can be embedded in a finitely-presented group $H_0 = \langle \mathcal{X}_0 : \mathcal{R}_0 \rangle$ with polynomial isoperimetric function d_{H_0}. Let $\mathcal{X}_1 = \mathcal{X}_0 \backslash \{J, X, Z\}$, and $\mathcal{X}_H = \{J, X, Z\} \cup \{s_y, t_y : y \in \mathcal{X}_1\}$. Define $f : \mathcal{F}_{\mathcal{X}_0} \to \mathcal{F}_{\mathcal{X}_H}$ by $f(y) = y$ for $y \in \{J, X, Z\}$ and $f(y) = s_y t_y$ for $y \in \mathcal{X}_1$, so in other words $f(w)$ is the word w with y replaced by $s_y t_y$ for all $y \in \mathcal{X}_1$. Finally, let $\mathcal{R}_H = \{z^2 : z \in \mathcal{X}_H\} \cup \{f(r) : r \in \mathcal{R}_0\}$. Then

$$\langle \mathcal{X}_H : \mathcal{R}_H \rangle = \langle H_0, s_y, t_y \text{ for } y \in \mathcal{X}_1 : s_y^2 = t_y^2 = 1 \text{ and } y = s_y t_y \text{ for all } y \in \mathcal{X}_1 \rangle,$$

and thus H_0 is a subgroup of $H := \langle \mathcal{X}_H : \mathcal{R}_H \rangle$ by repeatedly applying Lemma 7.2.1. The inclusion $\iota : G_0 \hookrightarrow H_0 \hookrightarrow H$ satisfies parts (a) and (b) of the proposition. Let ℓ be the length of the longest relation in $\mathcal{R}_0$. If $w \in \mathcal{F}_{\mathcal{X}_G}$ is trivial in $G_{\mathcal{S}}$, then w is also trivial in H_0. Hence by Lemma 7.2.3, there are $r_1, \ldots, r_k \in \mathcal{R}_0 \cup \mathcal{R}_0^{-1}$ and $z_1, \ldots, z_k \in \mathcal{F}_{\mathcal{X}_0}$ such that

$$w = z_1 r_1 z_1^{-1} z_2 r_2 z_2^{-1} \cdots z_k r_k z_k^{-1},$$

where $k \leqslant d_0(|w|)$ and $|z_i| \leqslant \ell k + \ell + |w|$ for all $1 \leqslant i \leqslant k$. Thus

$$\iota(w) = f(z_1) f(r_1) f(z_1)^{-1} \cdots f(z_k) f(r_k) f(z_k)^{-1}.$$

Since d_{H_0} is polynomial, $f(r_i) \in \mathcal{R}_H \cup \mathcal{R}_H^{-1}$ for all $1 \leqslant i \leqslant k$, and $|w| \leqslant |f(w)| \leqslant 2|w|$ for all $w \in \mathcal{F}_{\mathcal{X}_0}$, part (c) is true with e.g. $d_{\mathcal{S}}(n) := 2\ell d_{H_0}(n) + 2\ell + 2n$. □

7.4.2 Construction of $\mathcal{A}_{\mathcal{S}}(m)$

For this section, we fix a finitely-presented group $H_{\mathcal{S}} = \langle \mathcal{X}_H : \mathcal{R}_H \rangle$ and a polynomial $d_{\mathcal{S}}$ as in Proposition 7.4.8, and identify $G_{\mathcal{S}}$ with its image in $H_{\mathcal{S}}$ (so we do not mention the embedding ι explicitly). In particular, if $w \in \mathcal{F}_{\mathcal{X}_G}$, then $|w|$ will denote the length of w in $H_{\mathcal{S}}$ rather than $G_{\mathcal{S}}$ unless otherwise noted. The variables J, X, and Z will continue to denote generators of $H_{\mathcal{S}}$, while S, T and W will be length two words in $H_{\mathcal{S}}$. We also continue with the notation $X_{mi} = S^i W^m X W^{-m} S^{-i}$ and $Z_{mi} = T^i W^m Z W^{-m} T^{-i}$. Now that we are working with algebras, we let $[A, B]$ denote the algebra commutator $AB - BA$ instead of the group commutator.

To define $\mathcal{A}_{\mathcal{S}}(m)$, consider the set of variables

$$\mathcal{X}_0 := \{U_1, U_2, \widetilde{X}, \widetilde{Z}, O_P, O_Q\},$$

and let

$$U := U_1 U_2, \quad P := \frac{\mathbb{1} - O_P}{2}, \text{ and } Q := \frac{\mathbb{1} - O_Q}{2}$$

in $\mathbb{C}^*\langle \mathcal{X}_0 \rangle$. For every $m \in \mathbb{N}$, let $\mathcal{A}_{\mathcal{S}}(m)$ be the finitely presented $*$-algebra generated by $\mathcal{X}_H \cup \mathcal{X}_0$, subject to the relations

(R0) $x^* x = x x^* = x^2 = 1$ for all $x \in \mathcal{X}_H \cup \mathcal{X}_0$,

(R1) $r = 1$ for all $r \in \mathcal{R}_H$, i.e. all the relations for $H_{\mathcal{S}}$ hold,

(R2) $[U, X] = [U, Z] = [U, S] = [U, T] = [U, J] = [Q, X] = [Q, Z] = [Q, S] = [Q, T] = [Q, J] = 0$, i.e. U and Q commute with X,Z,S,T, and J,

(R3) $[\widetilde{X}, Q] = \widetilde{X}Q - X_{m,0}Q = 0$ and $[\widetilde{Z}, Q] = \widetilde{Z}Q - Z_{m,0}Q = 0$,

(R4) $U\widetilde{X}U^* - S\widetilde{X}S^* = U\widetilde{Z}U^* - T\widetilde{Z}T^* = 0$,

(R5) $[P, Q] = 0$, i.e. P commutes with Q, and

(R6) $(P + \widetilde{X}P\widetilde{X} - UPU^*)(\mathbb{1} + J\widetilde{X}\widetilde{Z}\widetilde{X}\widetilde{Z}) = 0.$

Note that relations (R0) imply that all the generators are order-two unitaries, so $\mathcal{A}_{\mathcal{S}}(m) = \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}_H \cup \mathcal{X}_0}/\langle \mathcal{R}_m \rangle$, where $\mathcal{R}_m$ denotes the relations in (R1)-(R6). Since O_P and O_Q have order two, P and Q are projections in $\mathcal{A}_{\mathcal{S}}(m)$. The point of the generators O_P and O_Q is to add the projections P and Q while making $\mathcal{A}_{\mathcal{S}}(m)$ a quotient of a free product of $\mathbb{Z}_2$'s. Similarly, the point of U_1 and U_2 is to add the unitary U without putting any restriction on its order. For the intuition behind the remaining relations, see the representation constructed in the proof of Lemma 7.4.10 below. Before proceeding to the lemma, we record some facts about the presentation for later use:

Remark 7.4.9.

1. *If $\mathcal{A} = \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}_H \cup \mathcal{X}_0}$, then $\|r\|_{\mathcal{A}} \leqslant 6$ for all $r \in \mathcal{R}_m$.*

2. *The number of relations in $\mathcal{R}_m$ is independent of m.*

3. *The relations r in (R3) satisfy $\|r\|_{1,1} \leqslant 2m + 3$, and the other relations in $\mathcal{R}_m$ do not depend on m.*

Lemma 7.4.10. *If $m \in \mathcal{S}$ then there is a tracial state τ on $\mathcal{A}_{\mathcal{S}}(m)$ such that $\tau(PQ) > 0$.*

Proof. Suppose $m \in \mathcal{S}$ and let $n := h(m) < \infty$, so the Turing machine M halts at the n-th step on the input m. Let τ_0 be the canonical trace on $\mathbb{C}H_{\mathcal{S}}$, and let $(\pi : \mathbb{C}H_{\mathcal{S}} \to \mathcal{B}(\mathcal{H}_0), v)$ be the GNS representation of τ_0. Let $\mathcal{H}_1$ be the Hilbert space $\ell^2(\mathbb{Z}_{n+1})$ with the canonical basis $\{e_i : i \in \mathbb{Z}_{n+1}\}$, let $E_{i,i}$ be the rank-one projection onto e_i for every $i \in \mathbb{Z}_{n+1}$, and let $C : e_i \mapsto e_{i+1}$ be the left cyclic shift operator on $\ell^2(\mathbb{Z}_{n+1})$. Let $\widetilde{\mathcal{H}} = \mathcal{H}_0 \otimes \mathcal{H}_1$, and define a $*$-representation $\widetilde{\pi} : \mathbb{C}^*\langle \mathcal{X}_H \cup \mathcal{X}_0 \rangle \to \mathcal{B}(\widetilde{\mathcal{H}} \oplus \widetilde{\mathcal{H}})$ by

$$\widetilde{\pi}(x) = \begin{pmatrix} \pi(x) \otimes Id_{\mathcal{H}_1} & \\ & \pi(x) \otimes Id_{\mathcal{H}_1} \end{pmatrix} \text{ for all } x \in \mathcal{X}_H,$$

$$\widetilde{\pi}(U_1) = \begin{pmatrix} & Id_{\mathcal{H}_0} \otimes C \\ Id_{\mathcal{H}_0} \otimes C^{-1} & \end{pmatrix}, \quad \widetilde{\pi}(U_2) = \begin{pmatrix} & Id_{\widetilde{\mathcal{H}}} \\ Id_{\widetilde{\mathcal{H}}} & \end{pmatrix},$$

$$\widetilde{\pi}(\widetilde{X}) = \begin{pmatrix} \sum_{i=0}^{n} \pi(X_{mi}) \otimes E_{-i,-i} & \\ & \sum_{i=0}^{n} \pi(X_{mi}) \otimes E_{i,i} \end{pmatrix},$$

$$\widetilde{\pi}(\widetilde{Z}) = \begin{pmatrix} \sum_{i=0}^{n} \pi(Z_{mi}) \otimes E_{-i,-i} & \\ & \sum_{i=0}^{n} \pi(Z_{mi}) \otimes E_{i,i} \end{pmatrix},$$

$$\widetilde{\pi}(Q) = \begin{pmatrix} Id_{\mathcal{H}_0} \otimes E_{0,0} & \\ & Id_{\mathcal{H}_0} \otimes E_{0,0} \end{pmatrix}, \text{ and}$$

$$\widetilde{\pi}(P) = \begin{pmatrix} \sum_{i=0}^{n} \pi(P_i) \otimes E_{-i,-i} & \\ & \sum_{i=0}^{n} \pi(P_i) \otimes E_{i,i} \end{pmatrix},$$

where in the last equation $P_i := (\frac{\mathbb{1}-J}{2})(\frac{\mathbb{1}-Z_{m,i}}{2})(\frac{\mathbb{1}-Z_{m,i+1}}{2}) \cdots (\frac{\mathbb{1}-Z_{m,n-1}}{2})$ for all $0 \leqslant i \leqslant n-1$, and $P_n := \frac{\mathbb{1}-J}{2}$. Note that

$$\widetilde{\pi}(U) = \widetilde{\pi}(U_1)\widetilde{\pi}(U_2) = \begin{pmatrix} Id_{\mathcal{H}_0} \otimes C & \\ & Id_{\mathcal{H}_0} \otimes C^{-1} \end{pmatrix}.$$

It is not hard to check that $\widetilde{\pi}(r) = 0$ for all relations r in (R0)-(R6). Indeed, it is clear that $\widetilde{\pi}(x)$ is a unitary squaring to $\mathbb{1}$ for $x \in \mathcal{X}_H \cup \{U_1, U_2, \widetilde{X}, \widetilde{Z}\}$, and $\widetilde{\pi}(Q)$ is a projection. Since $Z_{m,0}, \cdots, Z_{m,n-1}$ and J commute in $\mathbb{C}H_{\mathcal{S}}$, $\widetilde{\pi}(P)$ is a projection as well. So $\widetilde{\pi}(r) = 0$ for all r in (R0). We also have $\widetilde{\pi}(r) = 0$ for r in (R1), (R2), and (R5) by inspection. For (R3),

$$\widetilde{\pi}(\widetilde{X})\widetilde{\pi}(Q) = \widetilde{\pi}(Q)\widetilde{\pi}(\widetilde{X}) = \widetilde{\pi}(X_{m,0})\widetilde{\pi}(Q) = \begin{pmatrix} \pi(X_{m,0}) \otimes E_{0,0} & \\ & \pi(X_{m,0}) \otimes E_{0,0} \end{pmatrix},$$

and similarly $\widetilde{\pi}(\widetilde{Z})\widetilde{\pi}(Q) = \widetilde{\pi}(Q)\widetilde{\pi}(\widetilde{Z}) = \widetilde{\pi}(Z_{m,0})\widetilde{\pi}(Q)$. For (R4), recall from the presentation of $G_{\mathcal{S}}$ that $\pi(X_{m,0}) = \pi(X_{m,n+1})$ and $\pi(S)\pi(X_{m,i})\pi(S^*) = \pi(X_{m,i+1})$ for all $i \in \mathbb{Z}$. Since $CE_{i,i}C^{-1} = E_{i+1,i+1}$ for all $i \in \mathbb{Z}_{n+1}$,

$$\widetilde{\pi}(S)\widetilde{\pi}(\widetilde{X})\widetilde{\pi}(S^*) = \begin{pmatrix} \sum_{i=0}^{n} \pi(X_{m,i+1}) \otimes E_{-i,-i} & \\ & \sum_{i=0}^{n} \pi(X_{m,i+1}) \otimes E_{i,i} \end{pmatrix}$$

$$= \begin{pmatrix} \sum_{i=0}^{n} \pi(X_{m,i}) \otimes E_{-(i-1),-(i-1)} & \\ & \sum_{i=0}^{n} \pi(X_{m,i}) \otimes E_{i-1,i-1} \end{pmatrix}$$
$$= \widetilde{\pi}(U)\widetilde{\pi}(\widetilde{X})\widetilde{\pi}(U^*).$$

Similarly $\widetilde{\pi}(T)\widetilde{\pi}(\widetilde{Z})\widetilde{\pi}(T^*) = \widetilde{\pi}(U)\widetilde{\pi}(\widetilde{Z})\widetilde{\pi}(U^*)$. This just leaves (R6). For this case,

$$\widetilde{\pi}\big((P + \widetilde{X}P\widetilde{X} - UPU^*)(\mathbb{1} + J\widetilde{X}\widetilde{Z}\widetilde{X}\widetilde{Z})\big) = \begin{pmatrix} A_1 & \\ & A_2 \end{pmatrix} \text{ where}$$
$$A_1 = \sum_{i=0}^{n} \pi\big((P_i + X_{mi}P_iX_{mi} - P_{i+1})(1 + JX_{mi}Z_{mi}X_{mi}Z_{mi})\big) \otimes E_{-i,-i},$$
$$A_2 = \sum_{i=0}^{n} \pi\big((P_i + X_{mi}P_iX_{mi} - P_{i+1})(1 + JX_{mi}Z_{mi}X_{mi}Z_{mi})\big) \otimes E_{i,i},$$

and $P_{n+1} := P_0$. Recall from the presentation of $G_{\mathcal{S}}$ that J is a unitary of order 2 and is central. Hence in $\mathbb{C}H_{\mathcal{S}}$, $\frac{1-J}{2}$ and $\frac{1+J}{2}$ are projections, and $(\frac{1+J}{2})P_i = 0$ for $0 \leqslant i \leqslant n$. Also for all $0 \leqslant i \leqslant n-1$, $X_{mi}Z_{mi}X_{mi}Z_{mi} = J$, X_{mi} commutes with P_{i+1}, and $P_i = (\frac{1-Z_{mi}}{2})P_{i+1}$. Hence $1 + JX_{mi}Z_{mi}X_{mi}Z_{mi} = 2$, and

$$P_i + X_{mi}P_iX_{mi} - P_{i+1} = (\tfrac{1-Z_{mi}}{2})P_{i+1} + (\tfrac{1-JZ_{mi}}{2})P_{i+1} - P_{i+1} = -Z_{mi}(\tfrac{1+J}{2})P_{i+1} = 0.$$

For $i = n$, $X_{mn}Z_{mn}X_{mn}Z_{mn} = 1$, so

$$(P_n + X_{mn}P_nX_{mn} - P_0)(1 + JX_{mn}Z_{mn}X_{mn}Z_{mn}) = (2 - P_0)\tfrac{(1-J)(1+J)}{2} = 0.$$

It follows that $\pi\big((P_i + X_{mi}P_iX_{mi} - P_{i+1})(1 + JX_{mi}Z_{mi}X_{mi}Z_{mi})\big) = 0$ for all $0 \leqslant i \leqslant n$, and hence $A_1 = A_2 = 0$. We conclude that $\widetilde{\pi}(r) = 0$ for all r in (R0)-(R6). Hence $\widetilde{\pi}$ induces a representation of $\mathcal{A}_{\mathcal{S}}(m)$ on $\widetilde{\mathcal{H}} \oplus \widetilde{\mathcal{H}}$.

The image of $\widetilde{\pi}$ is contained in $M_2\big(\pi(\mathbb{C}H_{\mathcal{S}}) \otimes \mathcal{B}(\mathcal{H}_1)\big)$ This algebra is isomorphic to $\pi(\mathbb{C}H_{\mathcal{S}}) \otimes M_{2(n+1)}(\mathbb{C})$, which has a tracial state $\tau := \tau_0 \otimes \tau'$ where τ' is the unique tracial state on $M_{2(n+1)}(\mathbb{C})$. Finally,

$$\tau\big(\widetilde{\pi}(PQ)\big) = \tau \begin{pmatrix} \pi(P_0) \otimes E_{0,0} & \\ & \pi(P_0) \otimes E_{0,0} \end{pmatrix} = \tfrac{1}{(n+1)}\tau_0(P_0) = \tfrac{1}{2^{n+1}(n+1)} > 0,$$

so the lemma follows. □

We now look at what happens when $m \notin \mathcal{S}$. For all $n \geqslant 0$, let

$$\widetilde{P}_n := QU^nPU^{-n}Q \text{ and } \widetilde{X}_n := U^n\widetilde{X}U^{-n}$$

in $\mathbb{C}^*\langle \mathcal{X}_H \cup \mathcal{X}_0 \rangle$. Note that $\widetilde{X}_n^2 = 1$ in $\mathbb{C}\mathbb{Z}_2^{\mathcal{X}_H \cup \mathcal{X}_0}$.

Proposition 7.4.11. *There are constants C and k such that for any $m \in \mathbb{N}$ and $0 \leqslant n < h(m)$, $\widetilde{P}_n + \widetilde{X}_n\widetilde{P}_n\widetilde{X}_n - \widetilde{P}_{n+1}$ is trivial in $\mathcal{A}_{\mathcal{S}}(m) = \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}_H \cup \mathcal{X}_0}/\langle \mathcal{R}_m \rangle$, and has an $\mathcal{R}_m$-decomposition in $\mathbb{C}\mathbb{Z}_2^{\mathcal{X}_H \cup \mathcal{X}_0}$ of size $\leqslant C\big((n+1)m\big)^k$.*

Although we won't need this, the constants C and k can be computed from a description of the Turing machine $M_{\mathcal{S}}$ that recognizes $\mathcal{S}$.

Proof. For the proof, say that $\alpha(n) = O(\beta(n))$ for functions α, β if there is a constant $C > 0$ such that $\alpha(n) \leqslant C\beta(n) + C$ for all $n \geqslant 0$. Recall from Remark 7.4.9 that $\|r\|_{\mathcal{A}} \leqslant 6$ for all $r \in \mathcal{R}_m$ when $\mathcal{A} = \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}_H \cup \mathcal{X}_0}$. Let

$$f = QU^n(P + \widetilde{X}P\widetilde{X} - UPU^*)U^{-n} \text{ and } g = U^n(1 + J\widetilde{X}\widetilde{Z}\widetilde{X}\widetilde{Z})U^{-n}Q.$$

By relation (R6), fg is trivial in $\mathcal{A}_{\mathcal{S}}(m)$ and has an $\mathcal{R}_m$-decomposition in $\mathcal{A}$ of size $6n + 4$. To prove the proposition, we show that

$$fg = 2\left(\widetilde{P}_n + \widetilde{X}_n\widetilde{P}_n\widetilde{X}_n - \widetilde{P}_{n+1}\right)$$

in $\mathcal{A}_{\mathcal{S}}(m)$, while keeping track of the size using Lemma 7.3.3. For the first step, since U and S commute and $U\widetilde{X}U^* = S\widetilde{X}S^*$, we see that $\widetilde{X}_n = S^n\widetilde{X}S^{-n}$ in $\mathcal{A}_{\mathcal{S}}(m)$. Similarly $U^n\widetilde{Z}U^{-n} = T^n\widetilde{Z}T^{-n}$ and U commutes with J, so

$$g = (1 + JS^n\widetilde{X}S^{-n} \cdot T^n\widetilde{Z}T^{-n} \cdot S^n\widetilde{X}S^{-n} \cdot T^n\widetilde{Z}T^{-n})Q.$$

Replacing $U^n\widetilde{X}U^{-n}$ and $U^n\widetilde{Z}U^{-n}$ with $S^n\widetilde{X}S^{-n}$ and $T^n\widetilde{Z}T^{-n}$ requires $O(n^2)$ applications of the defining relations, and the intermediate polynomials in this calculation have degree $O(n)$, so by Lemma 7.3.3,

$$g - (1 + JS^n\widetilde{X}S^{-n} \cdot T^n\widetilde{Z}T^{-n} \cdot S^n\widetilde{X}S^{-n} \cdot T^n\widetilde{Z}T^{-n})Q$$

has an $\mathcal{R}_m$-decomposition of size $O(n^3)$.

Next, $\widetilde{X}_n Q = Q\widetilde{X}_n = S^n \widetilde{X} Q S^{-n} = Q X_{mn}$ and $U^n \widetilde{Z} U^{-n} Q = Q Z_{mn}$ for all $n \geqslant 0$ by relations (R2) and (R3), so

$$(1 + JS^n \widetilde{X} S^{-n} \cdot T^n \widetilde{Z} T^{-n} \cdot S^n \widetilde{X} S^{-n} \cdot T^n \widetilde{Z} T^{-n}) Q = Q(1 + J X_{mn} Z_{mn} X_{mn} Z_{mn}).$$

This identity requires using the relations $O(n)$ times, and X_{mn} and Z_{mn} have degree $O(m+n)$, so by Lemma 7.3.3 again,

$$(1 + JS^n \widetilde{X} S^{-n} \cdot T^n \widetilde{Z} T^{-n} \cdot S^n \widetilde{X} S^{-n} \cdot T^n \widetilde{Z} T^{-n}) Q - Q(1 + J X_{mn} Z_{mn} X_{mn} Z_{mn})$$

has an $\mathcal{R}_m$-decomposition of size $O(n^2 + nm)$.

Now suppose that $0 \leqslant n < h(m)$. From the presentation of $G_{\mathcal{S}}$, we see that

$$X_{mn} Z_{mn} X_{mn} Z_{mn} = J,$$

so $Q(1 + J X_{mn} Z_{mn} X_{mn} Z_{mn}) = Q(1 + J^2) = 2Q$. The word $J X_{mn} Z_{mn} X_{mn} Z_{mn}$ has length $16m + 16n + 5$, so by Proposition 7.4.8, part (c) there are $r_1, \ldots, r_k \in \mathcal{R}_H \cup \mathcal{R}_H^{-1}$ and $z_1, \ldots, z_k \in \mathcal{F}_{\mathcal{X}_H}$ with $J X_{mn} Z_{mn} X_{mn} Z_{mn} = z_1 r_1 z_1^{-1} \cdots z_k r_k z_k^{-1}$ in $\mathcal{F}_{\mathcal{X}_H}$, $k \leqslant d_{\mathcal{S}}(16m + 16n + 5)$, and $|z_i| \leqslant d_{\mathcal{S}}(16m + 16n + 5)$ for all $1 \leqslant i \leqslant k$. Replacing r_i with 1 from right to left, we see that $Q(1 + J X_{mn} Z_{mn} X_{mn} Z_{mn}) - 2Q$ has an $\mathcal{R}_m$-decomposition of size $O(d_{\mathcal{S}}(16m + 16n + 5)^2) = O(d_{\mathcal{S}}(m)^2 + d_{\mathcal{S}}(n)^2)$. From Lemma 7.3.3, part (c), we get that $fg - 2fQ$ has an $\mathcal{R}_m$-decomposition of size $O(n^3 + n^2 + nm + d_{\mathcal{S}}(m)^2 + d_{\mathcal{S}}(m)^2)$.

We now look at fQ. Since Q commutes with $\widetilde{X}_n$,

$$\begin{aligned} fQ &= QU^n P U^{-n} Q + QU^n \widetilde{X} P \widetilde{X} U^{-n} Q - QU^{n+1} P U^{-(n+1)} Q \\ &= \widetilde{P}_n + Q\widetilde{X}_n \cdot U^n P U^{-n} \cdot \widetilde{X}_n Q - \widetilde{P}_{n+1} \\ &= \widetilde{P}_n + \widetilde{X}_n \cdot \widetilde{P}_n \cdot \widetilde{X}_n - \widetilde{P}_{n+1}. \end{aligned}$$

This identity requires replacing $\widetilde{X}_n$ with $S^n \widetilde{X} S^{-n}$ again, so

$$fQ - (\widetilde{P}_n + \widetilde{X}_n \cdot \widetilde{P}_n \cdot \widetilde{X}_n - \widetilde{P}_{n+1})$$

has an $\mathcal{R}_m$-decomposition of size $O(n^3)$. Ultimately we conclude that $\widetilde{P}_n + \widetilde{X}_n \cdot \widetilde{P}_n \cdot \widetilde{X}_n - \widetilde{P}_{n+1}$ has an $\mathcal{R}_m$-decomposition of size $O(n^3 + n^2 + nm + d_{\mathcal{S}}(m)^2 + d_{\mathcal{S}}(m)^2)$. □

Proof of Theorem 7.4.1. Let $\mathcal{X} = \mathcal{X}_H \cup \mathcal{X}_0$, and let $\widetilde{P}_n$, $\widetilde{X}_n$, and $\mathcal{R}_m$ be as above. The relations in (R1) are independent of m, and the remaining relations are spelled out explicitly in (R2)-(R6), so we see that the mapping $m \mapsto \mathcal{R}_m$ is computable. Parts (a) and (d) of the theorem hold by construction, and part (b) follows from Proposition 7.4.11. Finally, since $[P, Q] = 0$ in $\mathcal{A}_{\mathcal{S}}(m)$, Lemma 7.4.10 implies that there is a tracial state τ on $\mathcal{A}_{\mathcal{S}}(m)$ with $\tau(\widetilde{P}_0^2) = \tau(PQ) > 0$. □

7.5 Proof of Theorem 7.1.3

In this section, we prove the following theorem.

Theorem 7.5.1. *There is an integer n_0, such that for all $N \geqslant n_0$, the promise problem*

> *Given $\alpha \in \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle$, determine if α is trace-positive in $\mathbb{C}^*\langle x_1, \ldots, x_N\rangle$, or if $\pi(\alpha)$ is not trace-positive in $\mathbb{C}\mathbb{Z}_2^{*N}$, promised that one of the two is the case.*

is coRE-hard, where $\pi : \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle \to \mathbb{Q}\mathbb{Z}_2^{*N}$ is the homomorphism sending x_i to the generator of the ith factor of $\mathbb{Z}_2^{*N}$.

Suppose that $N \geqslant n_0$, and that the homomorphism π in Theorem 7.5.1 factors through a $*$-algebra $\mathcal{A}$, meaning that there are homomorphisms $\pi_1 : \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle \to \mathcal{A}$ and $\pi_2 : \mathcal{A} \to \mathbb{Q}\mathbb{Z}_2^{*N}$ such that $\pi = \pi_2 \circ \pi_1$. Suppose also that we have some way of representing the elements of $\mathcal{A}$ as strings such that the homomorphism π_1 is computable. Then Theorem 7.5.1 has the following immediate corollary:

Corollary 7.5.2. *It is coRE-hard to determine whether $\alpha \in \mathcal{A}$ is trace-positive in $\mathcal{A}_{\mathbb{C}}$.*

Proof. Suppose $\alpha \in \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle$. If α is trace-positive in $\mathbb{C}^*\langle x_1, \ldots, x_N\rangle$, then $\pi_1(\alpha)$ is trace-positive in $\mathcal{A}_{\mathbb{C}}$. If $\pi(\alpha)$ is not trace-positive in $\mathbb{C}\mathbb{Z}_2^{*N}$, then there is a tracial state τ on $\mathbb{C}\mathbb{Z}_2^{*N}$ such that $(\tau \circ \pi_2)(\pi_1(\alpha)) = \tau(\pi(\alpha)) < 0$, so $\pi_1(\alpha)$ is not trace-positive in $\mathcal{A}_{\mathbb{C}}$. Since π_1 is computable, the promise problem in Theorem 7.5.1 reduces to the problem of determining if $\alpha \in \mathcal{A}$ is trace-positive. □

Theorem 7.1.3 is a special case of Corollary 7.5.2 with $\mathcal{A} = \mathbb{Q}^*\{x_1, \ldots, x_N\}$, $\mathbb{Q}\mathcal{F}_N$, or $\mathbb{Q}\mathbb{Z}_M^{*N}$ (for every $M \geqslant M'$, there is a $*$-homomorphism $\mathbb{Q}\mathbb{Z}_M^{*N} \to \mathbb{Q}\mathbb{Z}_{M'}^{*N}$ sending the ith generator of $\mathbb{Q}\mathbb{Z}_M^{*N}$ to the ith generator of $\mathbb{Q}\mathbb{Z}_{M'}^{*N}$). The corollary also applies to other algebras such as the algebra of contractions and the algebra of self-adjoint contractions, as well as free products of any of the algebras mentioned.

For the proof of Theorem 7.5.1, suppose $\mathcal{S} \subseteq \mathbb{N}$ is an RE set, and let $\mathcal{X}$, $\widetilde{P}_n$ and $\widetilde{X}_n$, $n \geqslant 0$, and $\mathcal{A}_{\mathcal{S}}(m) = \mathbb{C}^*\langle \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} : \mathcal{R}_m \rangle$, $m \geqslant 1$, be as in Theorem 7.4.1. Before proceeding to the proof, we need the following propositions.

Proposition 7.5.3. *There are positive integers Λ, k such that if $m \notin \mathcal{S}$ and τ is a tracial $(\epsilon, \mathcal{R}_m)$-state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ for some $\epsilon \geqslant 0$, then $\|\widetilde{P}_0\|_\tau \leqslant \Lambda m^k \sqrt{\epsilon}$.*

Proof. Let C and k be the constants from Theorem 7.4.1, part (b). Suppose $m \notin \mathcal{S}$, $\epsilon \geqslant 0$, and τ is a tracial $(\epsilon, \mathcal{R}_m)$-state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$. By Theorem 7.4.1, part (a), $\widetilde{X}_n$ is a unitary involution in $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$. Since τ is tracial, $\|\widetilde{P}_n\|_\tau = \|\widetilde{X}_n \widetilde{P}_n \widetilde{X}_n\|_\tau$ for all n. Also $\widetilde{P}_n$ and $\widetilde{X}_n \widetilde{P}_n \widetilde{X}_n$ are hermitian squares in $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$, so $\tau(\widetilde{P}_n \widetilde{X}_n \widetilde{P}_n \widetilde{X}_n) = \tau(\widetilde{X}_n \widetilde{P}_n \widetilde{X}_n \widetilde{P}_n) \geqslant 0$. Hence

$$\begin{aligned}
\|\widetilde{P}_n\|_\tau^2 = \tau(\widetilde{P}_n^2) &= \tfrac{1}{2}\Big(\tau(\widetilde{P}_n^2) + \tau\big((\widetilde{X}_n \widetilde{P}_n \widetilde{X}_n)^2\big)\Big) \\
&\leqslant \tfrac{1}{2}\Big(\tau(\widetilde{P}_n^2) + \tau\big((\widetilde{X}_n \widetilde{P}_n \widetilde{X}_n)^2\big) + \tau(\widetilde{P}_n \widetilde{X}_n \widetilde{P}_n \widetilde{X}_n) + \tau(\widetilde{X}_n \widetilde{P}_n \widetilde{X}_n \widetilde{P}_n)\Big) \\
&= \tfrac{1}{2}\tau\big((\widetilde{P}_n + \widetilde{X}_n \widetilde{P}_n \widetilde{X}_n)^2\big) = \tfrac{1}{2}\|\widetilde{P}_n + \widetilde{X}_n \widetilde{P}_n \widetilde{X}_n\|_\tau^2.
\end{aligned}$$

By Proposition 7.3.4 and Theorem 7.4.1, part (b), $\|\widetilde{P}_n + \widetilde{X}_n \widetilde{P}_n \widetilde{X}_n - \widetilde{P}_{n+1}\|_\tau \leqslant C((n+1)m)^k \sqrt{\epsilon}$ for all $n \geqslant 0$. It follows that

$$\begin{aligned}
\|\widetilde{P}_n\|_\tau &\leqslant \tfrac{1}{\sqrt{2}}\|\widetilde{P}_n + \widetilde{X}_n \widetilde{P}_n \widetilde{X}_n\|_\tau \\
&\leqslant \tfrac{1}{\sqrt{2}}(\|\widetilde{P}_{n+1}\|_\tau + \|\widetilde{P}_n + \widetilde{X}_n \widetilde{P}_n \widetilde{X}_n - \widetilde{P}_{n+1}\|_\tau) \\
&\leqslant \tfrac{1}{\sqrt{2}}\|\widetilde{P}_{n+1}\|_\tau + \tfrac{1}{\sqrt{2}} C((n+1)m)^k \sqrt{\epsilon}.
\end{aligned}$$

By induction, we obtain

$$\|\widetilde{P}_0\|_\tau \leqslant (\tfrac{1}{\sqrt{2}})^t \|\widetilde{P}_t\|_\tau + C \sum_{n=1}^{t} \frac{n^k}{2^{n/2}} m^k \sqrt{\epsilon}$$

for all $t \geqslant 1$. Since $\widetilde{P}_t$ is a contraction in $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ by Theorem 7.4.1, part (a), $\|\widetilde{P}_t\|_\tau \leqslant 1$ for all $t \geqslant 1$. The series $\sum_{n=1}^{\infty} \frac{n^k}{2^{n/2}}$ converges, so taking $t \to +\infty$, we conclude that

$$\|\widetilde{P}_0\|_\tau \leqslant \Lambda m^k \sqrt{\epsilon}$$

for any integer $\Lambda \geqslant C \sum_{n=1}^{\infty} \frac{n^k}{2^{n/2}}$. □

Proposition 7.5.4. *Let $\mathcal{W}$ be the mapping from Lemma 7.3.11, and let*

$$\mathcal{W}_m := \left(\bigcup_{r \in \mathcal{R}_m \cup \mathcal{R}_m^*} \mathcal{W}(r) \right) \cup \mathcal{W}(\widetilde{P}_0) \cup \mathcal{R}_m$$

for $m \in \mathbb{N}$. There are positive integers $\widetilde{\Lambda}, k'$ such that if $m \notin \mathcal{S}$ and τ is a tracial $(\epsilon, \mathcal{W}_m)$-state on $\mathbb{C}^*\langle \mathcal{X} \rangle$, then $\|\widetilde{P}_0\|_\tau \leqslant \widetilde{\Lambda} m^{k'} \sqrt{\epsilon}$.

Proof. Let Λ, k be integers from Proposition 7.5.3, and let D be the integer from Theorem 7.4.1, part (d). Suppose $m \notin \mathcal{S}$, $\epsilon \geqslant 0$, and τ is a tracial $(\epsilon, \mathcal{W}_m)$-state on $\mathbb{C}^*\langle \mathcal{X} \rangle$. By Lemma 7.3.11, there is a tracial state $\widehat{\tau}$ on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ such that

$$\left| \|r\|_{\widehat{\tau}} - \|r\|_\tau \right| \leqslant 2\|r\|_{1,1} \sqrt{\epsilon} \leqslant 2Dm\sqrt{\epsilon}$$

for all $r \in \mathcal{R}_m \cup \mathcal{R}_m^*$. Since $\mathcal{R}_m \subseteq \mathcal{W}_m$, τ is an $(\epsilon, \mathcal{R}_m)$-state. For every $r \in \mathcal{R}_m \cup \mathcal{R}_m^*$, $\|r\|_\tau \leqslant \sqrt{\epsilon}$, and hence $\|r\|_{\widehat{\tau}} \leqslant (2Dm+1)\sqrt{\epsilon}$. We conclude that $\widehat{\tau}$ is a tracial $\left((2Dm+1)^2\epsilon, \mathcal{R}_m\right)$-state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$. By Proposition 7.5.3, $\|\widetilde{P}_0\|_{\widehat{\tau}} \leqslant \Lambda m^k \sqrt{(2Dm+1)^2\epsilon} = (2Dm+1)\Lambda m^k \sqrt{\epsilon}$. Again by Lemma 7.3.11, since $\tau(s^*s) \leqslant \epsilon$ for all $s \in \mathcal{W}(\widetilde{P}_0)$, we have

$$\left| \|\widetilde{P}_0\|_{\widehat{\tau}} - \|\widetilde{P}_0\|_\tau \right| \leqslant 2\|\widetilde{P}_0\|_{1,1} \sqrt{\epsilon} = 3\sqrt{\epsilon}.$$

It follows that

$$\|\widetilde{P}_0\|_\tau \leqslant \left((2Dm+1)\Lambda m^k + 3\right) \sqrt{\epsilon} \leqslant 6D\Lambda m^{k+1} \sqrt{\epsilon}.$$

Taking $\widetilde{\Lambda} := 6D\Lambda$ and $k' := k+1$ completes the proof. □

Proof of Theorem 7.5.1 . Let $n_0 := |\mathcal{X}|$, and suppose we are given an integer $N \geqslant n_0$. Pick an ordering on $\mathcal{X}$ so we can identify $\mathbb{Q}^*\langle\mathcal{X}\rangle$ with the subalgebra $\mathbb{Q}^*\langle x_1, \ldots, x_{n_0}\rangle$ of $\mathbb{Q}^*\langle x_1, \ldots, x_N\rangle$. We think of $\mathbb{C}^*\langle\mathcal{X}\rangle$ and $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ as subalgebras of $\mathbb{C}^*\langle x_1, \ldots, x_N\rangle$ and $\mathbb{C}\mathbb{Z}_2^{*N}$ similarly. Let $\widetilde{\Lambda}$, k', and $\mathcal{W}_m$ be as in Proposition 7.5.4. For any $m \in \mathbb{N}$, define a $*$-polynomial

$$\alpha(m) = \sum_{r \in \mathcal{W}_m \cup \mathcal{W}_m^*} r^* r - \frac{1}{\widetilde{\Lambda}^2 m^{2k'}} \widetilde{P}_0^* \widetilde{P}_0 \in \mathbb{Q}^*\langle\mathcal{X}\rangle \subseteq \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle. \tag{7.5.1}$$

Then $\alpha(m)$ is self-adjoint and the map $\alpha : \mathbb{N} \to \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle$ is computable by Theorem 7.4.1 and Lemma 7.3.11.

Let $\pi : \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle \to \mathbb{Q}\mathbb{Z}_2^{*N}$ be the homomorphism sending x_i to the ith generator of $\mathbb{Z}_2^{*N}$. Also let $q = q_2 \circ q_1$, where $q_1 : \mathbb{Q}\mathbb{Z}_2^{*N} \to \mathbb{Q}\mathbb{Z}_2^{*\mathcal{X}}$ is the homomorphism sending $x_i \mapsto x_i$ for $1 \leqslant i \leqslant n_0$ and $x_i \mapsto 1$ for $i > n_0$, and $q_2 : \mathbb{Q}\mathbb{Z}_2^{*\mathcal{X}} \to \mathcal{A}_{\mathcal{S}}(m)$ is the quotient map. By Theorem 7.4.1, if $m \in \mathcal{S}$ then there is a tracial state τ on $\mathcal{A}_{\mathcal{S}}(m)$ such that $\tau(\widetilde{P}_0^2) > 0$. By Lemma 7.3.11, $\pi(t) = 0$ for all $t \in \left(\bigcup_{r \in \mathcal{R}_m \cup \mathcal{R}_m^*} \mathcal{W}(r)\right) \cup \mathcal{W}(\widetilde{P}_0)$. Since $q(r) = 0$ for all $r \in \mathcal{R}_m$, $q(\pi(r^* r)) = 0$ for all $r \in \mathcal{W}_m \cup \mathcal{W}_m^*$, and hence $(\tau \circ q)(\pi(\alpha(m))) = -\frac{1}{\widetilde{\Lambda}^2 m^{2k'}} \tau(\widetilde{P}_0^2) < 0$. We conclude that $\pi(\alpha(m))$ is not trace-positive.

Now suppose $m \notin \mathcal{S}$, and that τ is a tracial state on $\mathbb{C}^*\langle x_1, \ldots, x_N\rangle$. Let $\epsilon := \sum_{r \in \mathcal{W}_m \cup \mathcal{W}_m^*} \tau(r^* r)$. Then τ is a tracial $(\epsilon, \mathcal{W}_m)$-state, so by Proposition 7.5.4, $\tau(\widetilde{P}_0^* \widetilde{P}_0) = \|\widetilde{P}_0\|_\tau^2 \leqslant \widetilde{\Lambda}^2 m^{2k'} \epsilon$. Hence $\tau(\alpha(m)) \geqslant 0$. Thus the complement $\overline{\mathcal{S}}$ of $\mathcal{S}$ reduces to the promise problem in the theorem statement. Taking $\mathcal{S}$ to be RE-hard, we see that the promise problem is coRE-hard. □

7.6 Proof of Theorem 7.1.1

The proof of Theorem 7.1.1 follows the same approach as the proof of Theorem 7.1.3. We start with a promise problem version of the theorem.

Theorem 7.6.1. *Suppose either $N \geqslant 2$ and $\mathcal{C} = \mathbb{C}\mathbb{Z}_3^{*N}$, or $N \geqslant 3$ and $\mathcal{C} = \mathbb{C}\mathbb{Z}_2^{*N}$. Let $\mathcal{P} = \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle$, and let $\pi : \mathcal{P} \to \mathcal{C}$ be the homomorphism sending x_i to the ith generator of $\mathcal{C}$. Then the promise problem*

Given $\alpha \in \mathcal{P} \otimes_{\mathbb{Q}} \mathcal{P}$, determine if α is positive in $\mathcal{P}_{\mathbb{C}} \otimes_{\mathbb{C}} \mathcal{P}_{\mathbb{C}}$, or if $(\pi \otimes \pi)(\alpha)$ is not positive in $\mathcal{C}_{\mathbb{C}} \otimes_{\mathbb{C}} \mathcal{C}_{\mathbb{C}}$, promised that one of the two is the case.

is coRE-hard.

To get Theorem 7.1.1 from Theorem 7.6.1, suppose that N, $\mathcal{C}$, $\mathcal{P}$, and π are as in the theorem, and that $\pi \otimes \pi$ factors through a $*$-algebra $\mathcal{A}$, meaning that there are homomorphisms $\pi_1 : \mathcal{P} \otimes \mathcal{P} \to \mathcal{A}$ and $\pi_2 : \mathcal{A} \to \mathcal{C} \otimes \mathcal{C}$ such that $\pi \otimes \pi = \pi_2 \circ \pi_1$. Suppose also that the first homomorphism π_1 in this factorization is computable. Then:

Corollary 7.6.2. *It is coRE-hard to determine whether $\alpha \in \mathcal{A}$ is positive in $\mathcal{A}_{\mathbb{C}}$.*

The proof is the same as the proof of Corollary 7.5.2, with the word "trace" deleted.

Theorem 7.1.1 follows immediately from Corollary 7.6.2 by taking $\mathcal{A}$ to be one of $\mathbb{Q}^*\langle x_1, \ldots, x_N\rangle \otimes \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle$ or $\mathbb{Q}\mathcal{F}_N \otimes \mathbb{Q}\mathcal{F}_N$ with $N \geqslant 2$, or $\mathbb{Q}\mathbb{Z}_M^{*N} \otimes \mathbb{Q}\mathbb{Z}_M^{*N}$ with $N \geqslant 3, M \geqslant 2$ or $N \geqslant 2, M \geqslant 3$. As with Corollary 7.5.2, Corollary 7.6.2 also applies to other algebras such as the algebra of contractions and the algebra of self-adjoint contractions, as well as free products of any of the algebras mentioned.

For the proof of Theorem 7.6.1, we use the same setup as in the previous section: we suppose $\mathcal{S} \in \mathbb{N}$ is an RE set, and let $\mathcal{X}, \widetilde{P}_n, \widetilde{X}_n$, $n \geqslant 0$, and $\mathcal{A}_{\mathcal{S}}(m) = \mathbb{C}^*\langle \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} : \mathcal{R}_m\rangle$, $m \in \mathbb{N}$, be as in Theorem 7.4.1. In addition, let $\iota : \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} \to \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} \otimes \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} : a \mapsto a \otimes \mathbb{1}$ be the left inclusion.

Proposition 7.6.3. *There are positive integers Γ, k such that if $m \notin \mathcal{S}$, φ is an $(\epsilon, \mathcal{X})$-synchronous state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} \otimes \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$, and $\tau := \varphi \circ \iota$ is an $(\epsilon, \mathcal{R}_m)$-state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ for some $\epsilon \geqslant 0$, then $\|\widetilde{P}_0\|_\tau \leqslant \Gamma m^k \sqrt{\epsilon}$.*

Proof. Suppose $m \notin \mathcal{S}$, $\epsilon \geqslant 0$, and φ is an $(\epsilon, \mathcal{X})$-synchronous state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} \otimes \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ such that $\tau := \varphi \circ \iota$ is an $(\epsilon, \mathcal{R}_m)$-state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$. By Theorem 7.4.1, part (a), $\widetilde{P}_n$ is a contraction in $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$, $\widetilde{X}_n$ is a monomial in $\mathbb{C}^*\langle\mathcal{X}\rangle$ of degree $4n+1$, and $\widetilde{X}_n$ is a unitary involution in $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$, so Lemma 7.3.7 implies

$$\left| \|\widetilde{X}_n \widetilde{P}_n \widetilde{X}_n\|_\tau - \|\widetilde{P}_n\|_\tau \right| = \left| \|\widetilde{X}_n \widetilde{P}_n \widetilde{X}_n \otimes \mathbb{1}\|_\varphi - \|\widetilde{P}_n \otimes \mathbb{1}\|_\varphi \right| \leqslant (4n+1)\sqrt{\epsilon}$$

for all $n \geqslant 0$. Hence

$$\begin{aligned}\Big|\|\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\|_\tau^2 - \|\widetilde{P}_n\|_\tau^2\Big| &= \big(\|\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\|_\tau + \|\widetilde{P}_n\|_\tau\big)\Big|\|\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\|_\tau - \|\widetilde{P}_n\|_\tau\Big| \\ &\leqslant \big(2\|\widetilde{P}_n\|_\tau + (4n+1)\sqrt{\epsilon}\big)(4n+1)\sqrt{\epsilon},\end{aligned}$$

so

$$\|\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\|_\tau^2 \geqslant \|\widetilde{P}_n\|_\tau^2 - (8n+2)\|\widetilde{P}_n\|_\tau\sqrt{\epsilon} - (4n+1)^2\epsilon \tag{7.6.1}$$

for all $n \geqslant 0$. By Theorem 7.4.1, part (a) again, $\widetilde{P}_n$ is a hermitian square in $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ with $\|\widetilde{P}_n\|_1 = 1$ and $\|\widetilde{P}_n\|_{1,1} = 3(n+1)/2 \leqslant 2n+2$ for every $n \geqslant 0$, so $\|\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\|_{1,1} \leqslant \|\widetilde{P}_n\|_{1,1} + \|\widetilde{P}_n\|_1(8n+2) \leqslant 10n+4$. Lemma 7.3.8 implies

$$\begin{aligned}\varphi\big(\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\widetilde{P}_n \otimes \mathbb{1} + \widetilde{P}_n\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n \otimes \mathbb{1}\big) &= 2\Re\Big(\varphi\big(\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\widetilde{P}_n \otimes \mathbb{1}\big)\Big) \\ &\geqslant -2\|\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\|_{1,1}\|\widetilde{P}_n \otimes \mathbb{1}\|_\varphi\sqrt{\epsilon} \\ &\geqslant -(20n+8)\|\widetilde{P}_n\|_\tau\sqrt{\epsilon}.\end{aligned}$$

By Equation (7.6.1), we obtain

$$\begin{aligned}\|\widetilde{P}_n + \widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\|_\tau^2 &= \|\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\|_\tau^2 + \|\widetilde{P}_n\|_\tau^2 + \varphi(\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\widetilde{P}_n \otimes \mathbb{1} + \widetilde{P}_n\widetilde{X}_n\widetilde{P}_n\widetilde{X}_n \otimes \mathbb{1}) \\ &\geqslant 2\|\widetilde{P}_n\|_\tau^2 - (28n+10)\|\widetilde{P}_n\|_\tau\sqrt{\epsilon} - (4n+1)^2\epsilon \\ &\geqslant 2\big(\|\widetilde{P}_n\|_\tau - (7n+7)\sqrt{\epsilon}\big)^2 - (11n+11)^2\epsilon,\end{aligned}$$

where the coefficients here (and below) are chosen for convenience. It follows that

$$2\big(\|\widetilde{P}_n\|_\tau - (7n+7)\sqrt{\epsilon}\big)^2 \leqslant \big(\|\widetilde{P}_n + \widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\|_\tau + (11n+11)\sqrt{\epsilon}\big)^2,$$

and hence

$$\|\widetilde{P}_n\|_\tau \leqslant \frac{1}{\sqrt{2}}\big(\|\widetilde{P}_n + \widetilde{X}_n\widetilde{P}_n\widetilde{X}_n\|_\tau + (25n+25)\sqrt{\epsilon}\big).$$

Let C and k be the constants from Theorem 7.4.1, part (b). By Lemma 7.3.9, $\|\widetilde{P}_n + \widetilde{X}_n\widetilde{P}_n\widetilde{X}_n - \widetilde{P}_{n+1}\|_\tau \leqslant C((n+1)m)^k\sqrt{\epsilon}$ for all $n \geqslant 0$. Thus

$$\|\widetilde{P}_n\|_\tau \leqslant \tfrac{1}{\sqrt{2}}\big(\|\widetilde{P}_{n+1}\|_\tau + C((n+1)m)^k\sqrt{\epsilon} + (25n+25)\sqrt{\epsilon}\big)$$

$$\leqslant \tfrac{1}{\sqrt{2}}\|\widetilde{P}_{n+1}\|_\tau + \tfrac{1}{\sqrt{2}}(C+25)((n+1)m)^k\sqrt{\epsilon}.$$

By induction, we obtain

$$\|\widetilde{P}_0\|_\tau \leqslant (\tfrac{1}{\sqrt{2}})^t\|\widetilde{P}_t\|_\tau + (C+25)\sum_{n=1}^{t}\frac{n^k}{2^{n/2}}m^k\sqrt{\epsilon}$$

for all $t \geqslant 1$. Since $\widetilde{P}_t$ is a contraction, $\|\widetilde{P}_t\|_\tau \leqslant 1$ for all $t \geqslant 1$. As in the proof of Theorem 7.1.3, the series $\sum_{n=1}^{\infty}\frac{n^k}{2^{n/2}}$ converges, so taking $t \to +\infty$, we conclude that

$$\|\widetilde{P}_0\|_\tau \leqslant \Gamma m^k\sqrt{\epsilon}$$

for any integer $\Gamma \geqslant (C+25)\sum_{n=1}^{\infty}\frac{n^k}{2^{n/2}}$. □

Proposition 7.6.4. *Let $\mathcal{W}$ be the mapping from Lemma 7.3.11. For every $m \in \mathbb{N}$, let $\mathcal{W}_m = \big(\bigcup_{r\in\mathcal{R}_m\cup\mathcal{R}_m^*}\mathcal{W}(r)\big)\cup\mathcal{W}(\widetilde{P}_0)\cup\mathcal{R}_m$ be as in Proposition 7.5.4, and let*

$$\widetilde{\mathcal{W}}_m := \{s\otimes\mathbb{1} : s\in\mathcal{W}_m\}\cup\{s\otimes\mathbb{1}, \mathbb{1}\otimes s : s\in\bigcup_{x\in\mathcal{X}}\mathcal{W}(x)\}.$$

There are positive integers $\widetilde{\Gamma}, k'$ such that if $m\notin\mathcal{S}$, φ is an $(\epsilon,\widetilde{\mathcal{W}}_m)$-state on $\mathbb{C}^*\langle\mathcal{X}\rangle\otimes\mathbb{C}^*\langle\mathcal{X}\rangle$, and φ is $(\epsilon,\mathcal{X})$-synchronous, then $\|\widetilde{P}_0\otimes\mathbb{1}\|_\varphi \leqslant \widetilde{\Gamma}m^{k'}\sqrt{\epsilon}$.

Proof. Let Γ, k be integers from Proposition 7.6.3, and let D be the integer from Theorem 7.4.1, part (d). Suppose $m\notin\mathcal{S}$, $\epsilon\geqslant 0$, and that φ is an $(\epsilon,\widetilde{\mathcal{W}}_m)$-state on $\mathbb{C}^*\langle\mathcal{X}\rangle\otimes\mathbb{C}^*\langle\mathcal{X}\rangle$ which is $(\epsilon,\mathcal{X})$-synchronous. Since $\varphi(s^*s\otimes\mathbb{1})\leqslant\epsilon$ and $\varphi(\mathbb{1}\otimes s^*s)\leqslant\epsilon$ for all $s\in\bigcup_{x\in\mathcal{X}}\mathcal{W}(x)$, and $\{s\otimes\mathbb{1} : s\in\bigcup_{r\in\mathcal{R}_m\cup\mathcal{R}_m^*}\mathcal{W}(r)\}\subseteq\widetilde{\mathcal{W}}_m$, by Lemma 7.3.12, there is a $(25\epsilon,\mathcal{X})$-synchronous state $\widehat{\varphi}$ on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}\otimes\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ such that

$$\big|\|r\otimes\mathbb{1}\|_{\widehat{\varphi}} - \|r\otimes\mathbb{1}\|_\varphi\big| \leqslant 2\|r\|_{1,1}\sqrt{\epsilon} \leqslant 2Dm\sqrt{\epsilon}$$

for all $r\in\mathcal{R}_m\cup\mathcal{R}_m^*$. Since $\{r\otimes\mathbb{1} : r\in\mathcal{R}_m\}\subseteq\widetilde{\mathcal{W}}_m$, for every $r\in\mathcal{R}_m\cup\mathcal{R}_m^*$, $\|r\otimes 1\|_\varphi\leqslant\sqrt{\epsilon}$, and hence $\|r\otimes\mathbb{1}\|_{\widehat{\varphi}}\leqslant(2Dm+1)\sqrt{\epsilon}$. Rounding $2Dm+1$ up to $2Dm+3$ so that $(2Dm+3)^2\geqslant 25$, we conclude that $\widehat{\varphi}$ is a $((2Dm+3)^2\epsilon,\mathcal{X})$-synchronous state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}\otimes\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ and $\widehat{\varphi}\circ\iota$ is a $((2Dm+3)^2\epsilon,\mathcal{R}_m)$-state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$. By Proposition 7.6.3,

$\|\widetilde{P}_0 \otimes \mathbb{1}\|_{\hat{\varphi}} \leqslant \Gamma m^k \sqrt{(2Dm+3)^2\epsilon} = (2Dm+3)\Gamma m^k \sqrt{\epsilon}$. Again by Lemma 7.3.12, since $\{s \otimes 1 : s \in \mathcal{W}(\widetilde{P}_0)\} \subseteq \widetilde{\mathcal{W}}_m$, we have

$$\left| \|\widetilde{P}_0 \otimes \mathbb{1}\|_{\hat{\varphi}} - \|\widetilde{P}_0 \otimes \mathbb{1}\|_{\varphi} \right| \leqslant 2\|\widetilde{P}_0\|_{1,1}\sqrt{\epsilon} \leqslant 3\sqrt{\epsilon}.$$

It follows that

$$\|\widetilde{P}_0 \otimes \mathbb{1}\|_{\varphi} \leqslant \left((2Dm+3)\Gamma m^k + 3\right)\sqrt{\epsilon} \leqslant 8D\Gamma m^{k+1}\sqrt{\epsilon}.$$

Taking $\widetilde{\Gamma} = 8D\Gamma$ and $k' = k+1$ completes the proof. □

Before proceeding to the proof of Theorem 7.6.1, we need a few more lemmas. The first is a standard fact about extending tracial states to (not necessarily tracial) states on tensor products.

Lemma 7.6.5. *If τ is a tracial state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$, then there is a $(0, \mathcal{X})$-synchronous state φ on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} \otimes \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ with $\varphi \circ \iota = \tau$.*

Proof. Let (π, v) be the GNS representation of τ, and let $\mathcal{C} = \overline{\pi(\mathcal{A})}$ be the closure of $\pi(\mathcal{A})$ in the operator norm, where $\mathcal{A} = \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$. By [BO08, Proposition 6.1.2], the tracial state defined by v on $\mathcal{C}$ extends to a state $\varphi' : \mathcal{C} \otimes \mathcal{C}^{op} \to \mathbb{C} : a \otimes b \mapsto \langle v, abv \rangle$. Note that the isomorphism $\omega_{\mathcal{X}} : \mathbb{C}^*\langle \mathcal{X} \rangle \to \mathbb{C}^*\langle \mathcal{X} \rangle^{op}$ defined in Section 7.3 descends to an isomorphism $\mathcal{A} \to \mathcal{A}^{op}$, and that π defines a $*$-homomorphism $\pi^{op} : \mathcal{A}^{op} \to \mathcal{C}^{op}$. Let $\varphi = \varphi' \circ (\pi \otimes (\pi^{op} \circ \omega_{\mathcal{X}}))$. Then φ is a state on $\mathcal{A} \otimes \mathcal{A}$ with $\varphi(a \otimes b) = \langle v, \pi(a\omega_{\mathcal{X}}(b))v \rangle = \tau(a \cdot \omega_{\mathcal{X}}(b))$. Since

$$\|x \otimes 1 - 1 \otimes x\|_{\varphi}^2 = \varphi(x^*x \otimes 1 - x \otimes x^* - x^* \otimes x + 1 \otimes x^*x) = \tau(x^2 - x^2 - x^2 + x^2) = 0$$

for all $x \in \mathcal{X}$, φ is $(0, \mathcal{X})$-synchronous. □

The remaining two lemmas are used to get from $\mathbb{Q}\mathcal{F}_N$ and $\mathbb{Q}\mathbb{Z}_2^{*N}$ for large N down to $\mathbb{Q}\mathbb{Z}_3^{*2}$ and $\mathbb{Q}\mathbb{Z}_2^{*3}$.

Lemma 7.6.6. *If H be a subgroup of a group G, then any state on $\mathbb{C}H$ extends to a state on $\mathbb{C}G$.*

One way to prove this lemma is to observe that $\mathbb{C}H$ and $\mathbb{C}G$ are subalgebras of the full group C^*-algebras $C^*(H)$ and $C^*(G)$. By definition of the full group C^*-algebra, any state on $\mathbb{C}H$ is the restriction of a state on $C^*(H)$, and since $C^*(H)$ is a subalgebra of $C^*(G)$, any state on $C^*(H)$ extends to a state on $C^*(G)$. There is also a $*$-algebra proof which we expect is known to experts, but have been unable to find in the literature, so we include a proof for reference.

Proof of Lemma 7.6.6. Let $\mathbb{C}H_+$ and $\mathbb{C}G_+$ be the convex cones of sums of squares in $\mathbb{C}H$ and $\mathbb{C}G$ respectively. We will show that $\mathbb{C}G_+ \cap \mathbb{C}H = \mathbb{C}H_+$. Indeed, let $r : \mathbb{C}G \to \mathbb{C}H$ be the linear function with $r(g) = g$ if $g \in H$ and $r(g) = 0$ if $g \notin H$. Pick a set of representatives $X \subset G$ for the coset space G/H. Any element α of $\mathbb{C}G$ can be written as $\sum_{x \in X} x\alpha_x$, where $\alpha_x \in \mathbb{C}H$, and α_x is zero for all but finitely many elements $x \in X$. If $h, h' \in H$ and $x, y \in X$, then $h^{-1}x^{-1}yh' \in H$ if and only if $x = y$, so

$$r(\alpha^*\alpha) = \sum_{x,y} r(\alpha_x^* x^{-1} y \alpha_y) = \sum_x \alpha_x^* \alpha_x$$

is a sum of squares in $\mathbb{C}H$. Consequently, if $a \in \mathbb{C}H$ and there are $\alpha_1, \ldots, \alpha_k \in \mathbb{C}G$ such that $a = \sum_i \alpha_i^* \alpha_i$, then $a = r(a) = \sum_i r(\alpha_i^* \alpha_i)$ is a sum of squares in $\mathbb{C}H$, so $\mathbb{C}G_+ \cap \mathbb{C}H = \mathbb{C}H_+$ as desired.

If f is a state on $\mathbb{C}H$, then f is nonnegative on $\mathbb{C}H \cap \mathbb{C}G_+ = \mathbb{C}H_+$. Since $\mathbb{C}G$ is archimedean, the M. Riesz extension theorem implies that f extends to a real linear functional on $\mathrm{span}_{\mathbb{R}} \mathbb{C}G_+$ which is nonnegative on $\mathbb{C}G_+$. From there, we can extend further to get a linear functional $\widetilde{f}$ on $\mathbb{C}G$ such that $\widetilde{f}(a^*) = \overline{\widetilde{f}(a)}$ for all $a \in \mathbb{C}G$, $\widetilde{f}|_{\mathbb{C}H} = f$, and $\widetilde{f}$ is nonnegative on $\mathbb{C}G_+$. Since $\widetilde{f}(1) = f(1) = 1$, the archimedean condition implies that $\widetilde{f}$ is a state. □

Lemma 7.6.7. *Suppose $N \geqslant 1$ and G is either $\mathcal{F}_K$ or $\mathbb{Z}_3^{*K}$ with $K \geqslant 2$, or $\mathbb{Z}_2^{*K}$ with $K \geqslant 3$. Then there is an injective group homomorphism $\mu : \mathcal{F}_N \to G$ and a computable*

$*$-*homomorphism* $\widetilde{\mu} : \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle \to \mathbb{Q}^*\langle x_1, \ldots, x_K\rangle$ *such that the diagram*

$$\begin{array}{ccc} \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle & \xrightarrow{\widetilde{\mu}} & \mathbb{Q}^*\langle x_1, \ldots, x_K\rangle \\ \Big\downarrow{\scriptstyle q_1} & & \Big\downarrow{\scriptstyle q_2} \\ \mathbb{Q}\mathcal{F}_N & \xrightarrow[\mu]{} & \mathbb{Q}G \end{array}$$

commutes, where q_1 *and* q_2 *are the quotient homomorphisms sending* x_j *to the* j*th generator of* $\mathcal{F}_N$ *and* G *respectively.*

Proof. Let $x_1, \ldots, x_N$ denote the generators of $\mathcal{F}_N$, y_1, y_2 denote the generators of $\mathcal{F}_2$, w_1, w_2 denote the generators of $\mathbb{Z}_3^{*2}$, and z_1, z_2, z_3 denote the generators of $\mathbb{Z}_2^{*3}$. It is well-known that the homomorphisms

$$\begin{aligned} &\gamma_1 : \mathcal{F}_N \to \mathcal{F}_2 : x_i \mapsto y_1^i y_2 y_1^{-i}, 1 \leqslant i \leqslant N, \\ &\gamma_2 : \mathcal{F}_2 \to \mathbb{Z}_3^{*2} : y_1 \mapsto w_1 w_2^{-1}, y_2 \mapsto w_1^{-1} w_2, \text{ and} \\ &\gamma_3 : \mathcal{F}_2 \to \mathbb{Z}_2^{*3} : y_i \mapsto z_1^{1-i} z_2 z_3 z_1^{1-i}, i = 1, 2 \end{aligned}$$

are injective. If $G = \mathcal{F}_K$ with $K \geqslant 2$, then we can take $\mu = \gamma_1$, where we think of $\mathcal{F}_2$ as a subgroup of $\mathcal{F}_K$ by mapping y_1 and y_2 to the first two generators, and let $\widetilde{\mu}$ be the lift of μ sending $x_i \mapsto x_1^i x_2 (x_1^*)^i$. If $G = \mathbb{Z}_3^{*K}$ with $K \geqslant 2$, we can take $\mu = \gamma_2 \circ \gamma_1$, where again we think of $\mathbb{Z}_3^{*2}$ as a subgroup of $\mathbb{Z}_3^{*K}$ by mapping w_1 and w_2 to the first two generators, and let $\widetilde{\mu}$ be the lift of μ sending $x_i \mapsto (w_1 w_2^*)^i w_1^* w_2 (w_2 w_1^*)^i$. Finally if $G = \mathbb{Z}_2^{*K}$ with $K \geqslant 3$, we can take $\mu = \gamma_3 \circ \gamma_1$, where we think of $\mathbb{Z}_2^{*3}$ as a subgroup of $\mathbb{Z}_2^{*K}$, and let $\widetilde{\mu}$ be the lift of μ sending $x_i \mapsto (x_2 x_3)^i (x_1 x_2 x_3 x_1)(x_3^* x_2^*)^i$. In all three cases, we see from the explicit formula that $\widetilde{\mu}$ is computable. □

Proof of Theorem 7.6.1. Set $\mathcal{P}_N := \mathbb{Q}^*\langle x_1, \ldots, x_N\rangle$ for $N \in \mathbb{N}$. Let $P_1(N)$ be the promise problem from the statement of the theorem with $\mathcal{P} = \mathcal{P}_N$ and $\mathcal{C} = \mathbb{Q}\mathbb{Z}_2^{*N}$, and let $P_2(N)$ be the promise problem with $\mathcal{P} = \mathcal{P}_N$ and $\mathcal{C} = \mathbb{Q}\mathbb{Z}_3^{*N}$. Although it isn't mentioned in the theorem statement, let $P_3(N)$ be the promise problem with $\mathcal{P} = \mathcal{P}_N$ and $\mathcal{C} = \mathbb{Q}\mathcal{F}_N$. As in

the proof of Theorem 7.5.1, let $n_0 = |\mathcal{X}|$. We start by showing that $P_1(N)$ is coRE-hard for all $N \geqslant n_0$.

For this, suppose $N \geqslant n_0$, and once again pick an ordering on $\mathcal{X}$ and identify $\mathbb{Q}^*\langle\mathcal{X}\rangle$, $\mathbb{C}^*\langle\mathcal{X}\rangle$, and $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ with subalgebras of $\mathcal{P}_N$, $\mathbb{C}^*\langle x_1, \ldots, x_N\rangle$, and $\mathbb{C}\mathbb{Z}_2^{*N}$ respectively. Let $\pi : \mathcal{P}_N \to \mathbb{Q}\mathbb{Z}_2^{*N}$ be the quotient map, and let $q = q_2 \circ q_1$, where $q_1 : \mathbb{Q}\mathbb{Z}_2^{*N} \to \mathbb{Q}\mathbb{Z}_2^{*\mathcal{X}}$ is the homomorphism sending $x_i \mapsto x_i$ for $1 \leqslant i \leqslant n_0$, and $q_2 : \mathbb{Q}\mathbb{Z}_2^{*\mathcal{X}} \to \mathcal{A}_{\mathcal{S}}(m)$ is the quotient map. Let $\widetilde{\Gamma}, k'$, and $\widetilde{W}_m$ be as in Proposition 7.6.4. For every $m \in \mathbb{N}$, define a $*$-polynomial

$$\beta(m) = \sum_{r \in \widetilde{\mathcal{W}}_m \cup \widetilde{\mathcal{W}}_m^*} r^* r + \sum_{x \in \mathcal{X}} (x \otimes \mathbb{1} - \mathbb{1} \otimes x)^* (x \otimes \mathbb{1} - \mathbb{1} \otimes x) - \tfrac{1}{\widetilde{\Gamma}^2 m^{2k'}} \widetilde{P}_0^* \widetilde{P}_0 \otimes \mathbb{1}$$

in $\mathbb{Q}^*\langle\mathcal{X}\rangle \otimes_{\mathbb{Q}} \mathbb{Q}^*\langle\mathcal{X}\rangle \subseteq \mathcal{P}_N \otimes_{\mathbb{Q}} \mathcal{P}_N$. Then $\beta(m)$ is self-adjoint and the map $\beta : \mathbb{N} \to \mathcal{P}_N \otimes_{\mathbb{Q}} \mathcal{P}_N$ is computable by Lemma 7.3.11, Theorem 7.4.1, and Proposition 7.6.4.

By Lemma 7.3.11, $(\pi \otimes \pi)(t \otimes \mathbb{1}) = (\pi \otimes \pi)(s \otimes \mathbb{1}) = (\pi \otimes \pi)(\mathbb{1} \otimes s) = 0$ for all $t \in \left(\bigcup_{r \in \mathcal{R}_m \cup \mathcal{R}_m^*} \mathcal{W}(r)\right) \cup \mathcal{W}(\widetilde{P}_0)$ and $s \in \bigcup_{x \in \mathcal{X}} \mathcal{W}(x)$. Hence

$$(\pi \otimes \pi)(\beta(m)) = \sum_{r \in \mathcal{R}_m \cup \mathcal{R}_m^*} r^* r \otimes \mathbb{1} + \sum_{x \in \mathcal{X}} (x \otimes \mathbb{1} - \mathbb{1} \otimes x)^2 - \tfrac{1}{\widetilde{\Gamma}^2 m^{2k'}} \widetilde{P}_0^2 \otimes \mathbb{1}$$

in $\mathbb{Q}\mathbb{Z}_2^{*\mathcal{X}} \otimes_{\mathbb{Q}} \mathbb{Q}\mathbb{Z}_2^{*\mathcal{X}} \subseteq \mathbb{Q}\mathbb{Z}_2^{*N} \otimes_{\mathbb{Q}} \mathbb{Q}\mathbb{Z}_2^{*N}$. If $m \in \mathcal{S}$, then by Theorem 7.4.1, part (c), there is a tracial state τ on $\mathcal{A}_{\mathcal{S}}(m)$ such that $\tau(\widetilde{P}_0^2) > 0$. Since $\tau \circ q_2$ is a tracial state on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ and $q_2(r) = 0$ for all $r \in \mathcal{R}_m$, Lemma 7.6.5 implies that there is a $(0, \mathcal{X})$-synchronous state φ on $\mathbb{C}\mathbb{Z}_2^{*\mathcal{X}} \otimes \mathbb{C}\mathbb{Z}_2^{*\mathcal{X}}$ such that $\varphi(\widetilde{P}_0^2 \otimes \mathbb{1}) = \tau(\widetilde{P}_0^2) > 0$ and $\varphi(r^* r \otimes \mathbb{1}) = \tau(q_2(r^* r)) = 0$ for all $r \in \mathcal{R}_m \cup \mathcal{R}_m^*$. Then $\widetilde{\varphi} := \varphi \circ (q_1 \otimes q_1)$ is a state on $\mathbb{C}\mathbb{Z}_2^{*N} \otimes \mathbb{C}\mathbb{Z}_2^{*N}$ such that $\widetilde{\varphi}\left((\pi \otimes \pi)(\beta(m))\right) = -\frac{1}{\widetilde{\Gamma}^2 m^{2k'}} \tau(\widetilde{P}_0^2) < 0$. We conclude that $(\pi \otimes \pi)(\beta(m))$ is not positive.

Now suppose $m \notin \mathcal{S}$. Let φ be a state on $(\mathcal{P}_N)_{\mathbb{C}} \otimes_{\mathbb{C}} (\mathcal{P}_N)_{\mathbb{C}}$, and let

$$\epsilon := \varphi\left(\sum_{r \in \widetilde{\mathcal{W}}_m \cup \widetilde{\mathcal{W}}_m^*} r^* r + \sum_{x \in \mathcal{X}} (x \otimes \mathbb{1} - \mathbb{1} \otimes x)^* (x \otimes \mathbb{1} - \mathbb{1} \otimes x)\right).$$

The restriction of φ to $\mathbb{C}^*\langle\mathcal{X}\rangle \otimes \mathbb{C}^*\langle\mathcal{X}\rangle$ is an $(\epsilon, \widetilde{\mathcal{W}}_m)$-state which is $(\epsilon, \mathcal{X})$-synchronous, so by Proposition 7.6.4, $\varphi(\widetilde{P}_0^* \widetilde{P}_0 \otimes \mathbb{1}) = \|\widetilde{P}_0 \otimes \mathbb{1}\|_\varphi^2 \leqslant \widetilde{\Gamma}^2 m^{2k'} \epsilon$. Hence $\varphi(\beta(m)) \geqslant 0$. We

conclude that the complement $\overline{\mathcal{S}}$ of $\mathcal{S}$ reduces to $P_1(N)$. Taking $\mathcal{S}$ to be RE-hard implies that $P_1(N)$ is coRE-hard for $N \geqslant n_0$.

Next, the quotient map $\pi^{(N)} : \mathcal{P}_N \to \mathbb{Q}\mathbb{Z}_2^{*N}$ factors as $\pi^{(N)} = \pi_2^{(N)} \circ \pi_1^{(N)}$, where $\pi_1^{(N)}$ is the quotient map $\mathcal{P}_N \to \mathbb{Q}\mathcal{F}_N$, and $\pi_2^{(N)}$ is the quotient map $\mathbb{Q}\mathcal{F}_N \to \mathbb{Q}\mathbb{Z}_2^{*N}$. If $(\pi \otimes \pi)(\alpha)$ is not positive in $\mathbb{C}\mathbb{Z}_2^{*N} \otimes \mathbb{C}\mathbb{Z}_2^{*N}$ for $\alpha \in \mathcal{P}_N \otimes \mathcal{P}_N$, then $(\pi_1^{(N)} \otimes \pi_1^{(N)})(\alpha)$ is not positive in $\mathbb{C}\mathcal{F}_N \otimes \mathbb{C}\mathcal{F}_N$. Thus $P_1(N)$ reduces to $P_3(N)$, and $P_3(N)$ is coRE-hard for $N \geqslant n_0$.

By Lemma 7.6.7, if $N \geqslant 1$ and $K \geqslant 2$ then there is an injective homomorphism $\mu : \mathcal{F}_N \to \mathbb{Z}_3^{*K}$ and a computable homomorphism $\widetilde{\mu} : \mathcal{P}_N \to \mathcal{P}_K$ such that $\pi_3^{(K)} \circ \widetilde{\mu} = \mu \circ \pi_1^{(N)}$, where $\pi_3^{(K)}$ is the quotient map $\mathcal{P}_K \to \mathbb{Q}\mathbb{Z}_3^{*K}$. If $\alpha \in \mathcal{P}_N \otimes \mathcal{P}_N$ is positive in $(\mathcal{P}_N)_{\mathbb{C}} \otimes (\mathcal{P}_N)_{\mathbb{C}}$, then $(\widetilde{\mu} \otimes \widetilde{\mu})(\alpha)$ is positive in $(\mathcal{P}_K)_{\mathbb{C}} \otimes (\mathcal{P}_K)_{\mathbb{C}}$. If $(\pi_1^{(N)} \otimes \pi_1^{(N)})(\alpha)$ is not positive in $\mathbb{C}\mathcal{F}_N \otimes \mathbb{C}\mathcal{F}_N$, then there is a state f on $\mathbb{C}\mathcal{F}_N \times \mathcal{F}_N$ such that $f(\pi_1^{(N)} \otimes \pi_1^{(N)})(\alpha)) < 0$. If we identify $\mathbb{C}\mathcal{F}_N \otimes \mathbb{C}\mathcal{F}_N$ with $\mathbb{C}\mathcal{F}_N \times \mathcal{F}_N$ and $\mathbb{C}\mathbb{Z}_3^{*K} \otimes \mathbb{C}\mathbb{Z}_3^{*K}$ with $\mathbb{C}\mathbb{Z}_3^{*K} \times \mathbb{Z}_3^{*K}$, then the homomorphism $\mu \otimes \mu$ is the algebra homomorphism coming from the injective group homomorphism $\mu \times \mu : \mathcal{F}_N \times \mathcal{F}_N \to \mathbb{Z}_3^{*K} \times \mathbb{Z}_3^{*K}$. By Lemma 7.6.6, the state f extends to a state $\widetilde{f}$ on $\mathbb{C}\mathbb{Z}_3^{*K} \times \mathbb{Z}_3^{*K}$, and

$$\widetilde{f}((\mu \times \mu)(\pi_1^{(N)} \otimes \pi_1^{(N)})(\alpha)) = f((\pi_1^{(N)} \otimes \pi_1^{(N)})(\alpha)) < 0.$$

Hence $(\pi_3^{(K)} \otimes \pi_3^{(K)})(\widetilde{\mu} \otimes \widetilde{\mu})(\alpha) = (\mu \otimes \mu)(\pi_1^{(N)} \otimes \pi_1^{(N)})(\alpha)$ is not positive. Since $\widetilde{\mu} \otimes \widetilde{\mu}$ is computable, $P_3(N)$ reduces to $P_2(K)$ for any $N \geqslant 1$ and $K \geqslant 2$. It follows that $P_2(K)$ is coRE-hard for all $K \geqslant 2$. Similarly, $P_3(N)$ reduces to $P_1(K)$ for all $N \geqslant 1$ and $K \geqslant 3$, so $P_1(K)$ is coRE-hard for all $K \geqslant 3$. □

The following example shows that Theorem 7.6.1 is not true for $\mathcal{C} = \mathbb{Z}_2^{*2}$.

Example 7.6.8. *Let $G = \mathbb{Z}_2^{*2}$ be the infinite dihedral group. This group is amenable and linear. Hence the product group $G \times G$ is also amenable and linear. By a theorem of Bekka, $\mathbb{C}G \times G$ is residually finite-dimensional [Bek99], in the sense that an element $\alpha \in \mathbb{C}G \otimes \mathbb{C}G = \mathbb{C}G \times G$ is positive if and only if $\phi(\alpha)$ is positive for all finite-dimensional representations ϕ. Every finite-dimensional representation of $\mathbb{C}G \times G$ decomposes into irreducible representations, so α is positive if and only if $\phi(\alpha)$ is positive for all irreducible*

finite-dimensional representations. The irreducible representations of G have dimension 1 and 2, so the irreducible representations of $G \times G$ have dimension 1, 2, and 4. Thus $\alpha \in \mathbb{C}G \times G$ is positive if and only if $\phi(\alpha)$ is positive for all representations of dimension 4. The question of whether $\phi(\alpha)$ is not positive for all representations of dimension 4 lies in the existential theory of the reals, and thus can be solved in PSPACE *[Can88]. In particular, the question of whether $\alpha \in \mathbb{C}G \times G$ is positive is decidable. We do not know whether $\mathbb{C}G \times G$ is archimedean closed.*

References

[ABOEM17] Dorit Aharonov, Michael Ben-Or, Elad Eban, and Urmila Mahadev. Interactive proofs for quantum computations. *arXiV:1704.04487*, 2017.

[ACGK19] Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu, and Elham Kashefi. Complexity-theoretic limitations on blind delegated quantum computation. In *International Colloquium on Automata, Languages and Programming*, pages 6:1–6:13, 2019.

[AMP12] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Physical Review Letters*, 108:100402, 2012.

[ANT19] Vadim Alekseev, Tim Netzer, and Andreas Berthold Thom. Quadratic modules, C^*-algebras, and free convexity. *Transactions of the American Mathematical Society*, 372(11):7525–7539, 2019.

[Art27] Emil Artin. Über die zerlegung definiter funktionen in quadrate. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5:100–115, 1927.

[Arv77] William Arveson. Notes on extensions of C^*-algebras. *Duke Mathematical Journal*, 44(2):329 – 355, 1977.

[BCK+23] Pedro Baptista, Ranyiliu Chen, Jed Kaniewski, David R. Lolck, Laura Mančinska, Thor Gabelgaard Nielsen, and Simon Schmidt. A mathematical

foundation for self-testing: Lifting common assumptions. *arXiv:2310.12662*, 2023.

[BDKS14] Sabine Burgdorf, Ken Dykema, Igor Klep, and Markus Schweighofer. Addendum to "Connes' embedding conjecture and sums of hermitian squares" [Adv. Math. 217 (4) (2008) 1816–1837]. *Advances in Mathematics*, 252:805–811, 2014.

[Bei21] Salman Beigi. Separation of quantum, spatial quantum, and approximate quantum correlations. *Quantum*, 5:389, 2021.

[Bek99] Bachir Bekka. On the full C^*-algebras of arithmetic groups and the congruence subgroup problem. *Forum Mathematicum*, 11(6):705–715, 1999.

[Bel64] John S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, 1964.

[BG22] Anne Broadbent and Alex B. Grilo. QMA-hardness of consistency of local density matrices with applications to quantum zero-knowledge. *SIAM Journal of Computing*, 51(4):1400–1450, 2022.

[BGG$^+$90] Michael Ben-Or, Oded Goldreich, Shafi Goldwasser, Johan Håstad, Joe Kilian, Silvio Micali, and Phillip Rogaway. Everything provable is provable in zero-knowledge. In *Annual International Cryptology Conference*, 1990.

[BGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Widgerson. Multi-prover interactive proofs: how to remove intractability assumptions. In *Symposium on the Theory of Computing (STOC)*, 1988.

[BGS13] Anne Broadbent, Gus Gutoski, and Douglas Stebila. Quantum one-time programs. In *CRYPTO 2013*, volume 2, pages 344–360, 2013.

[BJSW16] Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous. Zero-knowledge proof systems for QMA. In *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 31–40, 2016.

[BJSW20] Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous. Zero-knowledge proof systems for QMA. *SIAM Journal of Computing*, 49(2):245–283, 2020.

[Bla06] Bruce Blackadar. *Operator algebras: theory of C^*-algebras and von Neumann algebras*, volume 122. Springer Science & Business Media, 2006.

[BMZ23] Anne Broadbent, Arthur Mehta, and Yuming Zhao. Quantum delegation with an off-the-shelf device. *arXiv:2304.03448*, 2023.

[BO08] Nathanial P. Brown and Narutaka Ozawa. *C^*-Algebras and Finite-Dimensional Approximations*, volume 88. Graduate Studies in Mathematics, 2008.

[BORS02] Jean-Camille Birget, Alexander Yu. Olshankii, Eliyahu Rips, and Mark V. Sapir. Isoperimetric functions of groups and computational complexity of the word problem. *Annals of Mathematics*, 156(2):467–518, 2002.

[BP15] Cédric Bamps and Stefano Pironio. Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing. *Physical Review A*, 91:052111, 2015.

[Bro18] Anne Broadbent. How to verify a quantum computation. *Theory of Computing*, 14(1):1–37, 2018.

[BŠCA18a] Joseph Bowles, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín. Device-independent entanglement certification of all entangled states. *Physical review letters*, 121(18):180503, 2018.

[BŠCA18b] Joseph Bowles, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín. Self-testing of Pauli observables for device-independent entanglement certification. *Physical Review A*, 98(4):042336, 2018.

[BT07] Mihály Bakonyi and Dan Timotin. Extensions of positive definite functions on free groups. *Journal of Functional Analysis*, 246(1):31–49, 2007.

[Bur11] Sabine Burgdorf. *Trace-positive polynomials, sums of hermitian squares and the tracial moment problem*. Phd thesis, Universität Konstanz, Feburary 2011. Available at https://www.math.uni-konstanz.de/~burgdorf/PhD.pdf.

[Can88] John Canny. Some algebraic and geometric computations in pspace. *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC)*, 1988.

[CE76] Man-Duen Choi and Edward G. Effros. The completely positive lifting problem for C^*-algebras. *Annals of Mathematics*, 104(3):585–609, 1976.

[CFGS18] Alessandro Chiesa, Michael Forbes, Tom Gur, and Nicholas Spooner. Spatial isolation implies zero knowledge even in a quantum world. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 755–765, 2018.

[CGJV19] Andrea Coladangelo, Alex B Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: New schemes for verifiable delegated quantum computation, with quasilinear resources. In *EUROCRYPT 2019*, volume 3, pages 247–277, 2019.

[CGS17] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. *Nature communications*, 8(1):1–5, 2017.

[CHLM22] Matthias Christandl, Nicholas Gauguin Houghton-Larsen, and Laura Mančinska. An operational environment for quantum self-testing. *Quantum*, 6:699, 2022.

[Cho80] Man-Duen Choi. The full C^*-algebra of the free group on two generators. *Pacific Journal of Mathematics*, 87(1):41–48, 1980.

[CHSH69] John F. Clauser, Michael A. Horne., Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[CHTW10] Richard Cleve, Peter Hoyer, Ben Toner, and John Watrous. Consequences and limits of nonlocal strategies. *arXiv preprint quant-ph/0404076v2*, 2010.

[Cim09] Jakob Cimprič. A representation theorem for archimedean quadratic modules on $*$-rings. *Canadian Mathematical Bulletin*, 52(1):39–52, 2009.

[CL17] André Chailloux and Anthony Leverrier. Relativistic (or 2-prover 1-round) zero-knowledge protocol for NP secure against quantum adversaries. In *Proceedings of Eurocrypt*, volume 3, pages 369–396, 2017.

[CLP17] Richard Cleve, Li Liu, and Vern I. Paulsen. Perfect embezzlement of entanglement. *Journal of Mathematical Physics*, 58(1), 2017.

[CM14] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. In *International Colloquium on Automata, Languages, and Programming*, pages 320–331. Springer, 2014.

[CMMN20] David Cui, Arthur Mehta, Hamoon Mousavi, and Seyed Sajjad Nezhadi. A generalization of CHSH and the algebraic structure of optimal strategies. *Quantum*, 4:346, 2020.

[Col17] Andrea Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. *Quantum Information & Computation*, 17(9-10):831–865, 2017.

[Col20] Andrea Coladangelo. A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations. *Quantum*, 4:282, 2020.

[CRSV18] Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. *Quantum*, 2:92, 2018.

[CS18] Andrea Coladangelo and Jalex Stark. Unconditional separation of finite and infinite-dimensional quantum correlations. *arXiv:1804.05116*, 2018.

[CS23] Claude Crépeau and John Stuart. Zero-knowledge MIPs using homomorphic commitment schemes. *arXiv:2304.09784*, 2023.

[CVZ19] Andrea Coladangelo, Thomas Vidick, and Tina Zhang. Non-interactive zero-knowledge arguments for QMA, with preprocessing. *arXiv:1911.07546*, 2019.

[Dix82] Jacques Dixmier. *C^*-algebras*. North-Holland, 1982.

[DM14] Artem Dudko and Konstantin Medynets. Finite factor representations of Higman–Thompson groups. *Groups, Geometry, and Dynamics*, 8(2):375–389, 2014.

[EL92] Ruy Exel and Terry A. Loring. Finite-dimensional representations of free product C^*-algebras. *International Journal of Mathematics*, 03:469–476, 1992.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[FK17] Joseph F. Fitzsimons and Elham Kashefi. Unconditionally verifiable blind quantum computation. *Physical Review A*, 96(1):012303, 2017.

[Fre22] Alexander Frei. The quantum commuting model (Ia): The CHSH game and other examples: Uniqueness of optimal states. *arXiv:2210.03716*, 2022.

[Fri12] Tobias Fritz. Tsirelson's problem and Kirchberg's conjecture. *Reviews in Mathematical Physics*, 24(05):1250012, 2012.

[Ger93] Stephen M. Gersten. Isoperimetric and isodiametric functions of finite presentations. In *Geometric group theory: Proceedings of the Symposium held in Sussex 1991, Volume 1*, volume 181 of *London Mathematical Society Lecture Note Series 181*, pages 79–97. Cambridge University Press, 1993.

[GH17] William T. Gowers and O. Hatami. Inverse and stability theorems for approximate representations of finite groups. *Sbornik: Mathematics*, 208(12):1784–1817, 2017.

[GM90] Ken R. Goodearl and Pere Menal. Free and residually finite-dimensional C^*-algebras. *Journal of Functional Analysis*, 90:391–410, 1990.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(3):690–728, 1991.

[Gri19] Alex B. Grilo. A simple protocol for verifiable delegation of quantum computation in one round. In *International Colloquium on Automata, Languages and Programming*, 2019.

[GSY19] Alex B. Grilo, William Slofstra, and Henry Yuen. Perfect zero knowledge for quantum multiprover interactive proofs. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 611–635, 2019.

[Had01] Don Hadwin. A noncommutative moment problem. *Proceedings of the American Mathematical Society*, 129(6):1785–1791, 2001.

[Hel02] J. William Helton. "Positive" noncommutative polynomials are sums of squares. *Annals of Mathematics*, 156(2):675–694, 2002.

[HKM12] J. William Helton, Igor Klep, and Scott McCullough. The convex positivstellensatz in a free algebra. *Advances in Mathematics*, 231(1):516–534, 2012.

[HM04] J. William Helton and Scott A. McCullough. A positivstellensatz for noncommutative polynomials. *Transactions of the American Mathematical Society*, 356(9):3721–3737, 2004.

[HMP04] J. William Helton, Scott A. McCullough, and Mihai Putinar. A non-commutative positivstellensatz on isometries. *Journal für die reine und angewandte Mathematik*, 2004(568):71–80, 2004.

[HMPS19] J. William Helton, Kyle P. Meyer, V. I. Paulsen, and Matthew Satriano. Algebras, synchronous games, and chromatic numbers of graphs. *New York Journal of Mathematics*, 25:328–361, 2019.

[Ji16] Zhengfeng Ji. Classical verification of quantum proofs. In *Proceedings of the 48th annual ACM symposium on Theory of Computing*, pages 885–898, 2016.

[Ji17] Zhengfeng Ji. Compression of quantum multi-prover interactive proofs. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 289–302, 2017.

[JJUW11] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. $\mathsf{QIP} = \mathsf{PSPACE}$. *Journal of the ACM*, 58(6):30, 2011.

[JNP+11] Marius Junge, Migue Navascues, Carlos Palazuelos, David Perez-Garcia, Volkher B. Scholz, and Reinhard F. Werner. Connes' embedding problem and Tsirelson's problem. *Journal of Mathematical Physics*, 52(1):012102, Jan 2011.

[JNV+20] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*=RE. *arXiv:2001.04383*, 2020.

[JP11] Kate Juschenko and Stanislav Popovych. Algebraic reformulation of Connes embedding problem and the free group algebra. *Israel Journal of Mathematics*, 181:305–315, 2011.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the 20th annual ACM symposium on Theory of computing*, pages 20–31, 1988.

[Kir93] Eberhard Kirchberg. On non-semisplit extensions, tensor products and exactness of group C^*-algebras. *Inventiones mathematicae*, 112:449–489, 1993.

[KM03] Hirotada Kobayashi and Keiji Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3):429–450, 2003.

[KMV22] Igor Klep, Victor Magron, and Jurij Volčič. Optimization over trace polynomials. *Annales Henri Poincaré*, 23:67–100, 2022.

[KPS18] Se-Jin Kim, Vern Paulsen, and Christopher Schafhauser. A synchronous game for binary constraint systems. *Journal of Mathematical Physics*, 59(3):032201, 2018.

[KR97] Richard V. Kadison and John R. Ringrose. *Fundamentals of the theory of operator algebras*. American Mathematical Society, 1997.

[Kri64] Jean-Louis Krivine. Anneaux préordonnés. *Journal d'Analyse Mathématique*, 12:307–326, 1964.

[KS08a] Igor Klep and Markus Schweighofer. Connes' embedding conjecture and sums of hermitian squares. *Advances in Mathematics*, 217(4):1816–1837, 2008.

[KS08b] Igor Klep and Markus Schweighofer. Sums of hermitian squares and the BMV conjecture. *Journal of Statistical Physics*, 133:739–760, 2008.

[KSV02] Alexei Yu. Kitaev, Alexander Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.

[KSV23] Igor Klep, Claus Scheiderer, and Jurij Volčič. Globally trace-positive noncommutative polynomials and the unbounded tracial moment problem. *Mathematische Annalen*, 387:1403–1433, 2023.

[Lor97] Terry A Loring. *Lifting solutions to perturbing problems in C*-algebras*, volume 8. American Mathematical Society, 1997.

[LPR20] Henri Lombardi, Daniel Perrucci, and Marie-Françoise Roy. An elementary recursive bound for effective positivstellensatz and Hilbert's 17th problem. *Memoirs of the American Mathematical Society*, 263, 2020.

[Mah18] Urmila Mahadev. Classical verification of quantum computations. *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 259–267, 2018.

[McC01] Scott McCullough. Factorization of operator-valued polynomials in several non-commuting variables. *Linear Algebra and its Applications*, 326(1):193–203, 2001.

[McK17] Matthew McKague. Self-testing in parallel with CHSH. *Quantum*, 1:1, 2017.

[Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(27):3373–3376, 1990.

[MNP21] Laura Mančinska, Thor Gabelgaard Nielsen, and Jitendra Prakash. Glued magic games self-test maximally entangled states. *arXiv:2105.10658*, 2021.

[MNY22] Hamoon Mousavi, Seyed Sajjad Nezhadi, and Henry Yuen. Nonlocal games, compression theorems, and the arithmetical hierarchy. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 1–11, 2022.

[MP05] Scott McCullough and Mihai Putinar. Noncommutative sums of squares. *Pacific Journal of Mathematics*, 218(1):167–171, 2005.

[MPS21] Laura Mančinska, Jitendra Prakash, and Christopher Schafhauser. Constant-sized robust self-tests for states and measurements of unbounded dimension. *arXiv:2103.01729*, 2021.

[MR19] Magdalena Musat and Mikael Rørdam. Factorizable maps and traces on the universal free product of matrix algebras. *International Mathematics Research Notices*, 2021(23):17951–17970, 2019.

[MS23] Laura Mančinska and Simon Schmidt. Counterexamples in self-testing. *Quantum*, 7:1051, 2023.

[MSZ23] Arthur Mehta, William Slofstra, and Yuming Zhao. Positivity is undecidable in tensor product of free algebras. *arXiv:2312.05617*, 2023.

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

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

[NC00] Michael A. Nielsen and Issac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

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

[NT13] Tim Netzer and Andreas Thom. Real closed separation theorems and applications to group algebras. *Pacific Journal of Mathematics*, 263(2), 2013.

[NTZ+24] Shlok Nahar, Devashish Tupkary, Yuming Zhao, Norbert Lütkenhaus, and Ernest Y.-Z. Tan. Postselection technique for optical Quantum Key Distribution with improved de Finetti reductions. *arXiv:2403.11851*, 2024.

[NV17] Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 1003–1015, 2017.

[NV18] Anand Natarajan and Thomas Vidick. Low-degree testing for quantum states, and a quantum entangled games PCP for QMA. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 731–742, 2018.

[NZ23] Anand Natarajan and Tina Zhang. Quantum free games. *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC)*, 2023.

[Oza04] Natutaka Ozawa. About the QWEP conjecture. *International Journal of Mathematics*, 15(05):501–530, 2004.

[Oza13] Narutaka Ozawa. About the Connes embedding conjecture - algebraic approaches. *Japanese Journal of Mathematics*, 8:147–183, 2013.

[Pad24] Connor Paddock. Rounding near-optimal quantum strategies for nonlocal games to strategies using maximally entangled states. *arXiv:2203.02525*, 2024.

[Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3):107–108, 1990.

[PSS+16] Vern I. Paulsen, Simone Severini, Daniel Stahlke, Ivan G. Todorov, and Andreas Winter. Estimating quantum chromatic numbers. *Journal of Functional Analysis*, 270(6):2188–2222, Mar 2016.

[PSZZ23] Connor Paddock, William Slofstra, Yuming Zhao, and Yangchen Zhou. An operator-algebraic formulation of self-testing. *Annales Henri Poincaré*, 2023.

[Put93] Mihai Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana University Mathematics Journal*, 42:969–984, 1993.

[Qua15] Ronan Quarez. Trace-positive non-commutative polynomials. *Proceedings of the American Mathematical Society*, 143(8):3357–3370, 2015.

[Rot73] Joseph J. Rotman. *The theory of groups*. Allyn and Bacon, Inc, 2 edition, 1973.

[RUV12] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. *arXiv:1209.0448*, Sep 2012.

[RUV13] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496:456–460, 2013.

[RY22] Gregory Rosenthal and Henry S. Yuen. Interactive proofs for synthesizing quantum states and unitaries. In *13th Innovations in Theoretical Computer Science Conference (ITCS)*, 2022.

[ŠB20] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, 2020.

[SBR02] Mark V. Sapir, Jean-Camille Birget, and Eliyahu Rips. Isoperimetric and isodiametric functions of groups. *Annals of Mathematics*, 156(2):345–466, 2002.

[Sch91] Konrad Schmüdgen. The K-moment problem for compact semi-algebraic sets. *Mathematische Annalen*, 289:203–206, 1991.

[Sch00] Claus Scheiderer. Sums of squares of regular functions on real algebraic varieties. *Transactions of the American Mathematical Society*, 352:1039–1069, 2000.

[Sch03] Claus Scheiderer. Sums of squares on real algebraic curves. *Mathematische Zeitschrift*, 245:725–760, 2003.

[Sch06] Claus Scheiderer. Sums of squares on real algebraic surfaces. *manuscripta math*, 119:395–410, 2006.

[Sch09] Konrad Schmüdgen. *Noncommutative Real Algebraic Geometry - Some Basic Concepts and First Ideas*. Springer New York, 2009.

[Sch20] Konrad Schmüdgen. *An Invitation to Unbounded Representations of $*$-Algebras on Hilbert Space*. Springer Cham, 2020.

[Sip12] Michael Sipser. *Introduction to the Theory of Computation*. Cengage Learning, 2012.

[Slo11] William Slofstra. Lower bounds on the entanglement needed to play XOR non-local games. *Journal of Mathematical Physics*, 52(10):102202, 2011.

[Slo19] William Slofstra. The set of quantum correlations is not closed. *Forum of Mathematics, Pi*, 7:e1, 2019.

[Slo20] William Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. *Journal of the American Mathematical Society*, 33:1–56, 2020.

[Ste74] Gilbert Stengle. A nullstellensatz and a positivstellensatz in semialgebraic geometry. *Mathematische Annalen*, 207:87–97, 1974.

[SVW16] Jamie Sikora, Antonios Varvitsiotis, and Zhaohui Wei. Minimum dimension of a Hilbert space needed to generate a quantum correlation. *Physical Review Letters*, 117(6):060401, 2016.

[SW08] Volkher B. Scholz and Reinhard F. Werner. Tsirelson's problem. *arXiv:0812.4305*, 2008.

[Tsi87] Boris S. Tsirelson. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36(4):557–570, 1987.

[Tsi93] Boris S. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8:329–345, 1993.

[Vid18] Thomas Vidick. An expository note on "a quantum linearity test for robustly verifying entanglement", 2018. Available at http://users.cms.caltech.edu/~vidick/notes/pauli_braiding_1.pdf.

[VZ20] Thomas Vidick and Tina Zhang. Classical zero-knowledge arguments for quantum computations. *Quantum*, 4:266, 2020.

[Wat00] John Watrous. Succinct quantum proofs for properties of finite groups. *Proceedings 41st Annual Symposium on Foundations of Computer Science (STOC)*, pages 537–546, 2000.

[Wat03] John Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.

[Wat09] John Watrous. Quantum computational complexity. In *Encyclopedia of complexity and systems science*, pages 7174–7201. Springer, 2009.

[WBMS16] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93:062121, 2016.

[Yue16] Henry Yuen. *Games, protocols, and quantum entanglement*. PhD thesis, Massachusetts Institute of Technology, 2016. Available at https://dspace.mit.edu/handle/1721.1/107364.

[Zha] Yuming Zhao. Robust self-testing for nonlocal games with stable game algebras. In preparation.

APPENDICES

Appendix A

The closure of finite-dimensional states

In this appendix, we prove Proposition 4.1.10:

Proposition 4.1.10. *For every state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ there is a sequence of quantum models $S_n, n \in \mathbb{N}$ such that $\lim_{n\to\infty} f_{S_n} = f$ in the weak*-topology.*

We first show that any tensor product state on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ can be approximated by a sequence of finite-dimensional states.

Lemma A.0.1. *For every tensor product model*

$$S = \left(\mathcal{H}_A, \mathcal{H}_B, \{M_a^x : a \in A, x \in X\}, \{N_b^y : b \in B, y \in Y\}, |\psi\rangle\right)$$

there is a sequence of finite-dimensional states $\{f_n\}_{n\in\mathbb{N}}$ on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ such that $\lim_{n\to\infty} f_n = f_S$ in the weak-topology.*

Proof. If $\mathcal{H}_A$ or $\mathcal{H}_B$ is finite-dimensional, then f_S is a finite-dimensional state and the lemma follows by taking $f_n = f_S$ for all $n \in \mathbb{N}$. Now suppose $\mathcal{H}_A$ and $\mathcal{H}_B$ are separable infinite-dimensional Hilbert spaces. The state $|\psi\rangle$ has decomposition

$$|\psi\rangle = \sum_{i=1}^{\infty} \lambda_i |\xi_i\rangle \otimes |\eta_i\rangle$$

where $\{\lambda_i\}_{i\in\mathbb{N}}$ is a non-negative sequence in $\ell^2(\mathbb{N})$ with $\sum_{i\in\mathbb{N}}\lambda_i^2 = 1$, and $\{|\xi_i\rangle : i \in \mathbb{N}\}$ and $\{|\eta_i\rangle : i \in \mathbb{N}\}$ are orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. For every $n \in \mathbb{N}$ we define projections $\Pi_n^A := \sum_{i=1}^n |\xi_i\rangle\langle\xi_i| \in \mathcal{B}(\mathcal{H}_A)$ and $\Pi_n^B := \sum_{i=1}^n |\eta_i\rangle\langle\eta_i| \in \mathcal{B}(\mathcal{H}_B)$, finite-dimensional spaces $\mathcal{H}_n^A := \Pi_n^A\mathcal{H}_A$ and $\mathcal{H}_n^B := \Pi_n^B\mathcal{H}_B$, and vector state $|\psi_n\rangle := \frac{1}{\mu_n}\sum_{i=1}^n \lambda_i |\xi_i\rangle \otimes |\eta_i\rangle \in \mathcal{H}_n^A \otimes \mathcal{H}_n^B$ where $\mu_n := \sqrt{\sum_{i=1}^n \lambda_i^2}$. Then for every $n \in \mathbb{N}$,

$$S_n := (\mathcal{H}_n^A, \mathcal{H}_n^B, \{\Pi_n^A M_a^x \Pi_n^A\}, \{\Pi_n^B N_b^y \Pi_n^B\}, |\psi_n\rangle)$$

is a quantum model. Let $\pi_A \otimes \pi_B$ be the associate representation of S, and let $\pi_n^A \otimes \pi_n^B$ be the associate representation of S_n for every $n \in \mathbb{N}$.

Claim A.0.2. *Given $\epsilon \geqslant 0$, for every monomial α in $\mathcal{A}_{POVM}^{X,A}$, there exists a $T_A \in \mathbb{N}$ such that*

$$\pi_n^A(\alpha) \otimes \mathbb{1} |\psi_n\rangle \approx_\epsilon \pi_A(\alpha) \otimes \mathbb{1} |\psi\rangle \tag{A.0.1}$$

for all $n \geqslant T_A$.

Proof of Claim A.0.2. We prove this claim by induction on the degree k of the monomial α. Since $\mu_n \to 1$ as $n \to \infty$, there is a $T \in \mathbb{N}$ such that $1 - \mu_n \leqslant \epsilon/2$ and $\sqrt{1-\mu_n^2} \leqslant \epsilon/2$ for all $n \geqslant T$. So

$$\||\psi_n\rangle - |\psi\rangle\| \leqslant \|(1-\mu_n)|\psi_n\rangle\| + \|\mu_n|\psi_n\rangle - |\psi\rangle\| \leqslant 1 - \mu_n + \sqrt{1-\mu_n^2} \leqslant \epsilon$$

for all $n \geqslant T$. Equation (A.0.1) holds for $k = 0$. Now assume it holds for all monomials of degree k for some $k \geqslant 0$. Let $\alpha = \alpha_1 \cdots \alpha_{k+1}$ be a monomial of degree $k+1$, and let $\alpha' := \alpha_2 \cdots \alpha_{k+1}$. By the induction hypothesis, there exists a $T_1 \in \mathbb{N}$ such that

$$\pi_n^A(\alpha') \otimes \mathbb{1} |\psi_n\rangle \approx_{\epsilon/2} \pi_A(\alpha') \otimes \mathbb{1} |\psi\rangle$$

for all $n \geqslant T_1$. For every $i, j \in \mathbb{N}$, let $s_{ij} := \langle \xi_i, \eta_j | \pi_A(\alpha) \otimes \mathbb{1} |\psi\rangle$. Since $\sum_{i,j\geqslant 1}|s_{ij}|^2 = \|\pi_A(\alpha) \otimes \mathbb{1} |\psi\rangle\|^2 \leqslant 1$, there is a $T_2 \in \mathbb{N}$ such that

$$\sum_{i,j=1}^n |s_{ij}|^2 \geqslant \sum_{i,j\geqslant 1} |s_{ij}|^2 - (\epsilon/2)^2$$

for all $n \geqslant T_2$. Note that $\|\pi_A(\alpha_1)\|_{op} \leqslant 1$. It follows that

$$\begin{aligned}\pi_A(\alpha) \otimes \mathbb{1} |\psi\rangle &\approx_{\epsilon/2} \Pi_n^A \otimes \Pi_n^B \big(\pi_A(\alpha) \otimes \mathbb{1} |\psi\rangle\big) = \Pi_n^A \pi_A(\alpha_1) \otimes \Pi_n^B \big(\pi_A(\alpha') \otimes \mathbb{1} |\psi\rangle\big) \\ &\approx_{\epsilon/2} \Pi_n^A \pi_A(\alpha_1) \otimes \Pi_n^B \big(\pi_n^A(\alpha') \otimes \mathbb{1} |\psi_n\rangle\big) = \Pi_n^A \pi_A(\alpha_1) \Pi_n^A \pi_n^A(\alpha') \otimes \mathbb{1} |\psi_n\rangle \\ &= \pi_n^A(\alpha_1)\pi_n^A(\alpha') \otimes \mathbb{1} |\psi_n\rangle = \pi_n^A(\alpha) \otimes \mathbb{1} |\psi_n\rangle\end{aligned}$$

for all $n \geqslant T := \max\{T_1, T_2\}$. So Equation (A.0.1) holds for all monomials of degree $k+1$. This completes the proof. □

Similarly, for any $\epsilon \geqslant 0$ and monomial $\beta \in \mathcal{A}_{POVM}^{Y,B}$, there exists a $T_B \in \mathbb{N}$ such that

$$\mathbb{1} \otimes \pi_n^B(\beta^*) |\psi_n\rangle \approx_\epsilon \mathbb{1} \otimes \pi_B(\beta^*) |\psi\rangle . \tag{A.0.2}$$

for all $n \geqslant T_B$. Then by Lemma 4.1.12, $\lim_{n\to\infty} f_{S_n}(\alpha \otimes \beta) = f(\alpha \otimes \beta)$ for all monomials α and β. So the lemma follows. □

The above lemma illustrates that the weak*-closure of the set of finite-dimensional states contains all tensor product states. To prove the set of finite-dimensional states is weak*-dense, we only need to show that the set of tensor product states is weak*-dense. Recall the following well-known fact (see e.g. [KR97, Corollary 4.3.10]).

Lemma A.0.3. *Suppose $\mathcal{A} \subseteq \mathcal{B}(\mathcal{H})$ is a concretely represented unital C^*-algebra, and let f be a state on $\mathcal{A}$. Then for every $\epsilon > 0$ and every finite set of elements $\alpha_1, \cdots, \alpha_n \in \mathcal{A}$, there are coefficients $\lambda_1, \cdots, \lambda_k \geqslant 0$ with $\sum_{i=1}^k \lambda_i = 1$ and vectors $|\psi_1\rangle, \cdots, |\psi_k\rangle \in \mathcal{H}$ such that*

$$|f(\alpha_i) - \sum_{j=1}^k \lambda_j \langle\psi_j| \alpha_i |\psi_j\rangle| \leqslant \epsilon$$

for all $1 \leqslant i \leqslant n$.

This lemma can be used to prove:

Lemma A.0.4. *For every state f on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ there is a sequence of tensor product models $\{S_n\}_{n\in N}$ such that $\lim_{n\to\infty} f_{S_n} = f$ in the weak*-topology.*

Proof. We first fix any faithful representations $\mathcal{A}_{POVM}^{X,A} \subseteq \mathcal{B}(\mathcal{H}_A)$ and $\mathcal{A}_{POVM}^{Y,B} \subseteq \mathcal{B}(\mathcal{H}_B)$ for some Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. Then $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ is the C^*-algebra generated by the concrete operators $m_a^x \otimes n_b^y$, $(a,b,x,y) \in A \times B \times X \times Y$, where each $m_a^x \otimes n_b^y$ acts on $\mathcal{H}_A \otimes \mathcal{H}_B$. For every $n \in \mathbb{N}$, let

$$C(n) := \{\alpha \otimes \beta : \alpha \text{ monomial in } \mathcal{A}_{POVM}^{X,A}, \beta \text{ monomial in } \mathcal{A}_{POVM}^{Y,B}, \deg(\alpha) + \deg(\beta) \leqslant n\}$$

be the set of monomials in $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ of degree $\leqslant n$. Then $C(n)$ is a finite set and $C(n) \subset C(n+1)$ for all $n \in \mathbb{N}$. For every $n \in \mathbb{N}$, by Lemma A.0.3 there are coefficients $\lambda_1^{(n)}, \cdots, \lambda_{k_n}^{(n)} \geqslant 0$ with $\sum_{i=1}^{k_n} \lambda_i^{(n)} = 1$ and vectors $|\psi_1^{(n)}\rangle, \cdots, |\psi_{k_n}^{(n)}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ such that

$$|f(\alpha \otimes \beta) - \sum_{i=1}^{k_n} \lambda_i^{(n)} \langle \psi_i^{(n)}| \alpha \otimes \beta |\psi_i^{(n)}\rangle| \leqslant \frac{1}{n} \text{ for all } \alpha \otimes \beta \in C(n). \tag{A.0.3}$$

Then $S_n := \left(\mathcal{H}_A, \mathcal{H}_B, \{m_a^x\}, \{n_b^y\}, \rho_n\right)$ is a tensor product model with a mixed state $\rho_n := \sum_{i=1}^{k_n} \lambda_i |\psi_i\rangle\langle\psi_i|$. Equation (A.0.3) implies

$$|f(\alpha \otimes \beta) - f_{S_n}(\alpha \otimes \beta)| \leqslant \frac{1}{n} \text{ for all } \alpha \otimes \beta \in C(n).$$

Then for every $\epsilon > 0$ and every monomial $\alpha \otimes \beta \in \mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$,

$$|f(\alpha \otimes \beta) - f_{S_n}(\alpha \otimes \beta)| \leqslant \epsilon$$

for all $n \geqslant \max\{\lceil \frac{1}{\epsilon} \rceil, \deg(\alpha) + \deg(\beta)\}$. So $\lim_{n\to\infty} f_{S_n}(\alpha \otimes \beta) = f(\alpha \otimes \beta)$ for any monomial $\alpha \otimes \beta$. The lemma follows. □

Proof of Proposition 4.1.10. Let f be a state on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$. By Lemma A.0.4 there is a sequence of tensor product models $\{S_n\}_{n\in\mathbb{N}}$ such that $f = \lim_{n\to\infty} f_{S_n}$ in the weak*-topology. Then for every $n \in \mathbb{N}$, by Lemma A.0.1 there is a sequence of finite-dimensional states $\{f_m^{(n)}\}_{m\in\mathbb{N}}$ such that $f_{S_n} = \lim_{m\to\infty} f_m^{(n)}$ in the weak*-topology. Hence $\{f_n^{(n)}\}_{n\in\mathbb{N}}$ is a sequence of finite-dimensional states such that $f = \lim_{n\to\infty} f_n^{(n)}$ in the weak*-topology. We conclude that the set of finite-dimensional states on $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$ is a weak*-dense subset of the state space of $\mathcal{A}_{POVM}^{X,A} \otimes_{\min} \mathcal{A}_{POVM}^{Y,B}$. □