ABSTRACT

Title of Dissertation: THE MEMBERSHIP PROBLEM FOR CONSTANT-SIZED QUANTUM CORRELATIONS IS UNDECIDABLE

Hong Hao Fu
Doctor of Philosophy, 2021

Dissertation Directed by: Dr. Carl A. Miller
Department of Computer Science

One of the most fundamental and counterintuitive features of quantum mechanics is entanglement, which is central to many demonstrations of the quantum advantage. Studying quantum correlations generated by local measurements on an entangled physical system is one of the direct ways to gain insights into entanglement. The focus of this dissertation is to get better understanding of the hardness of determining if a given correlation is quantum, which is also known as the membership problem of quantum correlations.

Previous work has shown that the general membership problem is computationally undecidable. Where does the hardness come from? Is it just because the size of a quantum correlation (i.e., the number of real values in the description of the correlation) can be arbitrarily large? We would like to understand the role played by the varying sizes of correlations in the hardness of the membership problem.

It has been shown that certain quantum correlations require the measured

quantum system to be maximally entangled with a certain dimension. This is a unique phenomenon of quantum correlations and it is known as self-testing. The first step towards answering the hardness of the membership problem of quantum correlations is to get deeper understandings about self-testing, and more specifically, about the size of a correlation that can self-test a maximally entangled state of arbitrarily large dimension. If correlations of a fixed size can self-test entangled states of unbounded dimension, this phenomenon is a strong evidence suggesting that deciding membership of fixed-sized correlations can be very hard.

We first show that there exists an infinite subset of the set of all the prime numbers such that, for each prime p in this set, a maximally entangled state of local dimension $(p-1)$ can be self-tested by a correlation of a fixed size. Since this set is infinite, this result implies that constant-sized correlations are sufficient to self-test maximally entangled states of unbounded dimension.

Building on the self-testing result, we show that the varying sizes of correlations are not the only root of the hardness. Specifically, we show that the membership problem of fixed finite-sized correlations is still computationally undecidable when the fixed size is sufficiently large. That is, the hardness of the membership problem of quantum correlations is independent of the varying sizes of correlations. In fact, the hardness arises from the fact that the structure of some set of correlations of a particular size is so complicated that no finite description of this set can allow a Turing machine to decide if a correlation is quantum or not.

THE MEMBERSHIP PROBLEM FOR CONSTANT-SIZED QUANTUM CORRELATIONS IS UNDECIDABLE

by

Hong Hao Fu

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2021

Advisory Committee:
Professor Andrew M. Childs, Chair
Professor Carl A. Miller, Co-Chair/Advisor
Professor Xiaodi Wu
Professor Yi-Kai Liu
Professor Jonathan M. Rosenberg

Acknowledgments

The past five years has been a happy and fruitful journey for me. For this, I owe thanks to many people.

First and foremost, I would like to thank my advisor, Carl A. Miller for all the support and advice from him so that I can be a better scientific writer, a better presenter and a better researcher than I was five years ago. In 2018, Carl generously shared his thoughts about the membership problem of constant-sized quantum correlations with me, which is the start of a three-year project that leads to this dissertation. The success of this project is inseparable from all the enlightening discussions with Carl, his careful reviews of my drafts and this dissertation, and his many inspiring feedbacks. It has been a pleasure to work with and learn from such an extraordinary individual.

I thank the other members of my dissertation committee: Andrew M. Childs, Yi-Kai Liu, Xiaodi Wu and Jonathan M. Rosenberg for reviewing my dissertation and giving me advice about the future.

I am deeply grateful to my co-authors: Yanbao Zhang, Emanuel Knill and William Slofstra. Yanbao and Emanuel introduced me to the problems about device-independent randomness generation and expansion when I didn't have a clear research direction. I have gained not just new knowledge but also good research skills and habits. William shared with me his idea about using correlations to check the triviality of group members, which is the foundation of this dissertation. Without his pioneer work in nonlocal games and quantum correlation, my self-testing paper and this dissertation wouldn't exist. I would like to also thank him for patiently walking me through all the abstract algebra problems that I encounter during the project, and for his wonderful advice about writing.

I would like to thank Henry Yuen for hosting me in December 2019 and Penghui Yao for hosting me in January 2020. During the first visit at University of Toronto, I met Arthur Mehta, Hamoon Mousavi and Seyed Sajjad Nezhadi and had hours of interesting discussions. The discussions are still vivid in my memory. Seyed later joined UMD as a PhD student, which is because my persuasion as I believe.

My fives years at QuICS wouldn't be so joyful without my fellow students and colleagues: Jianxin Chen, Penghui Yao, Aniruddha Bapat, Abhinav Deshpande, Andrew Guo, Eddie Schoute, Minh Tran, Ali Izadi Rad, Charles Cao, Qi Zhao, Atul Mantri, Yusuf Alnawakhtha, Chen Bai, Shih-Han Hung, Jiaqi Leng, Jin-Peng Liu, Yuxiang Peng, Daochen Wang, Sheng Yang, Xin Wang and especially my officemates: Tongyang Li and Yuan Su. I am very grateful to all the help I received from Tongyang, Jianxin and Penghui when I first moved to Maryland, and to the delicious Thanksgiving turkeys prepared by Sheng and Tongyang.

I would like to thank the staff members of our center and the CS department including: Arlene Schenk, Javiera Caceres, Tom Hurst and Andrea Svejda for being suprisingly prompt in replying my emails.

Finally, I owe my deepest thank to my girlfriend, Zhijiao Liu, and my parents for always supporting my decisions, making sure that I can focus on my research, and cheering me up when I was down. Their endless love is my most precious and cherished wealth.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

1.1 Bipartite quantum correlation

One of the most counterintuitive and fundamental features of quantum mechanics is *entanglement*. To study entanglement, one can make local measurements on entangled systems and examine the statistics generated by the measurements. The central motivating question of this dissertation is the following: how hard is it to characterize such statistics generated by entangled particles without prior knowledge of the entanglement?

We consider the simple case with two entangled systems. In this case, statistics generated by local measurements on a quantum system are called *bipartite quantum correlations*. They arise in the following scenario. Suppose two spatially separated parties, say Alice and Bob, are going to perform some task under the supervision of a referee. Alice and Bob get a question from a fixed set with n_A and n_B questions respectively and for each question they need to give an answer from a fixed set with m_A and m_B answers respectively. The referee makes sure that Alice and Bob do not communicate after they get their questions and before they give their answers, which is a critical condition. Since the sets of questions and answers are known to Alice and Bob beforehand, the questions and answers can be simply represented by their indices in the corresponding sets. Let $[n]$ denote the set $\{0, 1, \ldots, n-1\}$, then the question and answer sets are $[n_A]$, $[n_B]$, $[m_A]$ and $[m_B]$. Since Alice and Bob cannot communicate, we can assume Alice and Bob are spatially isolated and this scenario is illustrated in the figure below.

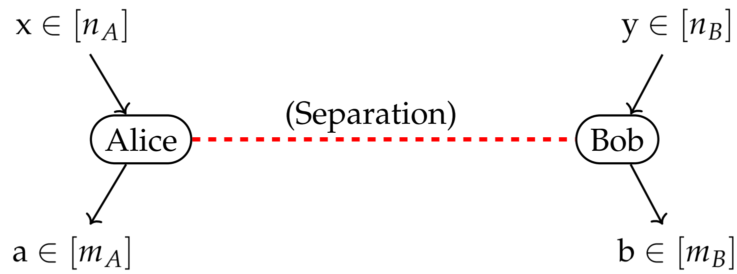

Figure 1.1: A scenario with spatially isolated Alice and Bob, where n_A, n_B, m_A, $m_B \in \mathbb{N}$.

Note that if there are a probability distribution of the questions and a scoring function on question-answer pairs, this scenario becomes a nonlocal game, which is an abstraction of a multi-prover interactive proof system (MIP) [1]. Such scenarios arise in the studies of entanglement-based quantum key distribution [2], quantum random number generation [3], and entanglement-assisted multi-prover interactive proof system (MIP*) [4]. For this dissertation, we focus on the behaviour of Alice and Bob without a nonlocal game setting.

From the point of view of the referee, Alice and Bob's behaviour is captured by the collection

$$P = \{P(a, b|x, y) : 0 \leq a < m_A,\ 0 \leq b < m_B,\ 0 \leq x < n_A,\ 0 \leq y < n_B\}$$

where $P(a, b|x, y)$ is the probability that Alice answers a and Bob answers b, when

Alice's question is x and Bob's question is y. The collection P is called a *correlation*, which can be viewed as a matrix. The columns and rows are labelled by Alice and Bob's question-answer pair (x, a) and (y, b) respectively, so that the entry in column (x, a) and row (y, b) is $P(a, b|x, y)$. Therefore, the *size* of correlation P is $n_A n_B m_A m_B$ (the size of the correlation matrix).

Such correlations are induced by strategies for Alice and Bob determined before the task. Since Alice and Bob cannot communicate during the task, their strategies must be of the following form. Each of them holds a local system of a larger system, which may be classical or quantum. Alice has n_A different measurements, one for each question, and each measurement has m_A outcomes, one for each answer. Bob has n_B different measurements, one for each question, and each measurement has m_B outcomes, one for each answer. Each of them performs their measurement corresponding to the given question on their local system and obtains their answer. We can see that their strategy can be described by their measurements and their local systems.

The first question to ask is whether it is possible to tell if they use entanglement to generate the observed correlation. This question is first answered by John Bell in 1964 [5]. Bell observed that there are correlations generated by local measurements on entangled systems that cannot be explained by local variables. Hence, such correlations are called *nonlocal correlations*. In other words, Alice and Bob cannot use shared randomness and deterministic measurements, which are measurements with a deterministic outcome, to reproduce the same correlation. Nonlocal correlation is one of the important and strong separations between classical and quantum mechanics.

Following Bell's results, when observing a certain correlation, physicists may ask whether the shared quantum system is finite-dimensional or infinite-dimensional, and mathematicians may ask whether the measurements are modelled as local operators or global but commuting operators. In fact, these questions correspond to different mathematical models or sets of quantum correlations.

In chapter 4, we formally introduce the four standard sets of quantum correlations:

- the finite-dimensional quantum correlations $C_q(n_A, n_B, m_A, m_B)$, where the measured quantum state is finite-dimensional and the measurements are local,
- the quantum spatial correlations $C_{qs}(n_A, n_B, m_A, m_B)$, where the measured quantum state can be infinite-dimensional but the measurements are local,
- the quantum approximable correlations $C_{qa}(n_A, n_B, m_A, m_B)$, which is the closure of $C_{qs}(n_A, n_B, m_A, m_B)$, and
- the quantum commuting-operator correlations $C_{qc}(n_A, n_B, m_A, m_B)$, where the measurements are global but commuting.

The convention that we follow in this dissertation is that C_t refers to $C_t(n_A, n_B, m_A, m_B)$ for $t \in \{q, qs, qa, qc\}$ when the tuple (n_A, n_B, m_A, m_B) is clear from context.

After two decades' efforts to study the four sets of quantum correlations, we know that for some n_A, n_B, m_A, m_B all four sets are different, and hence, the four sets form a strictly increasing sequence

$$C_q \subsetneq C_{qs} \subsetneq C_{qa} \subsetneq C_{qc}. \tag{1.1}$$

The separation between C_q and C_{qs} is due to Andrea Coladangelo and Jalex Stark [6]. The separation between C_{qs} and C_{qa} is due to William Slofstra [7]. The last separation between C_{qa} and C_{qc} is due to Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen [8]. It is interesting that these three separations rely on very different approaches.

About the geometries of these four sets, we know that the sets C_t, $t \in \{q, qs, qa, qc\}$, are convex subsets of $\mathbb{R}^N$ and that C_{qa} and C_{qc} are closed [9]. However, for some integers n_A, n_B, m_A and m_B, C_q and C_{qs} are not closed [7], which suggests describing these two sets is difficult.

Chapter 4 is partly based on the following paper:

[10] Honghao Fu, Carl A. Miller and William Slofstra *The membership problem for constant-sized quantum correlations is undecidable*, 2021, arXiv:2101.11087.

1.2 The membership problems of quantum correlations

Knowing the basic geometry properties of the four sets of quantum correlations is the first step towards the comprehensive understanding of quantum correlations. The next step, which is also the goal of this dissertation, is to understand the hardness of characterizing each set of quantum correlations. We study these questions from the computational complexity perspective.

Namely, we are interested in the computational hardness of the following decision problems for $t \in \{q, qs, qa, qc\}$ and subfields $\mathbb{K} \subseteq \mathbb{R}$, where $\mathbb{K}$ is countable.

Problem (Membership$_{t,\mathbb{K}}$)**.** *Given a tuple (n_A, n_B, m_A, m_B), and a correlation $P \in \mathbb{K}^{n_A n_B m_A m_B}$, is $P \in C_t(n_A, n_B, m_A, m_B)$?*

Such a problem requires a computer to know the exact entries of P. Note that if some entry of P is a real number that cannot be described using finite space, the hardness of this problem is trivialized. This is why we restrict to correlations in $\mathbb{K}^{n_A n_B m_A m_B}$ rather than $\mathbb{R}^{n_A n_B m_A m_B}$. Our choice of $\mathbb{K}$ makes sure that the correlation P can be processed by a computer in a finite amount of time. When $\mathbb{K}$ is clear from the context, we drop the subscript $\mathbb{K}$.

We choose to study the membership problems because the decidability of the membership problems is directly related to the existence of some finite-length descriptions of the sets of quantum correlations. If (Membership$_{t,\mathbb{K}}$) is decidable for some $t \in \{q, qs, qa, qc\}$, then some nice universal algorithm for C_t exists and can be used to determine the membership of correlations of any size.

As it turns out, all of the four membership problems are undecidable. The undecidability of (Membership$_{t,\mathbb{Q}}$) for $t \in \{q, qs, qa\}$ are proved in [7] and [8], where [8] in fact proves the undecidability of a stronger version of (Membership$_{t,\mathbb{Q}}$) – namely, the approximate version of (Membership$_{t,\mathbb{Q}}$). The undecidability of

($\text{Membership}_{qc,\mathbb{Q}}$) is proved by Matthew Coudron and William Slofstra [11]. These undecidability results imply that there does not exist an algorithm that can generate a finite description of $C_t(n_A, n_B, m_A, m_B)$ that allows a Turing machine to decide (Membership_t) for any $t \in \{q, qs, qa, qc\}$ and any n_A, n_B, m_A and m_B.

Now, we need to understand the cause of the hardness of the membership problems of quantum correlations. It should be noted that the families of undecidable correlations from the papers [7, 8, 11] all involve correlations with unbounded sizes. Therefore, one possible explanation for the hardness of (Membership_t) is that the parameters n_A, n_B, m_A and m_B are allowed to vary and there are infinitely many different choices of these parameters. Even if a finite description of $C_t(n_A, n_B, m_A, m_B)$ exists for all n_A, n_B, m_A and m_B, no Turing machine can store all of them, which can make (Membership_t) undecidable.

This dissertation is devoted to proving that the hardness of the membership problem is independent of the varying sizes of correlations. We would like to show that (Membership_t) is still undecidable when the parameters n_A, n_B, m_A and m_B are fixed. The problem that we study is called the membership problem for *constant-sized* quantum correlations.

Problem ($\text{Membership}(n_A, n_B, m_A, m_B)_{t,\mathbb{K}}$)**.** *Given a correlation $P \in \mathbb{K}^{n_A n_B m_A m_B}$, is $P \in C_t(n_A, n_B, m_A, m_B)$?*

The main result of this dissertation addresses the complexity of this problem, and it is summarized in the following theorem.

Theorem 1.1 (Informal version)**.** *There is an integer N such that the decision problem*

(Membership$(n_A, n_B, m_A, m_B)_{t,\mathbb{K}}$) is undecidable for $t \in \{qa, qc\}$ and $n_A, n_B, m_A, m_B > N$.

This result asserts that, provided that n_A, n_B, m_A, m_B are chosen to be sufficiently large, there is no description of the set $C_t(n_A, n_B, m_A, m_B)$ that would allow a Turing machine to decide membership in that set for $t \in \{qa, qc\}$.

The main result is a key step towards understanding the true sources of complexity of the membership problems of quantum correlations. It is the first result that shows the hardness of such problems does not rely on the varying sizes of the correlations. In fact, the main result indicates that the hardness of (Membership$_{qa}$) and (Membership$_{qc}$) is rooted in the complicated structure of a single set $C_t(n_A, n_B, m_A, m_B)$ for some n_A, n_B, m_A, m_B and $t \in \{qa, qc\}$. The structures of these sets are so complicated that no Turing machine can output a complete description in a finite amount of time.

The first step towards proving Theorem 1.1 is to deepen our knowledge of a unique phenomenon of quantum correlations called *self-testing*.

1.3 Self-testing

The idea of self-testing is first introduced by Dominic Mayers and Andrew Yao [12], and later formalized by Matthew McKague, Tzyh Haur Yang and Valerio Scarani [13]. Self-testing refers to a phenomenon of quantum correlations that certain correlations are sufficient for us to deduce that some local transformation can turn the measured state into the tensor product of a particular entangled state and some junk state. We also call such correlations self-tests.

Since the only assumption about self-testing is that Alice and Bob are spatially separated, and only classical interactions are required between the referee and the two participants, self-testing becomes a powerful tool for applications in quantum cryptography and computational complexity theory. It allows a classical party to delegate quantum computations to some untrusted service provider and verify that the computations are performed honestly and correctly [14, 15]. Self-testing also becomes a critical component of the security proofs of device-independent quantum cryptographic protocols [12, 16]. Self-tests also help to bound the computational power of MIP* protocols [8, 17, 18].

The case of self-testing of the EPR pair,

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

is fully understood. The techniques for this case are first introduced in [13], then improved in [19]. Self-testings of tensor products of maximally entangled qubits are proved in [20, 21], with the last one being the one with the smallest question and answer sets. The idea of self-testing of general bipartite entangled states with local dimension d is first proposed in [22] and realized in [23], which uses 4 questions but each question has d answers. The number of questions is later reduced to 2 in [24], but the number of answers is still d.

In chapter 5, we show that maximally entangled states of unbounded dimension can be self-tested by correlations of a fixed size. For comparison, all the correlations used in the results listed above have sizes dependent on the local dimension of the entangled state.

Theorem 1.2 (Informal version)**.** *There exists an infinite-sized set D of odd prime numbers such that, for any $p \in D$, the maximally entangled state of local dimension $(p-1)$ can be self-tested with a constant-sized quantum correlation.*

To prove Theorem 1.2, we construct a correlation of size $\Theta(r^2)$ for each odd prime number p whose smallest primitive root is r. We say that r is a primitive root of p if r is the multiplicative generator of the group $\mathbb{Z}_p^*$. This correlation is denoted by $Q_{p,r}$ and the size of $Q_{p,r}$ is independent of p, although it does depend on r.

The correlation $Q_{p,r}$ is obtained by combining two correlations: P_{A_r} and $\hat{Q}_{-\pi/p}$, which will be introduced below. The question set of $Q_{p,r}$ is the union of the question sets of P_{A_r} and $\hat{Q}_{-\pi/p}$, and this how we combine the two correlations.

The correlation P_{A_r} is a perfect correlation associated with a binary linear system, where the variables of the system are binary and the addition is taken modulo 2. To better introduce this correlation, we introduce a nonlocal game called the binary linear system game, illustrated in the figure below. In this game, Alice and Bob each gets a question, which is either a variable or an equation of the binary linear system. The distribution over the questions is uniform. They win this game under the following conditions:

- if they receive the same question, they must give the same answer;

- if their questions are equations, they must give a satisfying assignment, and their assignments to the common variables, if there are any, must be the same; and
- if one receives an equation and the other one receives a variable from that equation, then the assignment to the equation must be satisfying and the assignment to the variable must match the assignment to the equation.

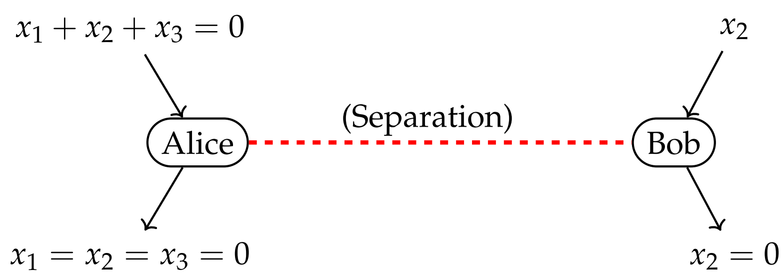

Figure 1.2: One success iteration of a binary linear system game.

A widely-used and thoroughly-studied example is the Magic square game [25] with the following linear system

$$\begin{aligned} x_1 + x_2 + x_3 &= 0 & \qquad x_4 + x_5 + x_6 &= 0 \\ x_7 + x_8 + x_9 &= 0 & \qquad x_1 + x_4 + x_7 &= 0 \\ x_2 + x_5 + x_8 &= 1 & \qquad x_3 + x_6 + x_9 &= 0. \end{aligned}$$

Using two copies of $|EPR\rangle$, the winning correlation of this game can be induced. It has been shown that if a strategy can induce the winning correlation, the shared state must be $|EPR\rangle^{\otimes 2}$ up to some local isometry [26]. Thus, the winning correlation of the Magic square game is a self-test for $|EPR\rangle^{\otimes 2}$. The key observation that leads to the self-testing proof is that, in a winning strategy of this game, if we denote Alice's binary observable for x_1 by X, and denote Alice's binary observable for x_4 by Z, then X and Z must satisfy the anti-commutation relation

$$ZXZ = -X.$$

The correlation P_{A_r} is a winning correlation of the binary linear system game associated with a linear system, which is denoted by $A_r \boldsymbol{x} = 0$. P_{A_r} can enforce the relation

$$U^{\dagger} O U = O^{r}, \tag{1.2}$$

for unitaries U and O, which correspond to products of the binary observables used by Alice and Bob, and some integer r. The inspiration comes from Slofstra's work [7], where he proposes and validates a new way to design a correlation that can enforce conjugacy relations of the form $X^{\dagger} Y X = Z$ for unitaries X, Y and Z. Following Slofstra's design, the numbers of equations and variables of $A_r \boldsymbol{x} = 0$ are of order $\Theta(r)$.

The reason that we choose eq. (1.2) to be the relation enforced by P_{A_r} is the following. Inducing P_{A_r} guarantees that the strategy contains unitaries U and O on Alice's and Bob's side satisfying eq. (1.2). Moreover, if we can certify that the unitary O has the eigenvalue $\omega_p := e^{i2\pi/p}$ where r is a primitive root of p, eq. (1.2) automatically guarantees that the spectrum of O contains $\{\omega_p^j | 1 \leq$

$j \leq p-1\}$, and that Alice and Bob's local system must be of dimension at least $(p-1)$. Therefore, the correlation $\hat{Q}_{-\pi/p}$ is introduced to certify an eigenvalue of O. We prove that in an inducing strategy of $\hat{Q}_{-\pi/p}$ there must exist a unitary that has eigenvalues $e^{i2\pi/p}$ and $e^{-i2\pi/p}$.

The first step to prove Theorem 1.2 is to prove the full correlation $Q_{p,r}$ is a self-test. Following the intuition introduced in the previous paragraph, we can prove that the correlation $Q_{p,r}$ can self-test the state $|\tilde{\psi}\rangle$ defined by

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{p-1}} \sum_{j=1}^{p-1} |j\rangle|d-j\rangle.$$

The last step of proving Theorem 1.2 involves a number theory result. It has been shown that there exists an integer $r \in \{2,3,5\}$ such that there are infinitely many primes whose primitive root is r [27]. The set D in the statement of Theorem 1.2 is the set of all such primes. By applying the self-testing result of $Q_{p,r}$ to all $p \in D$, we prove that for any $p \in D$, a maximally entangled state of dimension $(p-1)$ can be self-tested by a constant-sized correlation.

Chapter 5 is based on the following paper:

[28] Honghao Fu, *Constant-sized correlations are sufficient to robustly self-test maximally entangled states with unbounded dimension*, 2019, arXiv:1911.01494.

1.4 Overview of the undecidability proof

In chapters 6 and 7, we prove that Membership$(n_A, n_B, m_A, m_B)_{t,\mathbb{K}}$ for $t \in \{qa, qc\}$ are undecidable for sufficiently large n_A, n_B, m_A and m_B. The central idea of the undecidability proof is to reduce Membership$(n_A, n_B, m_A, m_B)_{t,\mathbb{K}}$ for $t \in \{qa, qc\}$ to the word problem of a group. The word problem of a group asks if an element of the group is trivial in the group and this problem is known to be undecidable [29, Chapter 12]. In this section, we sketch the proof of our main result.

In chapter 6, we first introduce the Minsky machine developed by Marvin Minsky [30], and the Kharlampovich-Myasnikov-Sapir group (KMS group), first introduced by Olga Kharlampovich, Alexei Myasnikov and Mark Sapir [31]. A Minsky machine is a kind of universal computation machine just like a Turing machine, which consists of a few counters and each command is either incrementing or decrementing a subset of the counters. Since a Minsky machine can simulate any Turing machine, deciding if a Minsky machine accepts an input is equivalent to the halting problem, which is undecidable. Because the forms of commands of a Minsky machine are simple, it is easier to write down a group that can simulate a Minsky machine rather than a Turing machine. A KMS group can simulate a Minsky machine, in the sense that the proof that some element of this group is trivial corresponds to a sequence of the commands of the Minsky machine that takes the input configuration of a particular input to the accept configuration. Therefore, the word problem of a KMS group is undecidable.

In Section 6.4, we extend a KMS group G and construct a family of groups $\{G_n \mid n \geq 1\}$ such that deciding if a fixed element w is trivial in G_n is equivalent to deciding if a Minsky machine accepts the input n. This approach is different from the approach taken in [7] and [11]. The previous approach uses a fixed

KMS group G, and different inputs of the Minsky machine are written in different group elements. This is why the authors of [7] and [11] need correlations of growing sizes to check if different group elements are trivial or not in G. In our approach, the input n is written in some relation of G_n so that we can write down correlations of a fixed size to check if w is trivial in G_n. This is the key step to ensure that the correlations that we construct are of the same fixed size.

In chapter 7, we prove that there exists a family of correlations $\{C_n \mid n \geq 1\}$ such that C_n is in $C_{qa}(N_A, N_B, M_A, M_B)$ if w is nontrivial in G_n, and on the other hand, C_n is not in $C_{qc}(N_A, N_B, M_A, M_B)$ if w is trivial in G_n, for some fixed N_A, N_B, M_A, M_B. Note that the numbers N_A, N_B, M_A and M_B are fixed across all the different n.

Intuitively, to induce C_n, Alice and Bob's binary observables correspond to generators of G_n, which are the same for all n. As mentioned in the previous paragraph, the input n is written in some relation of G_n. To enforce this relation, we use a correlation similar to $\hat{Q}_{-\pi/p}$, which is used in the self-testing proof, to write n into the entries of C_n and keep the size of C_n independent of n. For the other relations of G_n, we design a linear system such that a perfect correlation associated with this linear system can force Alice and Bob's binary observables to satisfy these relations. Then, the correlation C_n is a combination of the two correlations. The last step to prove Theorem 1.1 is to observe that, since $C_{qa}(N_A, N_B, M_A, M_B) \subseteq C_{qc}(N_A, N_B, M_A, M_B)$, if a correlation is in $C_{qa}(N_A, N_B, M_A, M_B)$, then it is also in $C_{qc}(N_A, N_B, M_A, M_B)$, and if a correlation is not in $C_{qc}(N_A,$

$N_B, M_A, M_B)$, then it is also not in $C_{qa}(N_A, N_B, M_A, M_B)$. Therefore,

$$C_n \in C_{qa}(N_A, N_B, M_A, M_B) \text{ if and only if } n \text{ is not a halting input}$$

$$C_n \in C_{qc}(N_A, N_B, M_A, M_B) \text{ if and only if } n \text{ is not a halting input.}$$

In other words, $\{C_n \mid n \geq 1\}$ is an undecidable family of correlations for both $C_{qa}(N_A, N_B, M_A, M_B)$ and $C_{qc}(N_A, N_B, M_A, M_B)$.

All the group theory results used in chapter 6 are introduced in chapter 3. Chapters 3, 6 and 7 are based on the following paper:

[10] Honghao Fu, Carl A. Miller and William Slofstra *The membership problem for constant-sized quantum correlations is undecidable*, 2021, arXiv:2101.11087.

We conclude this dissertation in chapter 8 by summarizing our contributions and discussing avenues for future research.

Chapter 2: Preliminaries

In this chapter, we introduce our notation and basics of quantum computing.

For a positive integer n, we use $[n]$ to denote the set $\{0, 1, \ldots, n-1\}$. $\mathbb{R}$ and $\mathbb{C}$ denote the set of real numbers and the set of complex numbers. $\mathbb{R}_{\geq 0}$ denotes the set of non-negative real numbers. We denote the n-th root of unity by $\omega_n := e^{i2\pi/n}$ for any $n \geq 1$.

We denote vectors in bold font, for example, $\boldsymbol{a}$ and $\boldsymbol{b}$. The j-th entry of the vector $\boldsymbol{a}$ is denoted by $\boldsymbol{a}(j)$. The transpose of the vector $\boldsymbol{a}$ is denoted by $\boldsymbol{a}^\intercal$ and the complex conjugate of it is denoted by $\bar{\boldsymbol{a}}$. The conjugate transpose of $\boldsymbol{a}$ is denoted by $\boldsymbol{a}^\dagger = \bar{\boldsymbol{a}}^\intercal$.

Definition 2.1. *A **Hilbert space** is a vector space $\mathcal{H}$ over $\mathbb{C}$ with an inner product $\langle \cdot, \cdot \rangle$ such that it is a complete metric space with respect to the norm defined by $\|\boldsymbol{a}\| = \sqrt{\langle \boldsymbol{a}, \boldsymbol{a} \rangle}$ for all $\boldsymbol{a} \in \mathcal{H}$, meaning that for every sequence $(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots)$, if*

$$\lim_{m \to \infty} \lim_{n \to \infty} \|\boldsymbol{a}_m - \boldsymbol{a}_n\| = 0,$$

then the sequence converges in this space.

To distinguish different Hilbert spaces, we use subscripts, for example, $\mathcal{H}_A$ and $\mathcal{H}_B$. We denote a Hilbert space over $\mathbb{C}$ of dimension d by $\mathbb{C}^d$ where the standard inner product is given by

$$\langle \boldsymbol{a}, \boldsymbol{b} \rangle = \sum_{j \in [d]} \bar{\boldsymbol{a}}(j) \boldsymbol{b}(j).$$

The standard basis of $\mathbb{C}^d$ is denoted by $\{\boldsymbol{e}_j \mid j \in [d]\}$.

The tensor product of $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$ for some $d_1, d_2 \geq 1$ is denoted by $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ and it is a $d_1 d_2$-dimensional Hilbert space spanned by $\{\boldsymbol{e}_i \otimes \boldsymbol{e}_j \mid i \in [d_1], j \in [d_2]\}$ [32, Lemma B.2]. Setting $\boldsymbol{e}_i \otimes \boldsymbol{e}_j = \boldsymbol{e}_{i \cdot d_2 + j} \in \mathbb{C}^{d_1 d_2}$ gives us an isomorphism between $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ and $\mathbb{C}^{d_1 d_2}$. Let $\boldsymbol{a} \in \mathbb{C}^{d_1}$ and $\boldsymbol{b} \in \mathbb{C}^{d_2}$ for some $d_1, d_2 \geq 1$. Then,

$$\boldsymbol{a} \otimes \boldsymbol{b} = (\boldsymbol{a}(1)\boldsymbol{b}(1), \ldots, \boldsymbol{a}(1)\boldsymbol{b}(d_2), \ldots, \boldsymbol{a}(d_1)\boldsymbol{b}(1), \ldots, \boldsymbol{a}(d_1)\boldsymbol{b}(d_2)) \in \mathbb{C}^{d_1 d_2}.$$

Definition 2.2. *A **pure quantum state** is a unit vector of some Hilbert space $\mathcal{H}$.*

If $\mathcal{H} = \mathbb{C}^d$, then the quantum state is of dimension d. We use the bra-ket notation for pure quantum states. For example, if ψ is a pure quantum state, we denote it by $|\psi\rangle$ and denote its conjugate transpose by $\langle\psi| = |\psi\rangle^\dagger$. The inner product of $|\psi\rangle$ and $|\phi\rangle$ is denoted by $\langle\psi|\phi\rangle$. For a set of of quantum states $\{|\psi_j\rangle \in \mathcal{H}_j \mid j \in [n]\}$, where $\mathcal{H}_j$ may be not equal to $\mathcal{H}_k$ if $j \neq k$, the tensor product of the quantum states in this set is denoted by $|\psi_0\rangle_{\mathcal{H}_0} \otimes |\psi_1\rangle_{\mathcal{H}_1} \otimes \ldots \otimes |\psi_{n-1}\rangle_{\mathcal{H}_{n-1}}$, which is also written as $|\psi_0\rangle_{\mathcal{H}_0}|\psi_1\rangle_{\mathcal{H}_1} \ldots |\psi_{n-1}\rangle_{\mathcal{H}_{n-1}}$, or simply, $|\psi_0\rangle \ldots |\psi_{n-1}\rangle$.

For a Hilbert space $\mathcal{H}$, any linear map $T : \mathcal{H} \to \mathcal{H}$ is referred to as a linear operator. A linear operator $T : \mathcal{H} \to \mathcal{H}$ is *bounded* if there exists a constant M such that

$$\|T\boldsymbol{a}\| \leq M\|\boldsymbol{a}\| \text{ for all } \boldsymbol{a} \in \mathcal{H}.$$

The set of such bounded linear operators on $\mathcal{H}$ is denoted by $\mathcal{L}(\mathcal{H})$. In $\mathcal{L}(\mathcal{H})$, we denote by $\mathbb{1}_{\mathcal{H}}$ the identity operator on $\mathcal{H}$, which satisfies the condition that $\mathbb{1}_{\mathcal{H}}|\psi\rangle = |\psi\rangle$ for any $|\psi\rangle \in \mathcal{H}$. When $\mathcal{H}$ is clear from the context, we may drop the subscript of $\mathbb{1}_{\mathcal{H}}$. When $\mathcal{H}$ is finite-dimensional, if an orthonormal basis $\{\boldsymbol{a}_j \mid j \in [n]\}$ is chosen for $\mathcal{H}$, a linear operator $T : \mathcal{H} \to \mathcal{H}$ can be written as an $n \times n$ matrix M such that the (i, j)-th entry, denoted by $M(i, j)$, equals $\boldsymbol{a}_i^\dagger T(\boldsymbol{a}_j)$ for any $i, j \in [n]$. If M has an inverse, i.e. an $n \times n$ matrix N such that $MN = \mathbb{1}$, the inverse of M is denoted by M^{-1}. For a matrix M, $M^\intercal$ is its transpose; $\overline{M}$ is its complex conjugate; and $M^\dagger$ is its conjugate transpose, which equals $\overline{M^\intercal}$. Let $M_1 \in \mathcal{L}(\mathbb{C}^{d_1})$ and $M_2 \in \mathcal{L}(\mathbb{C}^{d_2})$ be two matrices for some $d_1, d_2 \geq 2$. Define

$$M_1 \oplus M_2 = \begin{bmatrix} M_1 & 0 \\ 0 & M_2 \end{bmatrix} \in \mathcal{L}(\mathbb{C}^{d_1+d_2}),$$

$$M_1 \otimes M_2 = \begin{bmatrix} M_1(1,1)M_2 & \dots & M_1(1,d_1) \\ \vdots & \ddots & \vdots \\ M_1(d_1,1)M_2 & \dots & M_1(d_1,d_1)M_2 \end{bmatrix} \in \mathcal{L}(\mathbb{C}^{d_1 d_2}),$$

which are referred to as the direct sum of M_1 and M_2 and the tensor product of M_1 and M_2 respectively.

We can generalize the inverse of a matrix and the conjugate transpose of a matrix to operators on a general Hilbert space $\mathcal{H}$.

Definition 2.3. *The **inverse of a linear operator** $M \in \mathcal{L}(\mathcal{H})$, if exists, is an operator $N \in \mathcal{L}(\mathcal{H})$ such that $M(N(\boldsymbol{a})) = N(M(\boldsymbol{a})) = \boldsymbol{a}$ for all $\boldsymbol{a} \in \mathcal{H}$, and it is denoted by M^{-1}.*

Definition 2.4. *The **adjoint of a linear operator** $M \in \mathcal{L}(\mathcal{H})$ is the operator $N \in \mathcal{L}(\mathcal{H})$ such that $\langle M\boldsymbol{a}, \boldsymbol{b}\rangle = \langle \boldsymbol{a}, N\boldsymbol{b}\rangle$ for any $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{H}$, and it is denoted by $M^\dagger$.*

The existence of $M^\dagger$ and the fact that $M^\dagger$ is also bounded follow the Riesz representation theorem [32, Theorem A.3].

Definition 2.5. *A linear operator $U \in \mathcal{L}(\mathcal{H})$ is a **unitary operator** if $U^\dagger = U^{-1}$.*

The set of unitary operators on $\mathcal{H}$ is denoted by $\mathcal{U}(\mathcal{H})$.

Definition 2.6. *A linear operator $H \in \mathcal{L}(\mathcal{H})$ is a **Hermitian operator** if $H^\dagger = H$.*

A complex number z is an *eigenvalue* of $M \in \mathcal{L}(\mathcal{H})$ if $(M - z)\boldsymbol{a} = 0$ for some $\boldsymbol{a} \neq 0$.

Definition 2.7. *A Hermitian operator $P \in \mathcal{L}(\mathcal{H})$ is **positive semi-definite** if all its eigenvalues are non-negative.*

Definition 2.8. *A unitary operator $O \in \mathcal{L}(\mathcal{H})$ is an **observable** of order-m if $O^m = \mathbb{1}_{\mathcal{H}}$.*

The definition implies that the eigenvalues of an order-m observable, O, are of the form ω_m^j for some $j \in [m]$, and the eigenspaces of different eigenvalues are orthogonal. For example, the eigenvalues of a binary observable, i.e. an order-2 observable, are $+1$ and -1.

Definition 2.9. *A Hermitian operator $P \in \mathcal{L}(\mathcal{H})$ is a* ***projector*** *if $P^2\boldsymbol{a} = P\boldsymbol{a}$ for all $\boldsymbol{a} \in \mathcal{H}$.*

The definition of a projector implies that all the eigenvalues of it are $+1$ and 0. Given an orthonormal set of vectors, $S = \{|v_j\rangle \mid j \in [m]\}$, the projector onto the vector space spanned by S, i.e., $V = \mathrm{span}(S)$, is $\Pi_V = \sum_{j=1}^{m} |v_j\rangle\langle v_j|$.

For a matrix $X \in \mathcal{L}(\mathbb{C}^d)$, we denote its trace by $\mathrm{Tr}(X)$ and define the normalized trace as

$$\widetilde{\mathrm{Tr}}(X) := \frac{\mathrm{Tr}(X)}{d}.$$

We work with the *normalized Hilbert-Schmidt norm* and the *operator norm*.

Definition 2.10. *For a matrix $M \in \mathcal{L}(\mathbb{C}^d)$ for some integer $d \geq 1$, its* ***normalized Hilbert-Schmidt norm*** *is*

$$\|M\| = \sqrt{\frac{\mathrm{Tr}(M^\dagger M)}{d}}.$$

Definition 2.11. *For a matrix $M \in \mathcal{L}(\mathbb{C}^d)$ for some integer $d \geq 1$, its* ***operator norm*** *is*

$$\|M\|_{op} = \sup_{|\psi\rangle \in \mathbb{C}^d, \||\psi\rangle\| = 1} \|M|\psi\rangle\|.$$

The fundamental relations between the normalized Hilbert-Schmidt norm and the operator norm that we use in this dissertation are summarized in the following lemma.

Lemma 2.12. *For $A, B \in \mathcal{L}(\mathbb{C}^d)$,*

$$
\begin{aligned}
&|\widetilde{\mathrm{Tr}}(A)| \leq \|A\| \\
&\|A \otimes B\| = \|A\|\|B\| \\
&\|A + B\| \leq \|A\| + \|B\| \\
&\|AB\| \leq \|A\|_{op}\|B\| \\
&\|BA\| \leq \|B\|\|A\|_{op} \\
&\|A\| \leq \|A\|_{op} \leq \sqrt{d}\|A\|.
\end{aligned}
$$

The proof of this lemma can be found in [33], so we omit it here.

Here, we list some widely-used quantum states and operators. A pure quantum bit (*qubit*) is a unit vector of $\mathbb{C}^2$. The basis states $|0\rangle$ and $|1\rangle$ corresponds to $\boldsymbol{e}_0$ and $\boldsymbol{e}_1$ respectively. The Pauli operators of $\mathcal{L}(\mathbb{C}^2)$ are

$$
\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.
$$

The maximally entangled state of two qubits is denoted by

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

$|\mathsf{EPR}\rangle$ is a unit vector of $\mathbb{C}^2 \otimes \mathbb{C}^2$ and it is named after Einstein, Podolsky and Rosen [34] as the *EPR pair*. For any $d \geq 2$, we denote the generalized EPR pair in $\mathbb{C}^d \otimes \mathbb{C}^d$ by

$$|\mathsf{EPR}_d\rangle = \frac{1}{\sqrt{d}} \sum_{j \in [d]} |j\rangle|j\rangle.$$

We say a pure quantum state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ is *maximally entangled*, if there exists $U, V \in \mathcal{U}(\mathbb{C}^d)$ such that $(U \otimes V)|\psi\rangle = |\mathsf{EPR}_d\rangle$. We refer to such U and V as local unitaries as they only act on one d-dimensional Hilbert space.

Between two Hilbert spaces $\mathcal{H}$ and $\mathcal{H}'$, an isometry is a linear map $V : \mathcal{H} \to \mathcal{H}'$, such that $V^\dagger V = \mathbb{1}_{\mathcal{H}}$.

Definition 2.13. *For Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$, a linear map $\Phi : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ is a* ***local isometry*** *if there exist isometries $V_A : \mathcal{H}_A \to \mathcal{H}_{A'}$ and $V_B : \mathcal{H}_B \to \mathcal{H}_{B'}$ such that for any state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$,*

$$\Phi(|\psi\rangle) = (V_A \otimes V_B)|\psi\rangle.$$

Chapter 3: Group theory background

In this chapter, we introduce all the necessary group theory results for this dissertation. In Section 3.1, we introduce group presentations and four ways to extend a given group. In Section 3.2, we introduce group representations and approximate representations. In Section 3.3, we introduce solvable groups, sofic groups and hyperlinear groups. In Section 3.4, we introduce Slofstra's fa^*-embedding procedure, which we apply to a sofic group of certain structure.

Definition 3.1 (Group). *A group is a set G with an operation $\cdot$, such that*

1. *for any $a, b \in G$, $a \cdot b \in G$;*

2. *for any $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;*

3. *there exists an element e such that $e \cdot a = a \cdot e = a$ for any $a \in G$; and*

4. *for any $a \in G$, there exists an element $b \in G$ such that $a \cdot b = b \cdot a = e$, which is called the inverse of a.*

Note that the identity element is unique in a group G and it is always denoted by e. For simplicity, we write $a \cdot b$ as ab. For $g \in G$, we denote the inverse of g by g^{-1}. We denote the commutator of $g, h \in G$ by $[g, h] = g^{-1}h^{-1}gh$ and the conjugation of g by h by $h^{-1}gh$. For simplicity, we also write $h^{-1}gh$ as g^h.

Definition 3.2. *We say a group G is of **exponent** n for some $n \geq 1$ if $g^n = e$ for all $g \in G$.*

Definition 3.3. *For a group G, a subset H of G is a **subgroup** of G if H satisfies the four group requirements in Definition 3.1.*

When H is a subgroup of G, we write $H \leq G$.

Definition 3.4. *For a group G, a subgroup N is a **normal subgroup** of G if for all $n \in N$ and $g \in G$, $g^{-1}ng \in N$.*

When N is a normal subgroup of G, we write $N \trianglelefteq G$. If we define $g^{-1}Ng := \{g^{-1}ng \mid n \in N\}$, then $N \trianglelefteq G$ if and only if $g^{-1}Ng = N$ for all $g \in G$. If we define $gN := \{gn \mid n \in N\}$ and $Ng := \{ng \mid n \in N\}$, then $N \trianglelefteq G$ if and only if $gN = Ng$ for all $g \in G$.

Definition 3.5. *Let N be a normal subgroup of G, the **quotient group** of N in G is*

$$G/N = \{gN \mid g \in G\}$$

with an operation $\cdot$ such that $aN \cdot bN = (ab)N$ where ab follows the group multiplication rule of G.

Definition 3.6. *Let $S \subset G$, then **the normal subgroup generated by** S, denoted by $\langle S \rangle^G$, is the closure of $\{g^{-1}sg \mid s \in S, g \in G\}$ under the group multiplication.*

When G is clear from context, we drop the superscript G.

Definition 3.7. *Let G and H be two groups. A map $\phi : G \to H$ is a **group homomorphism** if $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for any $g_1, g_2 \in G$.*

The natural homomorphism from G to G/N is the map: $g \mapsto gN$. For a more detailed treatment, we refer to [29, Chapters 1 - 2].

3.1 Group presentations and extensions of groups

Definition 3.8 (Free group)**.** *Let S be a set. The free group generated by S, denote by $\mathcal{F}(S)$, consists of the empty word e and non-empty words of the form $w = s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$ where $s_i \in S$, $\epsilon_i = +1$ or -1, and s and s^{-1} are never adjacent. The group multiplication rule is given by* juxtaposition*, so if the two words are $w = w'v$ and $u = v^{-1}u'$, where w', v, v^{-1}, u' are also words, then $w \cdot u = w'u'$.*

This definition is obtained from the proof of [29, Theorem 11.1]. For a more formal treatment, we refer to [29, Pages 343 - 345].

Definition 3.9 (Group presentation)**.** *Given a set S, let $\mathcal{F}(S)$ be the free group generated by S and let R be a subset of $\mathcal{F}(S)$. Then $\langle S : R \rangle = \mathcal{F}(S)/\langle R \rangle^{\mathcal{F}(S)}$. If the group G is isomorphic to $\langle S : R \rangle$, then $\langle S : R \rangle$ is a **presentation** of G.*

The elements of S are the *generators* and the elements of R are the *relations*. If both sets S and R are finite, then we say the group $G = \langle S : R \rangle$ is *finitely presented*. In this dissertation, we focus on finitely-presentable groups. A relation $r \in R$ is written as $r = e$ to convey its significance in the quotient group G because all the conjugates of r equal e in G.

We give three examples of group presentations below. A presentation of $\mathbb{Z}_2^2$

is

$$\langle x_1, x_2 : x_1^2 = x_2^2 = x_1x_2x_1x_2 = e\rangle.$$

The elements of $\mathbb{Z}_2^2$ are e, x_1, x_2 and x_1x_2. The relation $x_1x_2x_1x_2$ implies that $x_1x_2 = x_2x_1$ in $\mathbb{Z}_2^2$, so we can write the relation as $x_1x_2 = x_2x_1$.

The second example is the dihedral group.

Definition 3.10. *Let n be a positive integer. The **dihedral group** D_n is a group with the following presentation*

$$\langle t_1, t_2 : t_1^2 = t_2^2 = (t_1t_2)^n = e\rangle.$$

The elements of D_n are $(t_1t_2)^j$ and $t_2(t_1t_2)^j$ for $j \in [n]$. In this dissertation, we will work with D_p where p is some odd prime number.

The third example is the solution group, which has two presentations.

Definition 3.11 (Definition 17 of [7])**.** *Let $A\boldsymbol{x} = 0$ be an $m \times n$ linear system over $\mathbb{Z}_2$, where A is an m-by-n matrix with entries in $\mathbb{Z}_2$ and 0 is an all-0 length-n vector. For $j \in [m]$, define $I_j = \{k \in [n] \mid A(j,k) = 1\}$. Then, the **homogeneous solution group***

of $A\boldsymbol{x} = 0$ *is*

$$\begin{aligned}\Gamma(A) := \langle x_0, x_1, \dots x_{n-1} : & x_j^2 = e \text{ for all } j \in [n], \\ & \prod_{k \in I_i} x_k = e \text{ for all } i \in [m], \\ & [x_j, x_k] = e \text{ if } j, k \in I_i \text{ for some } i \rangle.\end{aligned}$$

Proposition 3.12. *Let* $A\boldsymbol{x} = 0$ *be an* $m \times n$ *linear system over* $\mathbb{Z}_2$*. For* $j \in [m]$*, define*

$$G_j = \langle \{g_{j,k} \mid k \in I_j\} : g_{i,k}^2 = [g_{j,k}, g_{j,l}] = \prod_{k \in I_j} g_{j,k} = e \ \forall k, l \in I_j \rangle.$$

and a set

$$P = \{g_{i,k} = g_{j,k} \mid k \in I_i \cap I_j, i, j \in [m]\}.$$

Define

$$\Gamma'(A) := \frac{G_0 * G_1 \dots * G_{m-1}}{\langle P \rangle}.$$

Then, $\Gamma(A) \cong \Gamma'(A)$*.*

Proof. Define $\phi : \Gamma(A) \to \Gamma'(A)$ by

$$\phi(x_i) = g_{j_i, i} \text{ with } i \in I_{j_i}$$

for all $i \in [n]$. We are going to show that ϕ is an isomorphism.

First of all, $\phi(x_i)^2 = g_{j_i,i}^2 = e$ for all $i \in [n]$. For each $k, l \in I_j$ for some j,

$$\phi(x_k)\phi(x_l)\phi(x_k)\phi(x_l) = g_{i_k,k}g_{i_l,l}g_{i_k,k}g_{i_l,l} = g_{j,k}g_{j,l}g_{j,k}g_{j,l} = e.$$

For each $j \in [m]$,

$$\phi(\prod_{k \in I_j} x_k) = \prod_{k \in I_j} \phi(x_k) = \prod_{k \in I_j} g_{i_k,k} = \prod_{k \in I_j} g_{j,k} = e.$$

Let $w \in \mathcal{F}(\{x_i | i \in [n]\})$ such that $w = e$ in $\Gamma(A)$. Then w must be a product of the conjugates of the relations of $\Gamma(A)$ and we have established that $\phi(w) = e$. Hence, ϕ is a well-defined homomorphism.

Moreover, for each $g_{j,k}$, since $g_{j,k} = g_{i_k,k}$, we know the preimage of $g_{j,k}$ in $\Gamma(A)$ is x_k, which implies that ϕ is surjective.

To see ϕ is injective, consider $w \in \mathcal{F}(\{g_{j,k} | j \in [m], k \in I_j\})$ such that $w = e$ in $\Gamma'(A)$. Then w must be a product of the conjugates of relations of $\Gamma'(A)$. The preimage of relations of the form $g_{j,k}^2$ is x_k^2, which is trivial in $\Gamma(A)$. The preimage of relations of the form $[g_{j,k}, g_{j,l}]$ for $k, l \in I_j$ is $[x_k, x_l]$, which is trivial in $\Gamma(A)$. The preimage of relations of the form $\prod_{k \in I_j} g_{j,k}$ is $\prod_{k \in I_j} x_k$, which is trivial in $\Gamma(A)$. The preimage of relations of the form $g_{j,k}g_{j',k}$ for some $k \in I_j \cap I_{j'}$ is $x_k x_k$, which is also trivial in $\Gamma(A)$. Hence, ϕ is also injective and an isomorphism. □

Next we introduce four ways to construct new groups by extending given groups: taking a semidirect product of the given groups, taking the free product of the given groups, taking the free product of the given groups with amalgamation, and taking the HNN-extension of a given group.

3.1.1 Semidirect product

Definition 3.13. *Let K be a (not necessarily normal) subgroup of a group G. Then a subgroup $Q \leq G$ is a* ***complement*** *of K in G if $K \cap Q = \{e\}$ and $KQ = G$.*

Definition 3.14. *A group G is a* ***semidirect product*** *of K by Q, denoted by $G = K \rtimes Q$, if K is a normal subgroup of G and K has a complement $Q_1 \cong Q$.*

A few properties of semidirect product are summarized in the following lemma.

Lemma 3.15 (Lemma 7.20 of [29])**.** *If K is a normal subgroup of a group G, then the following statements are equivalent:*

1. *G is a semidirect product of K by G/K;*
2. *there is a subgroup $Q \leq G$ so that every element $g \in G$ has a unique expression $g = ax$, where $a \in K$ and $x \in Q$; and*
3. *there exists a homomorphism $s : G/K \to G$ with $v \circ s = \mathbb{1}_{G/K}$ (meaning that $v \circ s$ is the identity map on G/K), where $v : G \to G/K$ is the natural map.*

Definition 3.16. *Let Q and K be groups, let $Aut(K)$ be the group of automorphisms of K, and let $\theta : Q \to Aut(K) : x \mapsto \theta_x$ be a homomorphism. A semidirect product G of K by Q* ***realizes*** *θ, if for all $x \in Q$ and $a \in K$*

$$\theta_x(a) = x^{-1}ax.$$

3.1.2 Free product

Definition 3.17. *Let $\{G_i \mid i \in I\}$ be a family of groups. A* ***free product*** *of the G_i is a group H and a family of homomorphisms $j_i : G_i \to H$ such that, for every group K and every family of homomorphisms $f_i : G_i \to K$, there exists a unique homomorphism $\phi : H \to K$ such that $\phi j_i = f_i$ for all $i \in I$ as shown in the figure below.*

$$\begin{tikzcd} G_i \arrow[r, "j_i"] \arrow[dr, "f_i"'] & H \arrow[d, "\phi"] \\ & K \end{tikzcd}$$

Figure 3.1: Free product: group embedding diagram

The free product of $\{G_i \mid i \in I\}$ is denoted by $*_{i\in I} G_i$. In fact, the homomorphisms j_i are injective [29, Lemma 11.49].

Next we give more insights of the free product, which follows the proof of [29, Theorem 11.51].

For a family of groups $\{G_i \mid i \in I\}$, define $G_i^{\#} = G_i \setminus \{e\}$. Then the group elements of $*_{i\in I} G_i$ are the empty word e and non-empty words of the form $g_1 g_2 \ldots g_n$ where each $g_i \in G_j^{\#}$ for some j and adjacent g_i's lie in different $G_j^{\#}$. The multiplication is given by *juxtaposition*. More specifically, $e \cdot w = w \cdot e = w$ for all $w \in *_{i\in I} G_i$, and

$$(g_1g_2\dots g_n)\cdot(h_1h_2\dots h_m) = \begin{cases} g_1g_2\dots g_nh_1\dots h_m & \text{if } g_n \text{ and } h_1 \text{ lie in different } G_i^\# \\ g_1\dots g_{n-1}(g_nh_1)h_2\dots h_m & \text{if } g_n, h_1 \in G_i^\# \text{ but } g_nh_1 \neq e \text{ in } G_i \\ (g_1\dots g_{n-1})\cdot(h_2\dots h_m) & \text{if } g_n, h_1 \in G_i^\# \text{ and } g_nh_1 = e \text{ in } G_i. \end{cases}$$

Note that in the last case the juxtaposition rule is applied again to $(g_1\dots g_{n-1})\cdot(h_2\dots h_m)$.

Theorem 3.18 (Theorem 11.53 of [29]). *Let $\{G_i \mid i \in I\}$ be a family of groups, and let a presentation of G_i be $\langle S_i : R_i\rangle$, where $S_i \cap S_j = \emptyset$ for all $i \neq j \in I$. Then a presentation of $*_{i\in I}A_i$ is $\langle \bigcup_{i\in I} S_i : \bigcup_{i\in I} R_i\rangle$.*

When there are finitely many groups, we write $*_{i\in[n]}G_i$ as $G_0 * G_1 * \dots * G_{n-1}$. In this dissertation, we only take the free product of two groups G and H. For simplicity, when the presentation of G is clear from the context, we slightly abuse the notation and write a presentation of $G * H$ as $\langle G, S_H : R_H\rangle$. For a more detailed treatment of free products, we refer to [29, Pages 388 - 391].

3.1.3 Free product with amalgamation

Definition 3.19. *Let G_1 and G_2 be two groups with subgroups H_1 and H_2 respectively such that H_1 is isomorphic to H_2 under the isomorphism $\theta : H_1 \to H_2$. Then the **free***

product of G_1 ***and*** G_2 ***with amalgamation*** *is defined by*

$$G_1 *_\theta G_2 := \frac{G_1 * G_2}{\langle\{h_1 = \phi(h_1) \mid h_1 \in H_1\}\rangle^{G_1 * G_2}},$$

where $\langle\{h_1 = \theta(h_1) \mid h_1 \in H_1\}\rangle^{G_1 * G_2}$ *is the normal subgroup of* $G_1 * G_2$ *generated by all the relations of the form* $h_1 = \theta(h_1)$*.*

Definition 3.20. *For* $i \in \{1, 2\}$ *and* $a \in G_i$*, let* $l(a)$ *be a fixed representative of* aH_i *such that* $l(e) = e$ *and if* $a_1 H_i = a_2 H_i$*, then* $l(a_1) = l(a_2)$*. A* ***normal form*** *is an element of* $G_1 *_\theta G_2$ *of the form*

$$l(a_1)l(a_2)\ldots l(a_n)b,$$

where $b \in H_1$*,* $n \geq 0$*, the elements* $l(a_j)$ *are representatives of left cosets of* H_{i_j} *in* G_{i_j}*, and adjacent* $l(a_j)$ *lie in distinct* G_i*.*

Theorem 3.21 (Theorem 11.66 of [29])**.** *Let* G_1 *and* G_2 *be groups, let* H_i *be a subgroup of* G_i *for* $i = 1, 2$*, and let* $\theta : H_1 \to H_2$ *be an isomorphism. Then, for each element* $wN \in G_1 *_\theta G_2$*, where* $N = \langle\{h = \theta(h) \mid h \in H_1\}\rangle^{G_1 * G_2}$*, there is a unique normal form* $F(w)$ *with* $wN = F(w)N$*.*

Theorem 3.22 (Theorem 11.67 of [29])**.** *Let* G_1 *and* G_2 *be groups, let* H_1 *and* H_2 *be isomorphic subgroups of* G_1 *and* G_2 *respectively, and let* $\theta : H_1 \to H_2$ *be an isomorphism. Then,* G_1 *and* G_2 *are subgroups of* $G_1 *_\theta G_2$*.*

For a more detailed treatment of the free product of groups with amalgamation, we refer to [29, Pages 401 - 404].

3.1.4 HNN-extension

Free product of groups with amalgamation is used in the proof of the following theorem due to Graham Higmann, Bernhard Neumann and Hanna Neumann [35].

Theorem 3.23 (Theorem 11.70 [29])**.** *Let G be a group and let $\phi : A \to B$ be an isomorphism between subgroups A and B of G. Then, there exists a group K containing G and an element $t \in K$ with*

$$\phi(a) = t^{-1}at \text{ for all } a \in A.$$

This theorem is generalized to give a new way to construct new groups from a given group, known as the Higman-Neumann-Neumann extension (*HNN-extension*).

Definition 3.24. *Let H be a subgroup of G and let $\phi : H \to H$ be an injective homomorphism, then the **HNN-extension** of G is*

$$\frac{G * \mathcal{F}(\{t\})}{\langle \{t^{-1}ht = \phi(h) \mid h \in H\} \rangle^{G*\mathcal{F}(\{s\})}},$$

where $t \notin G$.

We slightly abuse the notation and write a presentation of the HNN-extension of G as

$$\overline{G} = \langle G, t : \{t^{-1}ht = \phi(h) \mid h \in H\} \rangle.$$

$\overline{G}$ is a subgroup generated by G and t of the group K in the statement of Theorem 3.23.

Next, we introduce the normal form of elements of an HNN extension.

Definition 3.25. *A **normal form** is a sequence $g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$ ($n \geq 0$) where*

1. *g_0 is an arbitrary element of G and $\epsilon_i \in \{-1, 1\}$ for all i,*
2. *if $\epsilon_i = -1$, then g_i is a representative of a coset of H in G,*
3. *if $\epsilon_i = 1$, then g_i is a representative of a coset of $\phi(H)$ in G, and*
4. *there is no consecutive subsequence of the form $t^{\epsilon}, e, t^{-\epsilon}$.*

Theorem 3.26 (Theorem 2.1 of Chapter IV of [36]). *Let $\overline{G} = \langle G, t : \{t^{-1}ht = \phi(h) \mid h \in H\}\rangle$ be an HNN extension. Then*

1. *The group G is embedded in $\overline{G}$ by the map $g \mapsto g$. If $g_0 t^{\epsilon_1} \ldots t^{\epsilon_n} g_n = e$ in $\overline{G}$, then $g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$ contains a subsequence of the form t^{-1}, h, t or $t, \phi(h), t^{-1}$ for some $h \in H$.*
2. *Every element w of $\overline{G}$ has a unique representative as $w = g_0 t^{\epsilon_1} \ldots t^{\epsilon_n} g_n$ where the sequence $g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$ is a normal form.*

This theorem is also referred to as the *Normal Form Theorem for HNN Extension*.

Definition 3.27. *Let G be a group, let H be a subgroup of G, and let ϕ be an automor-*

phism of H such that there exists $p > 0$ with $\phi^p(h) = h$ for all $h \in H$. Then,

$$\hat{G} := \frac{G * \langle t : t^p = e \rangle}{\langle \{t^{-1}ht = \phi(h) \mid h \in H\} \rangle^{G * \langle t : t^p = e \rangle}}$$

*is called the $\mathbb{Z}_p$-**HNN extension** of G.*

In the rest of this dissertation, we focus on the case that p is an odd prime number.

Definition 3.28. *A **normal form** of a $\mathbb{Z}_p$-HNN extension is a sequence g_0, $t^{\epsilon_1}, \ldots, t^{\epsilon_n}$, g_n ($n \geq 0$) where*

1. *g_0 is an arbitrary element of G and $\epsilon_i \in \{-1, 1\}$ for all i,*
2. *g_i is a representative of a right coset of H in G for $1 \leq i \leq n$,*
3. *there is no consecutive subsequence of the form t^{ϵ}, e, $t^{-\epsilon}$, and*
4. *there is no subsequence of the form $\overbrace{t^{\epsilon}, e, t^{\epsilon}, \ldots, t^{\epsilon}, e, t^{\epsilon}}^{k \text{ of } t^{\epsilon}}$ for $k > p/2$.*

Theorem 3.29. *Let $\hat{G}$ be a $\mathbb{Z}_p$-HNN extension of G with respect to an automorphism of $H \leq G$ such that $\phi^p(h) = h$ for all $h \in H$. Then, every element w of $\hat{G}$ has a unique representative as $w = g_0 t^{\epsilon_1} \ldots t^{\epsilon_n} g_n$ where the sequence g_0, $t^{\epsilon_1}, \ldots, t^{\epsilon_n}$, g_n is a normal form.*

The proof is similar to Theorem 3.26 and we present it in Appendix A.

Corollary 3.30. *Let $\hat{G}$ be a $\mathbb{Z}_p$-HNN extension of G with respect to an automorphism of $H \leq G$ such that $\phi^p(h) = h$ for all $h \in H$. Then, $G \leq \hat{G}$.*

This corollary follows from the fact that each $g \in G$ is a unique normal form.

Theorem 3.31. *Let $\hat{G}$ be a $\mathbb{Z}_p$-HNN extension of G with respect to an automorphism of $H \leq G$ such that $\phi^p(h) = h$ for all $h \in H$. Then,*

$$\hat{G} = K \rtimes \langle t : t^p = e \rangle,$$

where K is the subgroup generated by $t^{-i}Gt^i$ for $i = 0, 1, \ldots, p-2, p-1$ and the action of t on $k \in K$ is conjugation by t.

Proof. By Theorem 3.29 and each element of $\hat{G}$ has a representative as the product of a unique normal form as

$$g_0 t^{\epsilon_1} g_1 \ldots t^{\epsilon_n} g_n = g_0 g_1^{t^{-\epsilon_1}} g_2^{t^{-\epsilon_1 - \epsilon_2}} \ldots g_n^{t^{-\sum_{i=1}^{n} \epsilon_i}} t^{\sum_{i=1}^{n} \epsilon_i}$$

where the addition in the exponent of t is modulo p. Then the theorem follows.

□

3.2 Group representation and approximate representation

Definition 3.32. *A **unitary representation** of a group G on the Hilbert space $\mathcal{H}$ is a homomorphism from G to $\mathcal{U}(\mathcal{H})$, which is the unitary group of $\mathcal{H}$ with matrix multiplication.*

Note that if a presentation of G is $\langle S : R \rangle$, then a representation of G can also be expressed as a homomorphism $\phi : \mathcal{F}(S) \to \mathcal{U}(\mathcal{H})$ such that $\phi(r) = \mathbb{1}_{\mathcal{H}}$ for all $r \in R$.

For example, taking $\mathcal{H} = \mathbb{C}$ and mapping: $g \mapsto 1$ gives us the trivial representation of G. Among all the representations of G, we will work with the *regular representation* of G.

Definition 3.33. *Denote the Hilbert space over $\mathbb{C}$ with basis $\{|g\rangle : g \in G\}$ by $\ell^2 G$. Define $L_g \in \mathcal{U}(\ell^2 G)$ by*

$$L_g = \sum_{h \in G} |gh\rangle\langle h|$$

and $R_g \in \mathcal{U}(\ell^2 G)$ by

$$R_g = \sum_{h \in G} |hg^{-1}\rangle\langle h|$$

*for each $g \in G$. Then, the **left regular representation** of G is the homomorphism $\phi_L : G \to \mathcal{U}(\ell^2 G)$ such that $\phi_L(g) = L_g$; and the **right regular representation** of G is the homomorphism $\phi_R : G \to \mathcal{U}(\ell^2 G)$ such that $\phi_R(g) = R_g$ for each $g \in G$.*

It is immediate to see that

$$\begin{aligned} L_g L_{g'} &= L_{gg'} \\ R_g R_{g'} &= R_{gg'} \\ L_g R_{g'} &= R_{g'} L_g \end{aligned}$$

for all $g, g' \in G$. That is, L_g commutes with $R_{g'}$ for all $g, g' \in G$.

If $\mathcal{H}$ is finite-dimensional, we say a representation of G on $\mathcal{U}(\mathcal{H})$ is a *finite-*

dimensional representation. The set of elements that are trivial in all finite-dimensional representations form a normal subgroup of G, denoted by N^{fin}. For any group G, we define

$$G^{fin} := G/N^{fin}.$$

Definition 3.34 (Definition 10 of [7]). *A homomorphism $\phi : G \to H$ is a **fin-embedding** if the induced map: $G^{fin} \to H^{fin}$ is injective.*

Definition 3.35 (Definition 10 of [7]). *A homomorphism $\phi : G \to H$ is a **fin*-embedding** if it is injective and also a fin-embedding.*

Next, we define approximate representations of a group G.

Definition 3.36 (Definition 5 of [7]). *Let $G = \langle S : R \rangle$ be a finitely-presented group, and let $\mathcal{H}$ be a finite-dimensional Hilbert space. A finite-dimensional **ϵ-approximate representation** of G is a homomorphism $\phi : \mathcal{F}(S) \to \mathcal{U}(\mathcal{H})$ such that $\|\phi(r) - \mathbb{1}\| \leq \epsilon$ for all $r \in R$.*

Note that in the definition above, the group G is defined by its presentation $\langle S : R \rangle$ and each $g \in G$ has a defining representative in $\mathcal{F}(S)$. An element $g \in G = \langle S : R \rangle$, whose defining representative is $w \in \mathcal{F}(S)$, is *nontrivial in approximate representations* of G if there exist some $\delta > 0$ such that for all $\epsilon > 0$, there is an ϵ-approximate representation $\phi : \mathcal{F}(S) \to \mathcal{U}(\mathcal{H})$ such that $\|\phi(w) - \mathbb{1}\| \geq \delta$. On the other hand, an element $g \in G = \langle S : R \rangle$, whose representative is $w \in \mathcal{F}(S)$, is *trivial in approximate representations* of G if for all $\epsilon > 0$

and all ϵ-approximate representation $\phi : \mathcal{F}(S) \to \mathcal{U}(\mathcal{H})$, $\phi(w) = \mathbb{1}$.

Lemma 3.37. *Let ψ_j be an ϵ_j-approximate representation of $G = \langle S : R \rangle$ on $\mathbb{C}^{d_j}$ for $j \in [k]$. Then,*

$$\bigoplus_{j\in[k]} \psi_j : G \to \mathcal{U}(\mathbb{C}^{\sum d_j}),\ \textit{written as}\ g \mapsto \bigoplus_{j\in[k]} \psi_j(g)$$

is a $\max_{j\in[k]} \epsilon_j$-approximate representation; and

$$\bigotimes_{j\in[k]} \psi_j : G \to \mathcal{U}(\mathbb{C}^{\prod d_j}),\ \textit{written as}\ g \mapsto \bigotimes_{j\in[k]} \psi_j(g)$$

is a $\sum_{j\in[k]} \epsilon_j$-approximate representation.

Proof. Let $r \in R$. The direct product case can be proved by

$$\|\bigoplus_{j\in[k]} \psi_j(r) - \mathbb{1}\| = \sum_{j\in[k]} \frac{d_j\|\psi_j(r) - \mathbb{1}\|}{\sum_{j\in[k]} d_j} \le \max_{j\in[k]} \epsilon_j.$$

The tensor-product case can be proved using Triangle inequality as

$$\begin{aligned}\|\bigotimes_{j\in[k]} \psi_j(r) - \mathbb{1}\| &\le \|\bigotimes_{j\in[k]} \psi_j(r) - \mathbb{1}_{\mathbb{C}^{d_0}} \otimes \bigotimes_{j=1}^{k-1} \psi_j(r)\| + \ldots + \|\mathbb{1}_{\mathbb{C}^{\prod_{j\in[k-1]} d_j}} \otimes \psi_{k-1}(r) - \mathbb{1}\| \\ &= \sum_{j\in[k]} \|\psi_j(r) - \mathbb{1}\| = \sum_{j\in[k]} \epsilon_j,\end{aligned}$$

where we use the fact that $\|\psi_j(r)\| = 1$. □

Proposition 3.38. *The set of elements of $G = \langle S : R \rangle$ that are trivial in finite-dimensional approximate representations form a normal subgroup of G, denoted by N^{fa}.*

Proof. Every element in N^{fa} can be written as

$$\prod_{i\in[n]} w_i^{-1} g_i w_i$$

for some $n \geq 1$, where $w_i \in \mathcal{F}(S)$ and g_i is trivial in approximate representations of G. Let $\psi : G \to \mathcal{U}(\mathbb{C}^d)$ be an ϵ-approximate representation of G. Then,

$$\psi(\prod_{i\in[n]} w_i^{-1} g_i w_i) = \prod_{i\in[n]} \psi(w)^{-1}\psi(g_i)\psi(w) = \mathbb{1},$$

where we use the definition of elements that are trivial in finite-dimensional approximate representations. Since the equation above holds for all ϵ-approximate representations, the proposition follows. □

For a group G, we define

$$G^{fa} := G/N^{fa}.$$

Definition 3.39 (Definition 14 of [7])**.** *For finitely-presented groups G and H, a homomorphism $\phi : G \to H$ is an **fa-embedding** if the induced map: $G^{fa} \to H^{fa}$ is injective.*

Definition 3.40 (Definition 14 of [7])**.** *For finitely-presented groups G and H, a homomorphism $\phi : G \to H$ is an **fa*-embedding**, if it is injective, a fin-embedding and an fa-embedding.*

To determine if a homomorphism $\phi : G \to H$ is a fa^*-embedding, we use the following lemma.

Lemma 3.41 (Lemma 15 of [7]). *Let $G = \langle S : R \rangle$ and $H = \langle S' : R' \rangle$ be two finitely presented groups, and let $\Psi : \mathcal{F}(S) \to \mathcal{F}(S')$ be a lift of a homomorphism $\psi : G \to H$.*

1. *Suppose that for every representation (resp. finite-dimensional representation) ϕ of G, there is a representation (resp. finite-dimensional representation) γ of H such that ϕ is a direct summand of $\gamma \circ \psi$. Then ψ is injective (resp. a fin-embedding).*

2. *Suppose that there is an integer $N > 0$ and a real number $C > 0$ such that for every d-dimensional ϵ-representation ϕ of G, where $\epsilon > 0$, there is an Nd-dimensional $C\epsilon$-representation γ of H such that ϕ is a direct summand of $\gamma \circ \psi$. Then ψ is an fa-embedding.*

For more details, we refer to [7, Section 2].

3.3 Solvable groups, sofic groups and hyperlinear groups

Our main results require properties of solvable groups, sofic groups and hyperlinear groups. We formally introduce them below. We also state the relations between them and the properties of them in this section.

Definition 3.42. *A group G is **solvable** if it has subgroups $G_0 = \{e\}, G_1, \ldots, G_{k-1}$ and $G_k = G$ such that G_{j-1} is normal in G_j and G_j/G_{j-1} is an abelian group, for $1 \le j \le k$.*

Before we introduce sofic groups, we first introduce the permutation group S_n.

Definition 3.43. *The* ***permutation group*** S_n *is the group of all the permutations of* $[n]$ *where the operation is the composition of permutations.*

The *Hamming invariant length function* ℓ on S_n is defined by

$$\ell_{S_n}(\sigma) = \frac{1}{n}|\{i \in [n] \mid \sigma(i) \neq i\}|$$

for each $\sigma \in S_n$.

Definition 3.44. *A finitely-presented group* G *is* ***sofic*** *if for every* $\epsilon > 0$ *and every finite subset* F *of* $G \setminus \{e\}$*, there is a natural number* n *and a function* $\Psi : G \to S_n$ *such that* $\Psi(e_G) = e_{S_n}$ *and for every* $g, h \in F$*:*

- $\ell_{S_n}(\Psi(gh)(\Psi(g)\Psi(h))^{-1}) < \epsilon$*; and*
- $\ell_{S_n}(\Psi(g)) > r(g)$ *where* $r(g)$ *is a positive constant only depending on* g*.*

We denote the set of all $n \times n$ unitaries by $\mathcal{U}_n$ and define the *Hilbert-Schmidt invariant length function* on $\mathcal{U}_n$ by

$$\ell_{\mathcal{U}_n}(U) = \frac{1}{2}\|U - \mathbb{1}\|.$$

Definition 3.45. *A finitely-presented group* G *is* ***hyperlinear*** *if for every* $\epsilon > 0$ *and every finite subset* F *of* $G \setminus \{e\}$*, there is a natural number* n *and a function* $\Psi : G \to \mathcal{U}_n$ *such that* $\Psi(e_G) = \mathbb{1}$ *and for every* $g, h \in F$*:*

- $\ell_{\mathcal{U}_n}(\Psi(gh)(\Psi(g)\Psi(h))^{-1}) < \epsilon$*; and*
- $\ell_{\mathcal{U}_n}(\Psi(g)) > r(g)$ *where* $r(g)$ *is a positive constant only depending on* g*.*

For more details about sofic groups and hyperlinear groups, we refer to [37, Chapter 2.1 and 2.2].

For our proof, we use the following properties of solvable groups and sofic group introduced in [37, Chapter 2.3 and 2.4].

Proposition 3.46 (Proposition 2.3.1 of [37])**.** *Solvable groups are sofic.*

Proposition 3.47 (Proposition 2.2.5 of [37])**.** *Every sofic group is hyperlinear.*

Slofstra proves a lemma relating hyperlinear groups and approximate representations.

Lemma 3.48 (Lemma 13 of [7])**.** *A finitely-presented group G is **hyperlinear** if and only if every non-trivial element of G is nontrivial in approximate representations.*

About the closure properties of sofic groups, we record the following propositions from [37].

Proposition 3.49 (Property 5 of Proposition 2.4.1 of [37])**.** *If a group G is sofic and K is an abelian group, then the semidirect product of G by K is also sofic.*

Proposition 3.50 (Property 7 of Proposition 2.4.1 of [37])**.** *If H_1 and H_2 are finite subgroups of sofic groups G_1 and G_2, and $\alpha : H_1 \to H_2$ is an isomorphism, then the free product of G_1 and G_2 with amalgamation, $G_1 *_\alpha G_2$, is sofic.*

Proposition 3.51 (Property 8 of Proposition 2.4.1 of [37])**.** *If H is a solvable subgroup of a sofic group G, and $\alpha : H \to H$ is an injective homomorphism, then the HNN-extension of G by α is sofic.*

Proposition 3.52. *Let G be a sofic group, let H be a subgroup of G and let ψ be a isomorphism of H of order p. Then,*

$$\hat{G} = \frac{G * \langle t : t^p = e \rangle}{\langle \{ t^{-1} h t = \psi(h) \mid h \in H \} \rangle}$$

is also sofic.

This proof is very similar to that of Proposition 3.51 and it is based on Theorem 3.31 and Proposition 3.49. We present it in Appendix A.

3.4 Slofstra's embedding procedure

In this section, we give an overview of Slofstra's fa^*-embedding procedure, first introduced in [7]. This procedure preserves elements that are nontrivial in finite-dimensional approximate representations, in the sense that if some elements are nontrivial in finite-dimensional approximate representations, then their images in the embedded group are also nontrivial in finite-dimensional approximate representations. The embedding procedure is a key step in the reductions from $(\text{Membership}(n_A, n_B, m_A, m_B)_{qc,\mathbb{K}})$ and $(\text{Membership}(n_A, n_B, m_A, m_B)_{qa,\mathbb{K}})$ to a word problem.

We start by giving the definitions of homogeneous linear-plus-conjugacy groups and extended homogeneous linear-plus-conjugacy groups, which are generalized from the definition of solution groups.

Definition 3.53 (Definition 31 of [7]). *Let A be an $m \times n$ matrix over $\mathbb{Z}_2$, and $C \subseteq$*

$[n] \times [n] \times [n]$. *Let*

$$\Gamma_0(A, C) := \langle \Gamma(A) : x_i x_j x_i = x_k \text{ for all } (i, j, k) \in C \rangle.$$

*We say that a group G is a **homogeneous-linear-plus-conjugacy group** if it has a presentation of this form.*

Definition 3.54 (Definition 32 of [7]). *Let A be an $m \times n$ matrix over $\mathbb{Z}_2$, let $C_0 \subseteq [n] \times [n] \times [n]$, let $C_1 \subseteq [l] \times [n] \times [n]$, and let L be an $l \times l$ lower-triangular matrix with non-negative integer entries. Let*

$$E\Gamma_0(A, C_0, C_1, L) := \langle \Gamma_0(A, C_0), y_0, \ldots, y_{l-1} : y_i^{-1} x_j y_i = x_k \text{ for all } (i, j, k) \in C_1,$$
$$y_i^{-1} y_j y_i = y_j^{L(i,j)} \text{ for all } i > j \text{ with } L(i, j) > 0 \rangle.$$

*We say a group G is an **extended homogeneous-linear-plus-conjugacy group** if it has a presentation of this form.*

Slofstra's fa^* embedding procedure has two steps, which are summarized in the two propositions below.

Proposition 3.55 (Proposition 33 of [7]). *Let G be an extended homogeneous linear-plus-conjugacy group. Then there is an fa^*-embedding $\phi : G \to H$ where H is a linear-plus-conjugacy group.*

Proposition 3.56 (Proposition 27 and Lemma 29 of [7]). *Let $G = \langle S : R \rangle$ be a linear-plus-conjugacy group. Then there is an fa^*-embedding $G \to \Gamma$, where $\Gamma = \langle S_\Gamma : R_\Gamma \rangle$ is a solution group.*

Note that Slofstra gives the explicit formulation of the two fa^*-embeddings above and the groups H and Γ. The steps of this embedding procedure can be found in Appendix B. For more details, we refer to [7, Section 4].

The combination of Propositions 3.55 and 3.56 gives us an fa^*-embedding, ϕ_{tot}, of an extended homogeneous linear-plus-conjugacy group G into a solution group $\Gamma = \langle S_\Gamma : R_\Gamma \rangle$. Moreover, if some generators in S are known to be nontrivial, the proofs of Propositions 3.55 and 3.56 in [7] allow us to identify a finite subset $S \subseteq S_\Gamma$ such that each $s \in S$ is also nontrivial in Γ. It implies that if G is hyperlinear, by Definition 3.40 and Lemma 3.48, each $s \in S$ is also nontrivial in approximate representations of Γ. For more details of this assertion, we refer to [7, Section 4].

To prove our main result, in one of the steps, we need to bound the trace of the image of each $w \in W$ in approximate representations, where W is a finite set and each $w \in W$ is known to be nontrivial in approximate representations. For this purpose, we introduce the following proposition.

Proposition 3.57. *Let $G = \langle S : R \rangle$ and W be a finite subset of $\mathcal{F}(S)$ such that the image of each $w \in W$ is nontrivial in approximate representations of G. Then, for every $\epsilon, \zeta > 0$, there is an ϵ-approximate representation ϕ with $0 \leq \widetilde{\mathrm{Tr}}(\phi(w)) \leq \zeta$ for each $w \in W$.*

This proposition is generalized from [7, Lemma 12].

Proof. Let ϕ_w be an ϵ_w-approximate representation of G such that $\|\phi_w(w) - \mathbb{1}\| \geq \delta_w$. By definition of approximate representations, such ϕ_w, ϵ_w and δ_w exist. Define

$\phi = \oplus_{w\in W}\phi_w$, then ϕ is an $\epsilon := \max_{w\in W}\epsilon_w$-approximate representation of G such that for each $w \in W$, $\|\phi(w) - \mathbb{1}\| \geq \delta_w/|W|$. Define $\delta := \min_{w\in W}\delta_w/|W|$, then,

$$\|\phi(w) - \mathbb{1}\| \geq \delta \text{ for all } w \in W.$$

Suppose the dimension of ϕ is d. Let $\overline{\phi}$ be the approximate representation obtained from ϕ by entry-wise complex conjugate of ϕ with respect to the standard basis of $\mathbb{C}^d$. Then, $\overline{\phi}$ is also an ϵ-approximate representation of G. Define $\gamma : G \to \mathcal{U}(\mathbb{C}^{4d})$ by

$$\gamma(g) = \phi(g) \oplus \overline{\phi}(g) \oplus \mathbb{1}_{\mathbb{C}^{2d}}.$$

Then γ is also an ϵ-approximate representation, and

$$\mathrm{Tr}(\gamma(w)) = \mathrm{Tr}(\phi(w)) + \overline{\mathrm{Tr}(\phi(w))} + 2d \geq 0$$
$$\|\gamma(w) - \mathbb{1}\|^2 = \|\phi(w) - \mathbb{1}\|^2/2 \geq \delta^2/2$$

for all $w \in W$. These two relations imply that

$$0 \leq \widetilde{\mathrm{Tr}}(\gamma(w)) = \mathrm{Re}\,\widetilde{\mathrm{Tr}}(\gamma(w)) \leq \frac{2 - \|\gamma(w) - \mathbb{1}\|^2}{2} \leq 1 - \frac{\delta^2}{4},$$

where we use the fact that for any unitary U, $\|U - \mathbb{1}\|^2 = 2 - 2\,\mathrm{Re}\,\widetilde{\mathrm{Tr}}(U)$.

Finally, we pick k such that $(1 - \delta^2/4)^k \leq \zeta$ for the given ζ. Then, by Lemma 3.37, $\phi^{\otimes k}$ is an $k\epsilon$-representation of G such that $0 \leq \widetilde{\mathrm{Tr}}(\phi^{\otimes k}(w)) \leq \zeta$

for all $w \in W$. Therefore, if we start with a ϵ/k-approximate representation ϕ, we get the required ϵ-approximate representation. $\square$

Chapter 4: Introduction to quantum correlations

We introduce quantum correlations formally in this chapter. In Section 4.1, we formally introduce the four sets of quantum correlations. In Section 4.2, we show that quantum correlations can tell us certain relations satisfied by the measurements with respect to the shared state. Such observations are going to be used in later chapters. Lastly, in Section 4.3, we introduce a correlation associated with a binary linear system, which can give us stronger relations satisfied by the measurements with respect to the shared state.

4.1 Four sets of quantum correlations

Consider a scenario involving a referee and two non-communicating participants, Alice and Bob, where each of them needs to give an answer for a question chosen from a fixed set of questions. This scenario is nonlocal and illustrated in the figure below.

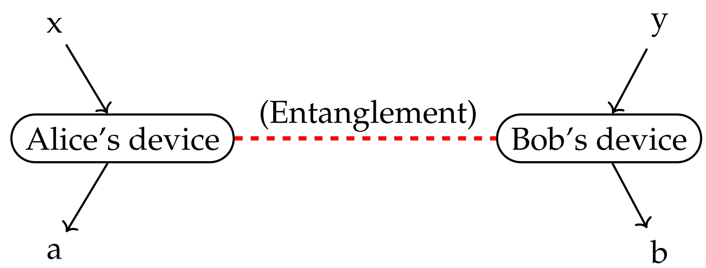

Figure 4.1: A nonlocal scenario between Alice and Bob with entanglement

Definition 4.1. *A* ***nonlocal scenario*** *is a tuple* $([n_A], [n_B], [m_A], [m_B])$*, where* n_A, n_B, m_A *and* m_B *are positive integers.* $[n_A]$ *is referred to as Alice's question set;* $[n_B]$ *is referred to as Bob's question set;* $[m_A]$ *is referred to as Alice's answer set; and* $[m_B]$ *is referred to as Bob's answer set.*

We are interested in the behaviour of Alice and Bob in this scenario. The behaviour of the two participants can be described by the joint conditional probability distribution of their answers for each pair of possible questions.

Definition 4.2. *A* ***bipartite correlation*** *of a nonlocal scenario* $([n_A], [n_B], [m_A], [m_B])$ *is a function* $P : [n_A] \times [n_B] \times [m_A] \times [m_B] \to \mathbb{R}_{\geq 0}$*, written as* $(i, j, k, l) \mapsto P(k, l|i, j)$ *where* $P(k, l|i, j)$ *is the probability for Alice to answer* k *and Bob to answer* l *when the question to Alice is* i *and to Bob is* j

Note that when we define quantum correlations in later chapters, we may label some questions with their corresponding group elements. In this case, the sets of questions may not be sets of integers, but the sets of questions in this dissertation are always finite and isomorphic to $[n]$ for some $n > 0$.

One way to view a correlation is to arrange the entries in a correlation matrix, where the columns are labelled by Alice's question-answer pairs and the rows are labelled by Bob's question-answer pairs. Then, the value at the intersection of row (j,l) and column (i,k) is $P(k,l|i,j)$. We give a simple example below.

(y,b) \ (x,a)	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$P(0,0\|0,0)$	$P(1,0\|0,0)$	$P(0,0\|1,0)$	$P(1,0\|1,0)$
$(0,1)$	$P(0,1\|0,0)$	$P(1,1\|0,0)$	$P(0,1\|1,0)$	$P(1,1\|1,0)$
$(1,0)$	$P(0,0\|0,1)$	$P(1,0\|0,1)$	$P(0,0\|1,1)$	$P(1,0\|1,1)$
$(1,1)$	$P(0,1\|0,1)$	$P(1,1\|0,1)$	$P(0,1\|1,1)$	$P(1,1\|1,1)$

Table 4.1: Example correlation matrix for a nonlocal scenario $([2],[2],[2],[2])$ with (x,a) labelling Alice's question-answer pair and (y,b) labelling Bob's question-answer pair.

Definition 4.3. *The **size of a correlation** $P : [n_A] \times [n_B] \times [m_A] \times [m_B] \to \mathbb{R}_{\geq 0}$ is the size of its correlation matrix, which equals $n_A n_B m_A m_B$.*

The size of the correlation given in Table 4.1 is 16.

We first introduce correlations induced by quantum spatial strategies with projective measurements.

Definition 4.4 (Projective measurement)**.** *For a Hilbert space $\mathcal{H}$, a set of projectors in $\mathcal{L}(\mathcal{H})$, $\{M_j \mid j \in [n]\}$, is a projective measurement if $M_i M_j = 0$ for all $i \neq j$ and $\sum_{j\in[n]} M_j = \mathbb{1}_{\mathcal{H}}$.*

Definition 4.5. *A **quantum spatial strategy with projective measurements** for a nonlocal scenario $([n_A],[n_B],[m_A],[m_B])$ is a tuple*

$$(|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{\{M_i^{(k)} \mid k \in [m_A]\} \mid i \in [n_A]\}, \{\{N_j^{(l)} \mid l \in [m_B]\} \mid j \in [n_B]\}),$$

where $\mathcal{H}_A$ and $\mathcal{H}_B$ are Hilbert spaces, $\{\{M_i^{(k)} \mid k \in [m_A]\} \mid i \in [n_A]\}$ is a set of *projective measurements on $\mathcal{H}_A$, and $\{\{N_j^{(l)} \mid l \in [m_B]\} \mid j \in [n_B]\}$ is a set of projective measurements on $\mathcal{H}_B$.*

Note that the tensor product structure emphasizes that the two parties cannot communicate with each other and that the projectors act on different Hilbert spaces (Fig. 4.1), which is the reason why we say the strategy is spatial.

When both $\mathcal{H}_A$ and $\mathcal{H}_B$ are finite-dimensional, we say the strategy is a *quantum finite-dimensional spatial strategy*. Otherwise, it is called a *quantum infinite-dimensional spatial strategy*. The correlation induced by a quantum spatial strategy is given by

$$P(k,l|i,j) = \langle \psi | M_i^{(k)} \otimes N_j^{(l)} | \psi \rangle$$

for all $i \in [n_A], j \in [n_B], k \in [m_A]$ and $l \in [m_B]$.

Definition 4.6. *The set $C_q(n_A, n_B, m_A, m_B)$ consists of all quantum correlations induced by quantum finite-dimensional spatial strategies with projective measurements of a nonlocal scenario $([n_A], [n_B], [m_A], [m_B])$.*

We can also define a relaxation of $C_q(n_A, n_B, m_A, m_B)$ by allowing infinite-dimensional strategies.

Definition 4.7. *The set $C_{qs}(n_A, n_B, m_A, m_B)$ consists of all quantum correlations induced by quantum finite-dimensional and infinite-dimensional spatial strategies with projective measurements of a nonlocal scenario $([n_A], [n_B], [m_A], [m_B])$.*

It is clear from the definitions that for each $([n_A], [n_B], [m_A], [m_B])$, $C_q(n_A,$

n_B, m_A, m_B) $\subseteq C_{qs}(n_A, n_B, m_A, m_B)$.

Definition 4.8. *The set $C_{qa}(n_A, n_B, m_A, m_B)$ is the set of correlations $P : [n_A] \times [n_B] \times [m_A] \times [m_B] \to \mathbb{R}_{\geq 0}$ such that for every $\epsilon > 0$ there exists a correlation $P_\epsilon \in C_{qs}(n_A, n_B, m_A, m_B)$ such that*

$$\max_{i\in[n_A], j\in[n_B], k\in[m_A], l\in[m_B]} |P(k,l|i,j) - P_\epsilon(k,l|i,j)| \leq \epsilon.$$

In other words, $C_{qa}(n_A, n_B, m_A, m_B)$ is the closure of $C_q(n_A, n_B, m_A, m_B)$. By the definition, we can also deduce that $C_{qs}(n_A, n_B, m_A, m_B) \subseteq C_{qa}(n_A, n_B, m_A, m_B)$.

A way to generalize the notion of quantum spatial strategy is to drop the requirement that the projective measurements act on different Hilbert spaces. Instead, we just require the projectors to commute.

Definition 4.9. *A* ***quantum commuting-operator strategy*** *of a nonlocal scenario $([n_A], [n_B], [m_A], [m_B])$ presented in terms of projective measurements is a tuple*

$$(|\psi\rangle \in \mathcal{H}, \{\{M_i^{(k)} \mid k \in [m_A]\} \mid i \in [n_A]\}, \{\{N_j^{(l)} \mid l \in [m_B]\} \mid j \in [n_B]\}),$$

where $\mathcal{H}$ is a Hilbert space, and $\{\{M_i^{(k)} \mid k \in [m_A]\} \mid i \in [n_A]\}$ and $\{\{N_j^{(l)} \mid l \in [m_B]\} \mid j \in [n_B]\}$ are two sets of projective measurements on $\mathcal{H}$ such that $M_i^{(k)} N_j^{(l)} = N_j^{(l)} M_i^{(k)}$ for all $i \in [n_A], j \in [n_B], k \in [m_A]$ and $l \in [m_B]$.

Here the Hilbert space $\mathcal{H}$ does not have to be finite-dimensional.

Proposition 4.10. *For a quantum spatial strategy*

$$(|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{\{M_i^{(k)} \mid k \in [m_A]\} \mid i \in [n_A]\}, \{\{N_j^{(l)} \mid l \in [m_B]\} \mid j \in [n_B]\}),$$

there exists a quantum commuting-operator strategy

$$(|\tilde{\psi}\rangle \in \mathcal{H}, \{\{\tilde{M}_i^{(k)} \mid k \in [m_A]\} \mid i \in [n_A]\}, \{\{\tilde{N}_j^{(l)} \mid l \in [m_B]\} \mid j \in [n_B]\})$$

such that $\langle\psi|M_i^{(k)} \otimes N_j^{(l)}|\psi\rangle = \langle\tilde{\psi}|\tilde{M}_i^{(k)}\tilde{N}_j^{(l)}|\tilde{\psi}\rangle$.

It suffices to choose $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, $|\tilde{\psi}\rangle = |\psi\rangle$, $\tilde{M}_i^{(k)} = M_i^{(k)} \otimes \mathbb{1}_{\mathcal{H}_B}$ and $\tilde{N}_j^{(l)} = \mathbb{1}_{\mathcal{H}_A} \otimes N_j^{(l)}$ and this proposition follows.

With quantum commuting-operator strategies we can define a larger set of quantum correlations.

Definition 4.11. *The set* $C_{qc}(n_A, n_B, m_A, m_B)$ *consists of all quantum correlations induced by quantum commuting-operator strategies of a scenario* $([n_A], [n_B], [m_A], [m_B])$.

By Proposition 4.10, we know that $C_{qs}(n_A, n_B, m_A, m_B) \subseteq C_{qc}(n_A, n_B, m_A, m_B)$. Since C_{qc} is its own closure [9, Theorem 4.3], we get that $C_{qa}(n_A, n_B, m_A, m_B) \subseteq C_{qc}(n_A, n_B, m_A, m_B)$. Combining the inclusion relations established so far, we reach a chain of inclusion

$$\begin{aligned} C_q(n_A, n_B, m_A, m_B) \subseteq C_{qs}(n_A, n_B, m_A, m_B) \\ \subseteq C_{qa}(n_A, n_B, m_A, m_B) \subseteq C_{qc}(n_A, n_B, m_A, m_B). \end{aligned}$$

Notationwise, when n_A, n_B, m_A and m_B are clear from context, we write C_t for $C_t(n_A, n_B, m_A, m_B)$ for $t \in \{q, qs, qa, qc\}$.

Definition 4.12. *A correlation $P : [n_A] \times [n_B] \times [m_A] \times [m_B] \to \mathbb{R}_{\geq 0}$ is **synchronous** if $n_A = n_B = n$, $m_A = m_B = m$, and*

$$\sum_{j \in [m]} P(j, j|i, i) = 1$$

for all $i \in [n]$.

For $t \in \{q, qs, qa, qc\}$, we can identify a subset of C_t, denoted by C_t^s which contains all the synchronous correlations in it.

4.2 Deriving operator-state relations from a correlation

Quantum correlation can tell us some weaker properties about the measurements and the quantum state by itself. In this section, we list some of such observations, which in turn will be used in self-testing proofs in chapter 5. When deriving such relations, we work in the commuting-operator model. We also omit the identity when only one projector from either Alice or Bob is applied. For example, $\langle \psi | M_i^{(k)} \cdot \mathbb{1} | \psi \rangle$ is written as $\langle \psi | M_i^{(k)} | \psi \rangle$.

Proposition 4.13 (Equivalence Test)**.** *Let $|\psi\rangle \in \mathcal{H}$ be a quantum state, and $\{M_j \mid j \in [n]\}$ and $\{N_j \mid j \in [n]\}$ be two commuting projective measurements on $\mathcal{H}$ for some*

$n \geq 2$. If $\langle \psi | M_j N_k | \psi \rangle = 0$ for all $j \neq k \in [n]$, then

$$M_j | \psi \rangle = N_j | \psi \rangle$$

for each $j \in [n]$.

Proof. Fix $j \in [n]$ and suppose that $\langle \psi | M_j N_j | \psi \rangle = x_j$ for some $x_j \geq 0$. We first calculate the norm of $M_j | \psi \rangle$, then the norm of $N_j | \psi \rangle$ follows easily.

$$\begin{aligned} \| M_j | \psi \rangle \|^2 =& \langle \psi | M_j | \psi \rangle \\ =& \langle \psi | M_j (\sum_{j \in [n]} N_j) | \psi \rangle \\ =& x_j + (j-1) \cdot 0 = x_j. \end{aligned}$$

From such calculations, we know

$$\| M_j | \psi \rangle \| = \| N_j | \psi \rangle \| = \sqrt{x_j}.$$

Then we will prove that $M_j | \psi \rangle = N_j | \psi \rangle$.

$$\begin{aligned} \| M_j | \psi \rangle - N_j | \psi \rangle \|^2 &= \langle \psi | (M_j - N_j)^2 | \psi \rangle \\ &= \langle \psi | M_j^2 | \psi \rangle + \langle \psi | N_j^2 | \psi \rangle - 2 \langle \psi | M_j N_j | \psi \rangle \\ &= x_j + x_j - 2x_j = 0. \end{aligned}$$

By the positivity of the vector norm, we know $M_j | \psi \rangle - N_j | \psi \rangle = 0$ for each $j \in$

$[n]$. $\square$

If we view the subscript j as Alice and Bob's answers, the condition of this proposition implies that the correlation generated by $(|\psi\rangle, \{M_j \mid j \in [n]\}, \{N_j \mid j \in [n]\})$ is synchronous.

Proposition 4.14. *Let $|\psi\rangle \in \mathcal{H}$ be a quantum state, $\{M_0^{(k)} \mid k \in [m_A]\}$ and $\{M_1^{(k)} \mid k \in [m_A]\}$ be two projective measurements on $\mathcal{H}$, both of which commute with the projective measurement $\{N^{(l,l')} \mid l, l' \in [m_A]\}$ on $\mathcal{H}$. If*

$$\langle\psi|M_0^{(k)} N^{(l,l')}|\psi\rangle = \langle\psi|M_1^{(k')} N^{(l,l')}|\psi\rangle = 0$$

for any $k \neq l$ and $k' \neq l'$, then

$$M_0^{(k)} M_1^{(k')}|\psi\rangle = M_1^{(k')} M_0^{(k)}|\psi\rangle$$

for any $k, k' \in [m_A]$.

Proof. The condition implies that the strategies

$$(|\psi\rangle, \{M_0^{(k)} \mid k \in [m_A]\}, \{\sum_{l' \in [m_A]} N^{(k,l')} \mid k \in [m_A]\}),$$

$$(|\psi\rangle, \{M_1^{(k')} \mid k' \in [m_A]\}, \{\sum_{l \in [m_A]} N^{(l,k')} \mid k' \in [m_A]\})$$

both satisfy the condition of Proposition 4.14, so we can derive that

$$M_0^{(k)}|\psi\rangle = \sum_{l'\in[m_A]} N^{(k,l')}|\psi\rangle,$$

$$M_1^{(k')}|\psi\rangle = \sum_{l\in[m_A]} N^{(l,k')}|\psi\rangle,$$

for each $k, k' \in [m_A]$. Then we can calculate that

$$\begin{aligned}
M_0^{(k)}M_1^{(k')}|\psi\rangle &= M_0^{(k)} \sum_{l\in[m_A]} N^{(l,k')}(|\psi\rangle = \sum_{l\in[m_A]} N^{(l,k')}M_0^{(k)}|\psi\rangle \\
&= \sum_{l\in[m_A]} N^{(l,k')} \sum_{l'\in[m_A]} N^{(k,l')}|\psi\rangle = N^{(k,k')}|\psi\rangle = \sum_{l'\in[m_A]} N^{(l',k)} \sum_{l\in[m_A]} N^{(l,k')}|\psi\rangle \\
&= M_1^{(k')} \sum_{l'\in[m_A]} N^{(l',k)}|\psi\rangle = M_1^{(k')}M_0^{(k)}|\psi\rangle,
\end{aligned}$$

for each $k, k' \in [m_A]$, where we repeatedly use the two equations above and the fact that the Alice and Bob's projectors commute. □

Lemma 4.15 (Substitution Lemma)**.** *Let $|\psi\rangle \in \mathcal{H}$ be a quantum state. Suppose there exist unitaries $\{V\} \cup \{V_i \mid i \in [k]\} \cup \{M_i \mid i \in [n]\}$ on $\mathcal{H}$ commuting with $\{N_i \mid i \in [n]\}$ on $\mathcal{H}$ such that*

$$M_i|\psi\rangle = N_i|\psi\rangle$$

for each $i \in [n]$, and

$$V|\psi\rangle = \prod_{i\in[k]} V_i|\psi\rangle.$$

Then,

$$V \prod_{i\in[n]} M_i|\psi\rangle = \left(\prod_{i\in[k]} V_i\right)\left(\prod_{i\in[n]} M_i\right)|\psi\rangle.$$

Proof. We prove this lemma by induction on n. The $n = 0$ case follows the condition that $V|\psi\rangle = \prod_{i\in[k]} V_i|\psi\rangle$.

Assume the conclusion holds for $n = m$. Consider the case $n = m + 1$, then

$$\begin{aligned}
V \prod_{i\in[m+1]} M_i|\psi\rangle &= V\left(\prod_{i\in[m]} M_i\right) M_m|\psi\rangle = V\left(\prod_{i\in[m]} M_i\right) N_m|\psi\rangle \\
&= N_m V\left(\prod_{i\in[m]} M_i\right)|\psi\rangle = N_m\left(\prod_{i\in[k]} V_i\right)\left(\prod_{i\in[m]} M_i\right)|\psi\rangle \\
&= \left(\prod_{i\in[k]} V_i\right)\left(\prod_{i\in[m]} M_i\right) N_m|\psi\rangle = \left(\prod_{i\in[k]} V_i\right)\left(\prod_{i\in[m+1]} M_i\right)|\psi\rangle.
\end{aligned}$$

By the principle of inductive proof, the proof is complete. □

4.3 A correlation associated with a binary linear system

In this section, we study a correlation induced by a representation of a solution group, which will be shown to be a perfect correlation associated with the corresponding linear system as defined below.

Definition 4.16. *Let $A\boldsymbol{x} = 0$ be a binary linear system where each row has κ nonzero* *entries. For each $i \in [m]$, we define* [1]

$$I_i = \{j \in [n] \mid A(i,j) = 1\}$$

$$S_i = \{\boldsymbol{x} \in \mathbb{Z}_2^{I_i} \cong \mathbb{Z}_2^{\kappa} \mid \sum_{j \in I_i} \boldsymbol{x}(j) \equiv 0 \pmod 2\}.$$

A correlation $P : [m+n] \times [m+n] \times \mathbb{Z}_2^{\kappa} \times \mathbb{Z}_2^{\kappa}$ is a ***perfect correlation*** *associated with $A\boldsymbol{x} = 0$ if*

P.1 *when $i > m$, $P(x,y|i,j) = 0$ if $x > 1$* [2]*;*

P.2 *when $j > m$, $P(x,y|i,j) = 0$ if $y > 1$;*

P.3 *when $i,j \in [m]$, $P(\boldsymbol{x},\boldsymbol{y}|i,j) = 0$ when $\boldsymbol{x} \notin S_i$, or $\boldsymbol{y} \notin S_j$, or there exists $k \in I_i \cap I_j$ such that $\boldsymbol{x}(k) \neq \boldsymbol{y}(k)$;*

P.4 *when $i > m$, $j \in [m]$ and $i - m \in I_j$,*

$$\sum_{\boldsymbol{y} \in S_j} P(\boldsymbol{y}(i-m), \boldsymbol{y}|i,j) = 1;$$

P.5 *when $j > m$, $i \in [m]$ and $j - m \in I_i$,*

$$\sum_{\boldsymbol{x} \in S_i} P(\boldsymbol{x}, \boldsymbol{x}(j-m)|i,j) = 1; \text{ and}$$

P.6 *when $i > m$, $P(0,0|i,i) + P(1,1|i,i) = 1$.*

[1] The isomorphism between $\mathbb{Z}_2^{I_i}$ and $\mathbb{Z}_2^{\kappa}$ is extended from the map $\phi_i : I_i \to [\kappa]$ that map the smallest $j \in I_i$ to 0, the second smallest to 1, and etc..

[2] Here, we fix a natural isomorphism between $\mathbb{Z}_2^{\kappa}$ and $[2^{\kappa}]$.

Intuitively, the correlation requires that whenever Alice or Bob gets a question $i \in [m]$, they need to give a satisfying assignment of equation i. That is, their answer should be from S_i. The correlation also requires that whenever Alice or Bob gets a question $j > m$, they need to give an assignment to the variable x_{j-m}. That is, their answer should be from $\{0,1\}$, as required by **P.1** and **P.2**. More specifically, **P.3** requires that when Alice and Bob get questions $i, j \in [m]$, they not only need to give satisfying assignments, their assignment to the common variable in both equations should be consistent; **P.4** and **P.5** require that when one party gives an assignment to some equation and the other party gives an assignment to a variable in the equation, the equation assignment should be satisfying and the variable assignment should be consistent between the two parties; and **P.6** requires that when both parties assign values to a common variable, their assignments should always be consistent.

Next, we define the correlation induced by the regular representation of a solution group. For a binary linear system $A\boldsymbol{x} = 0$, let L and R be the left and right representation of $\Gamma(A)$ respectively. Define projectors

$$M_i^{(\boldsymbol{x})} = \begin{cases} \prod_{j\in I_i}\left(\frac{\mathbb{1}+(-1)^{\boldsymbol{x}(j)}L(x_j)}{2}\right) & \text{if } i\in[m], \boldsymbol{x}\in S_i \\ \frac{\mathbb{1}+(-1)^{\boldsymbol{x}}L(x_{i-m})}{2} & \text{if } \boldsymbol{x}\in[2], \\ 0 & \text{otherwise;} \end{cases}$$

$$N_i^{(\boldsymbol{x})} = \begin{cases} \prod_{j\in I_i}\left(\frac{\mathbb{1}+(-1)^{\boldsymbol{x}(j)}R(x_j)}{2}\right), & \text{if } i\in[m], \boldsymbol{x}\in S_i \\ \frac{\mathbb{1}+(-1)^{\boldsymbol{x}}R(x_{i-m})}{2} & \text{if } \boldsymbol{x}\in[2], \\ 0 & \text{otherwise.} \end{cases}$$

Since $\prod_{j\in I_i}\rho(x_j)=\mathbb{1}$, we know $\{M_i^{(\boldsymbol{x})} \mid \boldsymbol{x}\in S_i\}$ and $\{N_i^{(\boldsymbol{x})} \mid \boldsymbol{x}\in S_i\}$ are projective measurements for each $i\in[m]$. Then the projective measurement strategy is

$$S_\rho = (|e\rangle \in \ell^2\Gamma(A), \{\{M_i^{(\boldsymbol{x})} \mid \boldsymbol{x}\in\mathbb{Z}_2^\kappa\} \mid i\in[m+n]\}, \{\{N_i^{(\boldsymbol{x})} \mid \boldsymbol{x}\in\mathbb{Z}_2^\kappa\} \mid i\in[m+n]\}),$$

and the induced quantum correlation $P_A : [m+n]\times[m+n]\times\mathbb{Z}_2^\kappa\times\mathbb{Z}_2^\kappa \to \mathbb{R}$ is defined by

$$P_A(\boldsymbol{x},\boldsymbol{y}|i,j) = \langle e|M_i^{(\boldsymbol{x})}N_j^{(\boldsymbol{y})}|e\rangle$$

for $i,j\in[m+n]$ and $\boldsymbol{x}\in\mathbb{Z}_2^\kappa, \boldsymbol{y}\in\mathbb{Z}_2^\kappa$.

Proposition 4.17. *The correlation P_A defined above is a perfect correlation associated with $A\boldsymbol{x}=0$.*

Proof. By the definition of P_A, when $i, j \in [m]$, it is easy to see that $P_A(\boldsymbol{x}, \boldsymbol{y}|i, j) = 0$ if $\boldsymbol{x} \notin S_i$ or $\boldsymbol{y} \notin S_j$. Next, consider $\boldsymbol{x} \in S_i$ and $\boldsymbol{y} \in S_j$ such that there exists $k_0 \in I_i \cap I_j$ and $\boldsymbol{x}(k_0) \neq \boldsymbol{y}(k_0)$. Without loss of generality, we can assume $\boldsymbol{x}(k_0) = 0$ and $\boldsymbol{y}(k_0) = 1$. Then, the expression of $P_A(\boldsymbol{x}, \boldsymbol{y}|i, j)$ contains the term

$$\frac{\mathbb{1} + L(x_{k_0})}{2} \frac{\mathbb{1} - R(x_{k_0})}{2} |e\rangle = \frac{1}{4}(|e\rangle + |x_{k_0}\rangle - |x_{k_0}\rangle - |e\rangle) = 0.$$

Hence, for any $i, j \in [m]$, if there exists $k_0 \in I_i \cap I_j$ such that $\boldsymbol{x}(k_0) \neq \boldsymbol{y}(k_0)$, then $P_A(\boldsymbol{x}, \boldsymbol{y}|i, j) = 0$.

Again, by the definition of P_A, it is easy to see that when $i > m$, $P_A(0, 0|i, i) + P_A(1, 1|i, i) = 1$. When $i \in [m]$, $j > m$ and $j - m \in I_i$, then

$$\sum_{\boldsymbol{x} \in S_i} P_A(\boldsymbol{x}, \boldsymbol{x}(j-m)|i, j) = \sum_{\boldsymbol{x} \in S_i} \langle e| \prod_{k \in I_i} \frac{\mathbb{1} + (-1)^{\boldsymbol{x}(k)} L(x_k)}{2} |e\rangle = 1,$$

where we use the fact that

$$\left[\frac{\mathbb{1} + (-1)^y L(x_{j-m})}{2}\right] \left[\frac{\mathbb{1} + (-1)^y R(x_{j-m})}{2}\right] |\psi\rangle = \frac{\mathbb{1} + (-1)^y L(x_{j-m})}{2} |e\rangle.$$

This is also true if we switch i and j, which can be proved analogously, so the proof is complete. □

In the next lemma, we study the implication of a correlation being a perfect correlation associated with a binary linear system $A\boldsymbol{x} = 0$. First, we establish some facts about commuting projectors.

Proposition 4.18. *Let $\{M_i \mid i \in [n]\}$ be a commuting set of projectors on $\mathcal{H}$ and $|\psi\rangle \in \mathcal{H}$. Then, $\prod_{i\in[n]} M_i|\psi\rangle = |\psi\rangle$ if and only if $M_i|\psi\rangle = |\psi\rangle$ for each $i \in [n]$.*

Proof. First of all, if $M_i|\psi\rangle = |\psi\rangle$ for each $i \in [n]$, then it is easy to see that $\prod_{i\in[n]} M_i|\psi\rangle = |\psi\rangle$. In the other direction, we can see that

$$\begin{aligned}\|M_0|\psi\rangle - \prod_{0<l<n} M_l|\psi\rangle\|^2 =& \langle\psi|M_0|\psi\rangle + \langle\psi|\prod_{0<l<n} M_l|\psi\rangle - 2\langle\psi|\prod_{i\in[n]} M_i|\psi\rangle \\ =& \langle\psi|M_0|\psi\rangle + \langle\psi|\prod_{0<l<n} M_l|\psi\rangle - 2.\end{aligned}$$

Since $\|M_0|\psi\rangle - \prod_{0<l<n} M_l|\psi\rangle\|^2 \geq 0$, $\langle\psi|M_0|\psi\rangle \leq 1$, and $\langle\psi|\prod_{0<l<n} M_l|\psi\rangle \leq 1$, we know

$$M_0|\psi\rangle = |\psi\rangle \qquad\qquad \langle\psi|\prod_{0<l<n} M_l|\psi\rangle = 1.$$

Then we can repeat this process to conclude that $M_i|\psi\rangle = |\psi\rangle$ for each $i \in [n]$. $\square$

Lemma 4.19. *For an $m \times n$ binary linear system $A\boldsymbol{x} = 0$, suppose that a commuting-operator strategy*

$$S = (|\psi\rangle \in \mathcal{H}, \{\{M_i^{(\boldsymbol{x})} \mid \boldsymbol{x} \in \mathbb{Z}_2^\kappa\} \mid i \in [m+n]\}, \{\{N_i^{(\boldsymbol{x})} \mid \boldsymbol{x} \in \mathbb{Z}_2^\kappa\} \mid i \in [m+n]\})$$

can induce a perfect correlation P_A associated with $A\boldsymbol{x} = 0$. Let $M_j := M_{j+m}^{(0)} - M_{j+m}^{(1)}$ and $N_j := N_{j+m}^{(0)} - N_{j+m}^{(1)}$ for $j \in [n]$. Then, for each $j \in [n]$,

$$M_j|\psi\rangle = N_j|\psi\rangle,$$

for each $i \in [m]$ and $k, l \in I_i$

$$M_k M_l |\psi\rangle = M_l M_k |\psi\rangle,$$

$$N_k N_l |\psi\rangle = N_l N_k |\psi\rangle,$$

and

$$\prod_{k \in I_i} M_k |\psi\rangle = \prod_{k \in I_i} N_k |\psi\rangle = |\psi\rangle.$$

Proof. Since when $i, j \in [m]$, $P_A(\boldsymbol{x}, \boldsymbol{y}|i, j) = 0$ for all $\boldsymbol{y}$, when $\boldsymbol{x} \notin S_i$, we know that $M_i^{(\boldsymbol{x})}|\psi\rangle = 0$ for all $\boldsymbol{x} \notin S_i$. Similarly, $N_j^{(\boldsymbol{y})}|\psi\rangle = 0$ for all $\boldsymbol{y} \notin S_j$. We define

$$M_{i,k} = \sum_{\boldsymbol{x} \in S_i : \boldsymbol{x}(k)=0} M_i^{(\boldsymbol{x})} - \sum_{\boldsymbol{x} \in S_i : \boldsymbol{x}(k)=1} M_i^{(\boldsymbol{x})},$$

$$N_{j,l} = \sum_{\boldsymbol{y} \in S_j : \boldsymbol{y}(l)=0} N_j^{(\boldsymbol{x})} - \sum_{\boldsymbol{y} \in S_j : \boldsymbol{y}(l)=1} N_j^{(\boldsymbol{x})},$$

for all $i, j \in [m]$ and $k \in I_i, l \in I_j$, and we can check that $M_{i,k}^2|\psi\rangle = N_{j,l}^2|\psi\rangle = |\psi\rangle$, and that $[M_{i,k}, M_{i,l}] = [N_{i,k}, N_{i,l}] = \mathbb{1}$ for all $i \in [m]$ and $k, l \in I_i$.

In the proof, we first establish the properties satisfied by $M_{i,k}$ and $N_{i,k}$ with respect to $|\psi\rangle$. Then, we prove that $M_k|\psi\rangle = M_{i,k}|\psi\rangle$ and $N_k|\psi\rangle = N_{i,k}|\psi\rangle$ for all i such that $k \in I_i$.

Let's fix a question pair (i, j) and assume $I_i \cap I_j = \{k_l \mid l \in [\alpha]\}$. Define

$\Pi_{k_l} = \sum_{\boldsymbol{x},\boldsymbol{y}:\boldsymbol{x}(k_l)=\boldsymbol{y}(k_l)} M_i^{(\boldsymbol{x})} N_j^{(\boldsymbol{y})}$ for each $l \in [\alpha]$. The fact that

$$\sum_{\boldsymbol{x},\boldsymbol{y}:\boldsymbol{x}(k_l)=\boldsymbol{y}(k_l) \text{ for all } l} P_A(\boldsymbol{x},\boldsymbol{y}|i,j) = 1$$

implies that $\langle\psi| \prod_{l\in[\alpha]} \Pi_{k_l} |\psi\rangle = 1$. By the previous proposition, we know

$$\Pi_{k_l}|\psi\rangle = |\psi\rangle \text{ for all } l \in [\alpha].$$

On the other hand, since $M_{i,k_l}N_{j,k_l}|\psi\rangle = 2\Pi_{k_l}|\psi\rangle - |\psi\rangle = |\psi\rangle$. we know that

$$\begin{aligned}
&\|M_{i,k_l}|\psi\rangle - N_{j,k_l}|\psi\rangle\|^2 \\
=&\langle\psi|M_{i,k_l}^2|\psi\rangle + \langle\psi|N_{j,k_l}^2|\psi\rangle - 2\langle\psi|M_{i,k_l}N_{j,k_l}|\psi\rangle \\
=&1+1-2=0,
\end{aligned}$$

which implies that $M_{i,k_l}|\psi\rangle = N_{j,k_l}|\psi\rangle$ for all $l \in [\alpha]$.

Also, notice that

$$\prod_{k\in I_i} M_{i,k} = \sum_{\boldsymbol{x}\in S_i} (-1)^{\sum_{k\in I_i}\boldsymbol{x}(k)} M_i^{(\boldsymbol{x})} = \sum_{\boldsymbol{x}\in S_i} M_i^{(\boldsymbol{x})}.$$

Because $\sum_{\boldsymbol{x}\notin S_i} M_i^{(\boldsymbol{x})}|\psi\rangle = 0$, we know

$$\prod_{k\in I_i} M_{i,k}|\psi\rangle = \sum_{\boldsymbol{x}\in S_i} M_i^{(\boldsymbol{x})}|\psi\rangle + \sum_{\boldsymbol{x}\notin S_i} M_i^{(\boldsymbol{x})}|\psi\rangle = \sum_{\boldsymbol{x}\in\mathbb{Z}_2^\kappa} M_i^{(\boldsymbol{x})}|\psi\rangle = |\psi\rangle.$$

With similar reasoning, we can conclude that $\prod_{l\in I_j} N_{j,l}|\psi\rangle = |\psi\rangle$ too.

By Property **P.1** and **P.2**, we know $M_{k+m}^{(x)}|\psi\rangle = N_{k+m}^{(x)}|\psi\rangle = 0$ for all $x > 1$ and $k \in [n]$. Therefore,

$$M_k^2|\psi\rangle = (M_{k+m}^{(0)} + M_{k+m}^{(1)})|\psi\rangle = \sum_{x\in[2^\kappa]} M_{k+m}^{(x)}|\psi\rangle = |\psi\rangle,$$

and similarly, $N_k^2|\psi\rangle = |\psi\rangle$. By Property **P.6** and Proposition 4.13, we know that $M_j|\psi\rangle = N_j|\psi\rangle$. Observe that

$$\langle\psi|M_{i,k}N_k|\psi\rangle = 2\sum_{\boldsymbol{x}\in S_i} P_A(\boldsymbol{x},\boldsymbol{x}(k)|i,k+m) - 1 = 1.$$

Then, we can use the same argument, which shows $M_{i,k}|\psi\rangle = N_{i,k}|\psi\rangle$, to show that $M_{i,k}|\psi\rangle = N_k|\psi\rangle$ for all $i \in [m]$. Analogously, we can get that $M_k|\psi\rangle = N_{i,k}|\psi\rangle$ for all $i \in [m]$. Combining the equations together, we get that

$$M_{i,k}|\psi\rangle = N_k|\psi\rangle = M_k|\psi\rangle = N_{i,k}|\psi\rangle.$$

Then, the commutation relation $M_{i,k}M_{i,l}|\psi\rangle = M_{i,l}M_{i,k}|\psi\rangle$ implies that

$$\begin{aligned} &M_kM_l|\psi\rangle = M_kN_l|\psi\rangle = N_lM_{i,k}|\psi\rangle = M_{i,k}M_{i,l}|\psi\rangle \\ =&M_{i,l}M_{i,k}|\psi\rangle = M_lM_k|\psi\rangle. \end{aligned}$$

On Bob's side, we can also get that $N_kN_l|\psi\rangle = N_lN_k|\psi\rangle$ if there exists i such that

$k, l \in I_i$. With similar reasoning, we can also get that

$$\prod_{k \in I_i} M_k |\psi\rangle = \prod_{k \in I_i} N_k |\psi\rangle = |\psi\rangle,$$

for all $i \in [m]$. $\square$

Chapter 5: Constant-sized self-tests of maximally entangled states of unbounded dimension

This chapter focuses on a unique phenomenon of quantum correlations – self-tests.

Definition 5.1. *We say a correlation $P : [n_A] \times [n_B] \times [m_A] \times [m_B] \to \mathbb{R}_{\geq 0}$ is a **self-test** of a quantum state $|\tilde{\psi}\rangle$, if for any quantum inducing strategy of P with shared state $|\psi\rangle$, there exist local isometries Φ_A, Φ_B and a quantum state $|junk\rangle$ such that*

$$\Phi_A \otimes \Phi_B(|\psi\rangle) = |\tilde{\psi}\rangle \otimes |junk\rangle.$$

Note that in the literature, some correlations are shown to be strong enough to self-test both the local measurements and the quantum state. For this dissertation, it suffices to focus on self-testing of the quantum state.

The main results of this chapter and the following chapters are based on a number theory result first proved in [27].

Lemma 5.2. *There exists $r \in \{2, 3, 5\}$ such that r is a primitive root of infinitely many primes.*

In Section 5.1, we introduce a correlation $Q_\mu : [2] \times [2] \times [2] \times [2] \to \mathbb{R}_{\geq 0}$

which is not only a self-test of $|EPR\rangle$ and can also certify certain operator-state relations. A key component of the proof of the self-testing property of Q_μ is the qubit swap-isometry. In Section 5.2, we present a generalized swap-isometry and give the sufficient conditions for using it to prove self-tests of general d-dimensional maximally entangled states. In Section 5.3, we introduce $\hat{Q}_{-\pi/p}$, which is designed based on $Q_{-\pi/p}$. Then, in Section 5.4, we construct $Q_{p,r}$ based on $\hat{Q}_{-\pi/p}$, which can self-test a $(p-1)$-dimensional maximally entangled state. The set $\{Q_{p,r}\}$, where $r \in \{2,3,5\}$ is a primitive root of infinitely many primes, allows us to assert that constant-sized correlations can self-test maximally entangled states of unbounded dimension.

5.1 The correlation Q_μ

We first give the inducing strategy of the correlation. Let $\mu \in [-\pi, \pi)$. Define

$$\tilde{M}_0^{(0)} = |0\rangle\langle 0|, \qquad \tilde{M}_0^{(1)} = |1\rangle\langle 1|,$$
$$\tilde{M}_1^{(0)} = \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|), \qquad \tilde{M}_1^{(1)} = \mathbb{1} - P_1^{(0)},$$

and

$$\begin{aligned}
\tilde{N}_0^{(0)} =&(\cos(\frac{\mu}{2})|0\rangle + \sin(\frac{\mu}{2})|1\rangle)(\cos(\frac{\mu}{2})\langle 0| + \sin(\frac{\mu}{2})\langle 1|),\\
\tilde{N}_0^{(1)} =&\mathbb{1} - Q_0^{(0)},\\
\tilde{N}_1^{(0)} =&(\cos(\frac{\mu}{2})|0\rangle - \sin(\frac{\mu}{2})|1\rangle)(\cos(\frac{\mu}{2})\langle 0| - \sin(\frac{\mu}{2})\langle 1|),\\
\tilde{N}_1^{(1)} =&\mathbb{1} - Q_1^{(0)}.
\end{aligned}$$

Definition 5.3. *The correlation $Q_\mu : [2] \times [2] \times [2] \times [2] \to \mathbb{R}$ is induced by the strategy*

$$(|EPR\rangle, \{\{\tilde{M}_x^{(a)} \mid a \in [2]\} \mid x \in [2]\}, \{\{\tilde{N}_y^{(b)} \mid b \in [2]\} \mid y \in [2]\}),$$

such that $Q_\mu(a, b|x, y) = \langle EPR|\tilde{M}_x^{(a)} \otimes \tilde{N}_y^{(b)}|EPR\rangle$.

The self-testing property of Q_μ is summarized in the following Lemma, which is first proved in [38, Proposition A.3].

Lemma 5.4. *For $\mu \in [-\pi, \pi)$, If a quantum strategy*

$$(|\psi\rangle, \{\{M_x^{(a)} \mid a \in [2]\} \mid x \in [2]\}, \{\{N_y^{(b)} \mid y \in [2]\} \mid b \in [2]\})$$

can induce Q_μ, then there exist a local isometry $\Phi = \Phi_A \otimes \Phi_B$ and an auxiliary state $|junk\rangle$ such that

$$\Phi(|\psi\rangle) = |junk\rangle \otimes |EPR\rangle.$$

Our proof is based on techniques borrowed from [19, Appendix A]. Before we give the proof, we highlight some of the important operator-state relations derived in the proof, which will be reused later. The notation of the relations and the proof follows the convention of [19]. which defines $M_x := M_x^{(0)} - M_x^{(1)}$, $N_y := N_y^{(0)} - N_y^{(1)}$ for $x, y \in [2]$ and

$$Z_A := M_0 \qquad\qquad X_A := M_1 \tag{5.1}$$

$$Z_B := \frac{N_0 + N_1}{2\cos\mu} \qquad\qquad X_B := \frac{N_0 - N_1}{2\sin\mu}. \tag{5.2}$$

The key relations are

$$Z_A|\psi\rangle = Z_B|\psi\rangle, \tag{5.3}$$

$$X_A|\psi\rangle = X_B|\psi\rangle, \tag{5.4}$$

$$X_A(\mathbb{1} + Z_B)|\psi\rangle = X_B(\mathbb{1} - Z_A)|\psi\rangle, \tag{5.5}$$

$$Z_A(\mathbb{1} + X_B)|\psi\rangle = Z_B(\mathbb{1} - X_A)|\psi\rangle, \tag{5.6}$$

$$Z_A X_A|\psi\rangle = -X_A Z_A|\psi\rangle, \tag{5.7}$$

$$X_A Z_A|\psi\rangle = -X_B Z_B|\psi\rangle. \tag{5.8}$$

Proof. The first step is to find a sum-of-square decomposition of the following expression

$$S = \frac{2}{\sin(\mu)}\mathbb{1} - \frac{\cos(\mu)}{\sin(\mu)}(M_1N_1 + M_1N_2) - M_2N_1 + M_2N_2.$$

Substituting in the values of Q_μ, we can see that $\langle\psi|S|\psi\rangle = 0$.

With the notation $c := \cos(\mu)$, $s := \sin(\mu)$, Z_A, X_A and Z_B, X_B as in eqs. (5.1) and (5.2). The two sum-of-squares decompositions of S are

$$S = \frac{sS^2 + 4sc^2(Z_A X_B + X_A Z_B)^2}{4}, \tag{5.9}$$

$$S = \frac{c^2}{s}(Z_A - Z_B)^2 + s(X_A - X_B)^2. \tag{5.10}$$

From the sum-of-square decompositions, we first prove eqs. (5.3) to (5.8). Define

$$T_1 = \frac{\sqrt{s}}{2}S, \qquad T_2 = \sqrt{s}c(Z_A X_B + X_A Z_B),$$
$$T_3 = \frac{c}{\sqrt{s}}(Z_A - Z_B), \qquad T_4 = \sqrt{s}(X_A - X_B)$$

then

$$S = T_1^2 + T_2^2 = T_3^2 + T_4^2. \tag{5.11}$$

The fact that the quantum strategy induces Q_μ implies that

$$\langle\psi|T_i^2|\psi\rangle = \|T_i|\psi\rangle\|^2 = 0 \iff T_i|\psi\rangle = 0$$

for $i = 1, 2, 3, 4$. From the definitions of T_i's and the positivity of vector norms, we can get that

$$(X_A Z_B + X_B Z_A)|\psi\rangle = 0 \tag{5.12}$$

$$(Z_A - Z_B)|\psi\rangle = 0 \tag{5.13}$$

$$(X_A - X_B)|\psi\rangle = 0, \tag{5.14}$$

which proves eqs. (5.3) and (5.4). Equations (5.12) and (5.13) give us that

$$[Z_A(\mathbb{1} + X_B) - (\mathbb{1} - X_A)Z_B]|\psi\rangle = (X_A Z_B + X_B Z_A)|\psi\rangle + (Z_A - Z_B)|\psi\rangle = 0,$$

which proves eq. (5.5). Similarly, eqs. (5.12) and (5.14) give us that

$$[X_A(\mathbb{1} + Z_B) - X_B(\mathbb{1} - Z_A)]|\psi\rangle = 0,$$

which proves eq. (5.6). Since $Z_A X_A + X_A Z_A = \frac{T_2}{c\sqrt{s}} + \frac{\sqrt{s} X_A T_3}{c} + \frac{Z_A T_4}{\sqrt{s}}$, we can deduce that

$$(Z_A X_A + X_A Z_A)|\psi\rangle = 0,$$

as in eq. (5.7). Lastly, to prove eq. (5.8), we notice that

$$X_A Z_A|\psi\rangle = -Z_A X_A|\psi\rangle = -Z_A X_B|\psi\rangle = -X_B Z_B|\psi\rangle.$$

Now we introduce the isometries Φ_A and Φ_B mentioned in the theorem, which are almost the same as the ones used in [19]. We first prove that we don't need to regularize Z_B and X_B because they are binary observables with respect to $|\psi\rangle$. We can use $Z_A|\psi\rangle = Z_B|\psi\rangle$ to prove that

$$Z_B^2|\psi\rangle = Z_A^2|\psi\rangle = |\psi\rangle.$$

With similar reasoning, we can see that X_B is also a binary observable with respect to $|\psi\rangle$.

The local isometry is illustrated in the figure below and it is known as *the swap-isometry*.

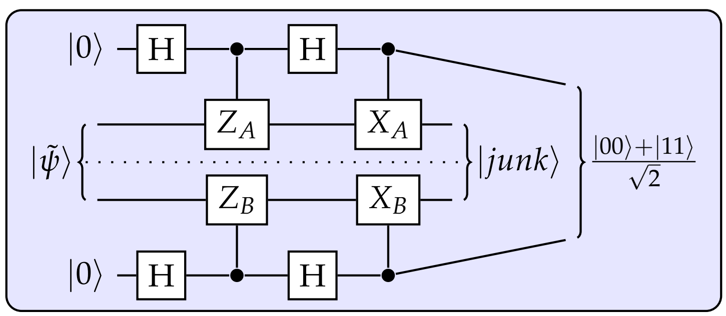

Figure 5.1: The qubit swap-isometry.

Then the proof follows from the observation that

$$\begin{aligned}\Phi_A \otimes \Phi_B(|\psi\rangle) =& \frac{1}{4}[(\mathbb{1} + Z_A)(1 + Z_B)|\psi\rangle|00\rangle + X_A(\mathbb{1} + Z_A)(1 - Z_B)|\psi\rangle|01\rangle \\ & + X_B(\mathbb{1} - Z_A)(1 + Z_B)|\psi\rangle|10\rangle + X_A X_B(\mathbb{1} - Z_A)(1 - Z_B)|\psi\rangle|11\rangle] \\ =& \frac{1}{2}(\mathbb{1} + Z_A)|\psi\rangle|00\rangle + \frac{1}{2}X_A X_B(\mathbb{1} - Z_A)|\psi\rangle|11\rangle \\ =& \frac{\sqrt{2}}{2}(\mathbb{1} + Z_A)|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),\end{aligned}$$

where we used the facts that $X_A X_B(\mathbb{1} - Z_A)|\psi\rangle = (\mathbb{1} + Z_A)|\psi\rangle$ proved below, and the fact $(\mathbb{1} + Z_A)(1 - Z_B)|\psi\rangle = (\mathbb{1} - Z_A)(1 + Z_B)|\psi\rangle = 0$.

$$
\begin{aligned}
X_A X_B(\mathbb{1} - Z_A)|\psi\rangle &= X_B(X_A - X_A Z_A)|\psi\rangle = X_B(X_A + Z_A X_A)|\psi\rangle \\
&= X_B(\mathbb{1} + Z_A)X_A|\psi\rangle = X_B^2(\mathbb{1} + Z_A)|\psi\rangle \\
&= (\mathbb{1} + Z_B)|\psi\rangle,
\end{aligned}
$$

which completes the proof. □

Our key observation about Q_μ is that it allows us to determine some eigenvalues of $N_0 N_1$, which is formally stated in the following proposition.

Proposition 5.5. *For $\mu \in [-\pi, \pi)$, if a quantum strategy $(|\psi\rangle \in \mathcal{H}, \{\{M_x^{(a)} \mid a \in [2]\} \mid x \in [2]\}, \{\{N_y^{(b)} \mid b \in [2]\} \mid y \in [2]\})$ can induce Q_μ, then there exist quantum states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$ such that $\||\psi_1\rangle\| = \||\psi_2\rangle\| = 1$ and*

$$
\begin{aligned}
N_0 N_1|\psi_1\rangle &= e^{-i2\mu}|\psi_1\rangle, \\
N_0 N_1|\psi_2\rangle &= e^{i2\mu}|\psi_2\rangle.
\end{aligned}
$$

Proof. The states are

$$|\psi_1\rangle = (M_0^{(0)} + iM_1 M_0^{(1)})|\psi\rangle, \tag{5.15}$$

$$|\psi_2\rangle = (M_0^{(0)} - iM_1 M_0^{(1)})|\psi\rangle. \tag{5.16}$$

We first show that $\||\psi_1\rangle\| = 1$.

$$\begin{aligned}\||\psi_1\rangle\|^2 =& \langle\psi|(M_0^{(0)} + M_0^{(1)} - iM_0^{(1)}M_1M_0^{(0)} + iM_0^{(0)}M_1M_0^{(1)})|\psi\rangle \\ =& 1 - i\langle\psi|M_0^{(1)}M_1M_0^{(0)} - M_0^{(0)}M_1M_0^{(1)}|\psi\rangle.\end{aligned}$$

Recall that $Z_A = M_0$, $X_A = M_1$, $Z_B = (N_0 + N_1)/2\cos(\mu)$ and $X_B = (N_0 - N_1)/2\sin(\mu)$. Using eqs. (5.4) and (5.8), we know

$$\begin{aligned}M_1M_0^{(0)}|\psi\rangle =& \frac{X_A(\mathbb{1} + Z_A)}{2}|\psi\rangle \\ =& \frac{X_B(\mathbb{1} - Z_B)}{2}|\psi\rangle \\ =& \frac{(\mathbb{1} + Z_B)X_B}{2}|\psi\rangle \\ M_0^{(1)}|\psi\rangle =& \frac{\mathbb{1} - Z_A}{2}|\psi\rangle \\ =& \frac{\mathbb{1} - Z_B}{2}|\psi\rangle,\end{aligned}$$

so $\langle\psi|M_0^{(1)}M_1M_0^{(0)}|\psi\rangle = 0$. With similar reasoning, we get $\langle\psi|M_0^{(0)}M_1M_0^{(1)}|\psi\rangle = 0$. Therefore, $\||\psi_1\rangle\| = 1$. The derivation of $\||\psi_2\rangle\| = 1$ is very similar, so we omit it here.

Next, we show $N_0N_1|\psi_1\rangle = e^{-i2\mu}|\psi_1\rangle$ and $N_0N_1|\psi_2\rangle = e^{i2\mu}|\psi_2\rangle$. From eq. (5.3), we get that

$$
\begin{aligned}
Z_B M_0^{(0)}|\psi\rangle =& \frac{Z_B(\mathbb{1}+Z_A)}{2}|\psi\rangle \\
=& \frac{Z_B+\mathbb{1}}{2}|\psi\rangle \\
=& \frac{\mathbb{1}+Z_A}{2}|\psi\rangle \\
=& M_0^{(0)}|\psi\rangle.
\end{aligned}
$$

With similar reasoning, we get

$$
Z_B M_0^{(1)}|\psi\rangle = -M_0^{(1)}|\psi\rangle.
$$

Substituting the expression of Z_B, we see that

$$
\begin{aligned}
(N_0+N_1)M_0^{(0)}|\psi\rangle &= 2\cos(\mu)M_0^{(0)}|\psi\rangle, \\
(N_0+N_1)M_0^{(1)}|\psi\rangle &= -2\cos(\mu)M_0^{(1)}|\psi\rangle.
\end{aligned}
$$

From eqs. (5.3) to (5.5) and (5.7), we get that

$$
\begin{aligned}
X_B M_0^{(0)}|\psi\rangle &= X_A M_0^{(1)}|\psi\rangle, \\
X_B M_0^{(1)}|\psi\rangle &= X_A M_0^{(0)}|\psi\rangle.
\end{aligned}
$$

Substituting in the expression of X_B, we get that

$$(N_0 - N_1)M_0^{(0)}|\psi\rangle = 2\sin(\mu)M_1M_0^{(1)}|\psi\rangle,$$
$$(N_0 - N_1)M_0^{(1)}|\psi\rangle = 2\sin(\mu)M_1M_0^{(0)}|\psi\rangle.$$

Simple cancelation gives us that

$$N_0M_0^{(0)}|\psi\rangle = [\cos(\mu)M_0^{(0)} + \sin(\mu)M_1M_0^{(1)}]|\psi\rangle,$$
$$N_1M_0^{(0)}|\psi\rangle = [\cos(\mu)M_0^{(0)} - \sin(\mu)M_1M_0^{(1)}]|\psi\rangle,$$
$$N_0M_0^{(1)}|\psi\rangle = [-\cos(\mu)M_0^{(1)} + \sin(\mu)M_1M_0^{(0)}]|\psi\rangle,$$
$$N_1M_0^{(1)}|\psi\rangle = [-\cos(\mu)M_0^{(1)} - \sin(\mu)M_1M_0^{(0)}]|\psi\rangle.$$

Then,

$$N_0N_1M_0^{(0)}|\psi\rangle = [\cos(2\mu)M_0^{(0)} + \sin(2\mu)M_1M_0^{(1)}]|\psi\rangle,$$
$$N_0N_1M_1M_0^{(1)}|\psi\rangle = [\cos(2\mu)M_1M_0^{(1)} - \sin(2\mu)M_0^{(0)}]|\psi\rangle.$$

Therefore,

$$N_0N_1(M_0^{(0)} + iM_1M_0^{(1)})|\psi\rangle = e^{-2i\mu}(M_0^{(0)} + iM_1M_0^{(1)})|\psi\rangle,$$
$$N_0N_1(M_0^{(0)} - iM_1M_0^{(1)})|\psi\rangle = e^{2i\mu}(M_0^{(0)} - iM_1M_0^{(1)})|\psi\rangle,$$

which complete the proof. $\square$

5.2 The generalized swap-isometry

In the previous section, we see that the swap-isometry is a key component of the proof of Lemma 5.4. In this section, we generalize the swap-isometry so that it can be used in the proofs of self-tests of general d-dimensional maximally entangled states. The importance of the generalized swap-isometry allows us to identify sufficient conditions for the self-test of general d-dimensional maximally entangled states, as formally stated in the following theorem.

Theorem 5.6. *Let k and d be two integers such that $d \geq 2$ and $k \leq d$, and $\{r_j \mid j \in [k]\}, \{s_j \mid j \in [k]\} \subseteq [d]$ be two sets of integers. If there exist a set of quantum states*

$$\{|\psi_j\rangle \mid j \in [k]\} \subseteq \mathcal{H}$$

and two commuting sets of unitaries

$$\{O_A, V_{A,j} \mid j \in [k]\} \subset \mathcal{U}(\mathcal{H}), \qquad \{O_B, V_{B,j} \mid j \in [k]\} \subset \mathcal{U}(\mathcal{H}),$$

such that

$$\| |\psi_j\rangle \| = \frac{1}{\sqrt{k}} \tag{5.17}$$

$$O_A|\psi_j\rangle = \omega_d^{r_j}|\psi_j\rangle \tag{5.18}$$

$$O_B|\psi_j\rangle = \omega_d^{s_j}|\psi_j\rangle \tag{5.19}$$

$$|\psi_j\rangle = V_{A,j}V_{B,j}|\psi_1\rangle \tag{5.20}$$

for $j \in [k]$, then, $|\psi\rangle = \sum_{j\in[k]} |\psi_j\rangle$ is a normalized quantum state, and there exist a local isometry $\Phi_A \otimes \Phi_B$ such that

$$\Phi_A \otimes \Phi_B(|\psi\rangle) = \sqrt{k}|\psi_1\rangle \otimes \frac{1}{\sqrt{k}} \sum_{j\in[k]} |r_j\rangle|s_j\rangle. \tag{5.21}$$

The isometry $\Phi_A \otimes \Phi_B$ is the generalized swap-isometry shown in the figure below.

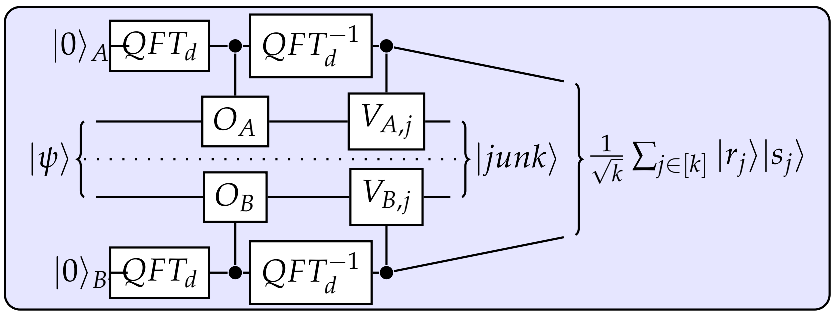

Figure 5.2: The generalized swap-isometry

The input state to the isometry is $|\psi\rangle \in \mathcal{H}$. Let $\mathcal{H}_{A'} = \mathcal{H}_{B'} = \mathbb{C}^d$, which are the systems added by the isometry. The isometry uses the d-dimensional quantum Fourier transform

$$QFT_d = \sum_{j\in[d]} \sum_{k\in[d]} \omega_d^{jk} |k\rangle\langle j|.$$

It also uses controlled-unitaries: the controlled-$O_{A/B}$, denoted by $C\text{-}O_{A/B} \in \mathcal{U}(\mathbb{C}^d \otimes \mathcal{H})$,

$$C\text{-}O_{A/B} = \sum_{j\in[d]} |j\rangle\langle j| \otimes O^j_{A/B};$$

and the controlled-$V_{A/B}$, denoted by $C\text{-}V_{A/B} \in \mathcal{U}(\mathbb{C}^d \otimes \mathcal{H})$, and defined by

$$C\text{-}V_{A/B} = \sum_{j \in [d]} |j\rangle\langle j| \otimes V^{\dagger}_{A/B,j}.$$

The isometry has the following steps:

Step1 Alice and Bob attach $|0\rangle_{A'}$ and $|0\rangle_{B'}$ to their sides;

Step2 Alice and Bob apply QFT_d to $|0\rangle_{A'}$ and $|0\rangle_{B'}$ respectively;

Step3 Alice and Bob apply $C\text{-}O_A$ and $C\text{-}O_B$;

Step4 Alice and Bob apply QFT_d^{-1} (the inverse of QFT_d) to the states in $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ respectively;

Step5 Alice and Bob apply $C\text{-}V_A$ and $C\text{-}V_B$.

Intuitively, the isometry contains three phases:

1. The **Preparation phase** (**Step1**);
2. The **Distinguishing phase** (**Step2** to **Step4**), where we entangled the state in $\mathcal{H}$ with the state in $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$;
3. The **Correction phase** (**Step5**), where we disentangle the state in $\mathcal{H}$ with the state in $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ and effectively transferring all the entanglement to the system $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$.

Proof. We first prove that $\|\psi\| = 1$. Since $|\psi_i\rangle$ and $|\psi_j\rangle$ are different eigenvectors of O_A for $i \neq j$, then we know $\langle \psi_i | \psi_j \rangle = 0$. Therefore,

$$\langle \psi | \psi \rangle = \sum_{j \in [k]} \langle \psi_j | \psi_j \rangle = k/k = 1.$$

Next, we show that it suffices to choose $\Phi_A \otimes \Phi_B$ to be the *generalized swap-isometry* by listing all the steps of it and showing how the state evolves.

1. After **Step1** the shared state becomes

$$|\psi\rangle |0\rangle_{A'} |0\rangle_{B'} = \sum_{j \in [k]} |\psi_j\rangle |0\rangle_{A'} |0\rangle_{B'}.$$

2. After **Step2** the state evolves to

$$\rightarrow \frac{1}{d} \sum_{j \in [k]} |\psi_j\rangle \sum_{\alpha_1, \alpha_2 \in [d]} |\alpha_1\rangle_{A'} |\alpha_2\rangle_{B'}.$$

3. After **Step3** the state evolves to

$$\begin{aligned} \rightarrow & \frac{1}{d} \sum_{j \in [k]} \sum_{\alpha_1, \alpha_2 \in [d]} O_A^{\alpha_1} O_B^{\alpha_2} |\psi_j\rangle |\alpha_1\rangle_{A'} |\alpha_2\rangle_{B'} \\ = & \frac{1}{d} \sum_{j \in [k]} \sum_{\alpha_1, \alpha_2 \in [d]} \omega_d^{r_j \alpha_1} \omega_d^{s_j \alpha_2} |\psi_j\rangle |\alpha_1\rangle_{A'} |\alpha_2\rangle_{B'}, \end{aligned}$$

where we use eqs. (5.18) and (5.19).

4. After **Step4** the state evolves to

$$\to \frac{1}{d^2} \sum_{j\in[k]} \sum_{\beta_1,\beta_2\in[d]} \left(\sum_{\alpha_1\in[d]} \omega_d^{(r_j-\beta_1)\alpha_1} \right) \left(\sum_{\alpha_2\in[d]} \omega_d^{(s_j-\beta_2)\alpha_2} \right) |\psi_j\rangle |\beta_1\rangle_{A'} |\beta_2\rangle_{B'}$$
$$= \sum_{j=1}^{k} |\psi_j\rangle |r_j\rangle_{A'} |s_j\rangle_{B'}.$$

5. After **Step5** the state becomes

$$\to \sum_{j\in[k]} V_{A,j}^\dagger V_{B,j}^\dagger |\psi_j\rangle |r_j\rangle_{A'} |s_j\rangle_{B'}$$
$$= \sum_{j\in[k]} V_{A,j}^\dagger V_{B,j}^\dagger V_{A,j} V_{B,j} |\psi_1\rangle |r_j\rangle_{A'} |s_j\rangle_{B'}$$
$$= |\psi_1\rangle \otimes \sum_{j\in[k]} |r_j\rangle_{A'} |s_j\rangle_{B'}$$
$$= \sqrt{k} |\psi_1\rangle \otimes \frac{1}{\sqrt{k}} \sum_{j\in[k]} |r_j\rangle_{A'} |s_j\rangle_{B'},$$

where we use eq. (5.20) and complete the proof.

□

5.3 Extending the correlation Q_μ

In this section, we introduce a correlation based on Q_μ. Recall that Q_μ can certify two eigenvalues of a unitary. The extended correlation can certify $(p-1)$ eigenvalues of some unitary under some condition for some odd prime p.

In the rest of the dissertation, we fix $\mu = -\pi/p$ for some odd prime p. We will introduce a correlation that is extended from $Q_{-\pi/p}$, denoted by $\hat{Q}_{-\pi/p}$.

We define $\hat{Q}_{-\pi/p} : [5] \times [5] \times [3] \times [3] \to \mathbb{R}$ by defining its inducing quantum strategy.

In $\mathbb{C}^{p-1}$, we define a subspace $V = \mathrm{span}(\{|1\rangle, |p-1\rangle\})$ and we denote the projector onto V by Π_V. For question $x = 0$, define projectors

$$\overline{M}_0^{(a)} = \overline{N}_0^{(a)} = \begin{cases} \Pi_V & \text{if } a = 0 \\ \mathbb{1} - \Pi_V & \text{if } a = 1 \\ 0 & \text{otherwise.} \end{cases}$$

For question $x = 1, 2$, we first introduce

$$\begin{aligned}
|j_+\rangle &= \cos(-\frac{j\pi}{2p})|j\rangle + \sin(-\frac{j\pi}{2p})|p-j\rangle, \\
|(p-j)_+\rangle &= \sin(-\frac{j\pi}{2p})|j\rangle - \cos(-\frac{j\pi}{2p})|p-j\rangle, \\
|j_-\rangle &= \cos(-\frac{j\pi}{2p})|j\rangle - \sin(-\frac{j\pi}{2p})|p-j\rangle, \\
|(p-j)_-\rangle &= \sin(-\frac{j\pi}{2p})|j\rangle + \cos(-\frac{j\pi}{2p})|p-j\rangle.
\end{aligned}$$

Then the projectors are

$$\overline{M}_1^{(a)} = \overline{N}_1^{(a)} = \begin{cases} \sum_{j=1}^{(p-1)/2} |j_+\rangle\langle j_+| & \text{if } a = 0 \\ \sum_{j=1}^{(p-1)/2} |(p-j)_+\rangle\langle (p-j)_+| & \text{if } a = 1 \\ 0 & \text{otherwise,} \end{cases}$$

$$\overline{M}_2^{(a)} = \overline{N}_2^{(a)} = \begin{cases} \sum_{j=1}^{(p-1)/2} |j_-\rangle\langle j_-| & \text{if } a = 0 \\ \sum_{j=1}^{(p-1)/2} |(p-j)_-\rangle\langle (p-j)_-| & \text{if } a = 1 \\ 0 & \text{otherwise.} \end{cases}$$

For question $x = 3$,

$$\overline{M}_3^{(a)} = \overline{N}_3^{(a)} = \begin{cases} |1\rangle\langle 1| & \text{if } a = 0 \\ |p-1\rangle\langle p-1| & \text{if } a = 1 \\ \mathbb{1} - \Pi_V & \text{otherwise.} \end{cases}$$

For question $x = 4$,

$$\overline{M}_4^{(a)} = \overline{N}_4^{(a)} = \begin{cases} \frac{(|1\rangle + |p-1\rangle)(\langle 1| + \langle p-1|}{2}) & \text{if } a = 0 \\ \frac{(|1\rangle - |p-1\rangle)(\langle 1| - \langle p-1|}{2}) & \text{if } a = 1 \\ \mathbb{1} - \Pi_V & \text{otherwise.} \end{cases}$$

Define a state

$$|\phi\rangle = \frac{1}{\sqrt{p-1}} \sum_{j=1}^{(p-1)/2} (|j\rangle|j\rangle + |p-j\rangle|p-j\rangle).$$

Then, the inducing strategy is

$$S_{-\pi/p} = (|\phi\rangle, \{\{\overline{M}_x^{(a)} \mid a \in [3]\} \mid x \in [5]\}, \{\{\overline{N}_y^{(b)} \mid b \in [3]\} \mid y \in [5]\}). \quad (5.22)$$

Definition 5.7. *The correlation* $\hat{Q}_{-\pi/p} : [5] \times [5] \times [3] \times [3] \to \mathbb{R}_{\geq 0}$ *is induced by* $S_{-\pi/p}$*:*

$$\hat{Q}_{-\pi/p}(a, b|x, y) = \langle\phi|\overline{M}_x^{(a)} \otimes \overline{N}_y^{(b)}|\phi\rangle.$$

As an analogue of Proposition 5.5, the implication of $\hat{Q}_{-\pi/p}$ is summarized in the next proposition.

Proposition 5.8. *If a quantum strategy* $(|\psi\rangle \in \mathcal{H}, \{\{M_x^{(a)} \mid a \in [3]\} \mid x \in [5]\}, \{\{N_y^{(b)} \mid b \in [3]\} \mid y \in [5]\})$ *can induce* $\hat{Q}_{-\pi/p}$*, then there exists a quantum state* $|\psi_1\rangle \in \mathcal{H}$ *such that* $\||\psi_1\rangle\|^2 = \frac{1}{p-1}$ *and*

$$M_1 M_2 |\psi_1\rangle = \omega_p^{-1} |\psi_1\rangle, \quad (5.23)$$

$$N_1 N_2 |\psi_1\rangle = \omega_p |\psi_1\rangle, \quad (5.24)$$

where $M_x := M_x^{(0)} - M_x^{(1)}$ *and* $N_y := N_y^{(0)} - N_y^{(1)}$ *for* $x, y \in \{1, 2\}$.

To help the proof of this proposition, we first give some values of $\hat{Q}_{-\pi/p}$.

$$\hat{Q}_{-\pi/p}(a,b|0,0) = \begin{cases} 2/(p-1) & \text{if } a=b=0 \\ (p-3)/(p-1) & \text{if } a=b=1 \\ 0 & \text{otherwise.} \end{cases}$$

$$\hat{Q}_{-\pi/p}(a,b|3,3) = \begin{cases} 1/(p-1) & \text{if } a=b=0 \\ 1/(p-1) & \text{if } a=b=1 \\ (p-3)/(p-1) & \text{if } a=b=2 \\ 0 & \text{otherwise.} \end{cases}$$

$$\hat{Q}_{-\pi/p}(a,b|0,3) = \begin{cases} 1/(p-1) & \text{if } a=0, b\in[2] \\ (p-3)/(p-1) & \text{if } a=1, b=2 \\ 0 & \text{otherwise.} \end{cases}$$

		$x=3$		$x=4$	
		$a=0$	$a=1$	$a=0$	$a=1$
$y=1$	$b=0$	$\frac{\cos^2(\pi/2p)}{p-1}$	$\frac{\sin^2(\pi/2p)}{p-1}$	$\frac{1-\sin(\pi/p)}{2(p-1)}$	$\frac{1+\sin(\pi/p)}{2(p-1)}$
	$b=1$	$\frac{\sin^2(\pi/2p)}{p-1}$	$\frac{\cos^2(\pi/2p)}{p-1}$	$\frac{1+\sin(\pi/p)}{2(p-1)}$	$\frac{1-\sin(\pi/p)}{2(p-1)}$
$y=2$	$b=0$	$\frac{\cos^2(\pi/2p)}{p-1}$	$\frac{\sin^2(\pi/2p)}{p-1}$	$\frac{1+\sin(\pi/p)}{2(p-1)}$	$\frac{1-\sin(\pi/p)}{2(p-1)}$
	$b=1$	$\frac{\sin^2(\pi/2p)}{p-1}$	$\frac{\cos^2(\pi/2p)}{p-1}$	$\frac{1-\sin(\pi/p)}{2(p-1)}$	$\frac{1+\sin(\pi/p)}{2(p-1)}$

Table 5.1: $\hat{Q}_{-\pi/p}$: the correlation values for $x \in \{3,4\}$, $y \in \{1,2\}$ and $a,b \in [2]$.

Proof. From the definition of $\hat{Q}_{-\pi/p}$, it is easy to see that

$$M_x^{(2)}|\psi\rangle = N_x^{(2)}|\psi\rangle = 0$$

for $x, y \in [3]$. Then

$$M_x^2|\psi\rangle = [M_x^{(0)} + M_x^{(1)}]|\psi\rangle + M_x^{(2)}|\psi\rangle = |\psi\rangle$$

for $x \in \{1, 2\}$. Similarly, we see that $N_y^2|\psi\rangle = |\psi\rangle$ for $y \in \{1, 2\}$. Using Proposition 4.13, we can get that

$$\begin{aligned}
M_0^{(0)}|\psi\rangle &= (M_3^{(0)} + M_3^{(1)})|\psi\rangle = (M_4^{(0)} + M_4^{(1)})|\psi\rangle \\
&= N_0^{(0)}|\psi\rangle = (N_3^{(0)} + N_3^{(1)})|\psi\rangle = (N_4^{(0)} + N_4^{(1)})|\psi\rangle, \\
M_0^{(1)}|\psi\rangle &= M_3^{(2)}|\psi\rangle = M_4^{(2)}|\psi\rangle \\
&= N_0^{(1)}|\psi\rangle = N_3^{(2)}|\psi\rangle = N_4^{(2)}|\psi\rangle,
\end{aligned}$$

and

$$\begin{aligned}
M_3^{(0)}|\psi\rangle &= N_3^{(0)}|\psi\rangle, & M_3^{(1)}|\psi\rangle &= N_3^{(1)}|\psi\rangle, \\
M_4^{(0)}|\psi\rangle &= N_4^{(0)}|\psi\rangle, & M_4^{(1)}|\psi\rangle &= N_4^{(1)}|\psi\rangle.
\end{aligned}$$

Then, we can show that $\hat{Q}_{-\pi/p}$ can be "reduced" to $Q_{-\pi/p}$ by proving that

$$S = \Big(\frac{M_0^{(0)}|\psi\rangle}{\|M_0^{(0)}|\psi\rangle\|}, \{\{M_x^{(0)}, M_x^{(1)}\} \mid x \in \{3,4\}\}, \{\{N_y^{(0)}, N_y^{(1)}\} \mid y \in \{1,2\}\}\Big)$$

can induce $Q_{-\pi/p}$, and that

$$S' = \Big(\frac{M_0^{(0)}|\psi\rangle}{\|M_0^{(0)}|\psi\rangle\|}, \{\{M_x^{(0)}, M_x^{(1)}\} \mid x \in \{1,2\}\}, \{\{N_y^{(0)}, N_y^{(1)}\} \mid y \in \{3,4\}\}\Big)$$

can induce $Q_{-\pi/p}$ with Alice and Bob's roles flipped. To prove S can induce $Q_{-\pi/p}$, we need to examine the terms of the form $\langle\psi|M_0^{(0)} M_x^{(a)} N_y^{(b)} M_0^{(0)}|\psi\rangle$ for $x = 3,4$, $y = 1,2$ and $a, b = 0, 1$. We find that these terms relate to $\langle\psi|M_x^{(a)} N_y^{(b)}|\psi\rangle$ by

$$\begin{aligned}
&\langle\psi|M_x^{(a)} N_y^{(b)}|\psi\rangle \\
=&\langle\psi|(M_0^{(0)} + M_0^{(1)}) M_x^{(a)} N_y^{(b)} (M_0^{(0)} + M_0^{(1)})|\psi\rangle \\
=&\langle\psi|M_0^{(0)} M_x^{(a)} N_y^{(b)} M_0^{(0)}|\psi\rangle,
\end{aligned}$$

where we use the facts that $M_x^{(a)} M_0^{(1)}|\psi\rangle = M_x^{(a)} M_x^{(2)}|\psi\rangle = 0$ for the relevant values of (x, y, a, b). Therefore,

$$\frac{\langle\psi|M_0^{(0)} M_x^{(a)} N_y^{(b)} M_0^{(0)}|\psi\rangle}{\|M_0^{(0)}|\psi\rangle\|^2} = \frac{\langle\psi|M_x^{(a)} N_y^{(b)}|\psi\rangle}{\|M_0^{(0)}|\psi\rangle\|^2},$$

for the relevant values of (x, y, a, b), and it is easy to verify that S induces $Q_{-\pi/p}$. For example, $\frac{\langle\psi|M_0^{(0)} M_1^{(0)} N_3^{(0)} M_0^{(0)}|\psi\rangle}{\|M_0^{(0)}|\psi\rangle\|^2} = \frac{\cos(\pi/2p)^2}{2}$. The proof of S' induces $Q_{-\pi/p}$

with Alice and Bob's roles flipped is similar, so we omit it here.

Now we define

$$\begin{aligned}|\psi_1\rangle =&\frac{1}{2}(M_3^{(0)} + iM_4M_3^{(1)} - iM_4M_3^{(0)} + M_3^{(1)})|\psi\rangle \\ =&\frac{1}{2}(\mathbb{1} - iM_4)(M_3^{(0)} + iM_4M_3^{(1)})|\psi\rangle,\end{aligned} \tag{5.25}$$

where $M_4 := M_4^{(0)} - M_4^{(1)}$. The derivation of $\||\psi_1\rangle\|$ is very similar to the corresponding part in the proof of Proposition 5.5, so we omit it here. Since S can induce $Q_{-\pi/p}$, by Proposition 5.5, we know that

$$N_1N_2(M_3^{(0)} + iM_4M_3^{(1)})M_0^{(0)}|\psi\rangle = \omega_p(M_3^{(0)} + iM_4M_3^{(1)})M_0^{(0)}|\psi\rangle.$$

On the other hand,

$$\begin{aligned}&(M_3^{(0)} + iM_4M_3^{(1)})M_0^{(0)}|\psi\rangle \\ =&(M_3^{(0)} + iM_4M_3^{(1)})(M_3^{(0)} + M_3^{(1)})|\psi\rangle \\ =&(M_3^{(0)} + iM_4M_3^{(1)})|\psi\rangle.\end{aligned}$$

Hence, using the fact that N_1N_2 commutes with $(\mathbb{1} - iM_4)$, we know

$$N_1N_2|\psi_1\rangle = \omega_p|\psi_1\rangle.$$

What remains to be proved is $M_1M_2|\psi_1\rangle = \omega_p^{-1}|\psi_1\rangle$. In order to prove it, we need another form of $|\psi_1\rangle$, which is

$$\begin{aligned}|\psi_1\rangle =&\frac{1}{2}(N_3^{(0)} - iN_4N_3^{(1)} + iN_4N_3^{(0)} + N_3^{(1)})|\psi\rangle. \\ =&(\mathbb{1} + iN_4)(N_3^{(0)} - iN_4N_3^{(1)})|\psi\rangle,\end{aligned}$$

where $N_4 := N_4^{(0)} - N_4^{(1)}$. Comparing the two forms of $|\psi_1\rangle$, it suffices to show

$$M_4(M_3^{(1)} - M_3^{(0)})|\psi\rangle = N_4(N_3^{(0)} - N_3^{(1)})|\psi\rangle.$$

This equation can be derived in the following way

$$\begin{aligned}&M_4(M_3^{(1)} - M_3^{(0)})|\psi\rangle \\ =&M_4(M_3^{(1)} - M_3^{(0)})M_0^{(0)}|\psi\rangle \\ =&(N_3^{(1)} - N_3^{(0)})N_4N_0^{(0)}|\psi\rangle \\ =&N_4(N_3^{(0)} - N_3^{(1)})N_0^{(0)}|\psi\rangle \\ =&N_4(N_3^{(0)} - N_3^{(1)})|\psi\rangle,\end{aligned}$$

where we use the fact that eq. (5.7) is satisfied in the inducing strategies S and S'. In the end, we apply Proposition 5.5 to S' to see that

$$\begin{aligned}&M_1M_2|\psi_1\rangle \\ =&(\mathbb{1} + iN_4)M_1M_2(N_3^{(0)} - iN_4N_3^{(1)})|\psi\rangle \\ =&\omega_p^{-1}|\psi_1\rangle,\end{aligned}$$

which completes the proof. $\square$

Proposition 5.9. *Suppose a quantum strategy* $(|\psi\rangle \in \mathcal{H}, \{\{M_x^{(a)} \mid a \in [3]\} \mid x \in [5]\},$ $\{\{N_y^{(b)} \mid b \in [3]\} \mid y \in [5]\})$ *can induce* $\hat{Q}_{-\pi/p}$*, and there exist commuting unitaries* $U_A, U_B \in \mathcal{U}(\mathcal{H})$ *such that* U_A *commutes with Bob's projectors,* U_B *commutes with Alice's projectors and*

$$U_A|\psi\rangle = U_B|\psi\rangle,$$

$$U_A^\dagger M_1 M_2 U_A|\psi\rangle = (M_1 M_2)^r|\psi\rangle,$$

$$U_B^\dagger N_1 N_2 U_B|\psi\rangle = (N_1 N_2)^r|\psi\rangle,$$

where r *is a primitive root of* p*. Then there exist quantum states* $\{|\psi_j\rangle \mid 1 \leq j \leq p-1\} \subseteq \mathcal{H}$ *such that* $\||\psi_j\rangle\|^2 = \frac{1}{p-1}$ *and*

$$M_1 M_2|\psi_j\rangle = \omega_p^{-j}|\psi_j\rangle,$$

$$N_1 N_2|\psi_j\rangle = \omega_p^{j}|\psi_j\rangle.$$

Proof. Define $|\psi_j\rangle = (U_A U_B)^{\log_r j}|\psi_1\rangle$ for $1 \leq j \leq p-1$ where $\log_r j$ is the discrete log. To simplify the notation, we write $O_A = M_1 M_2$ and $O_B = N_1 N_2$.

We first prove that $O_A|\psi\rangle = O_B^{-1}|\psi\rangle$. It is easy to check that

$$\hat{Q}_{-\pi/p}(0,0|x,x) = Q_{-\pi/p}(1,1|x,x) = 1/2,$$

$$\hat{Q}_{-\pi/p}(0,1|x,x) = Q_{-\pi/p}(1,0|x,x) = 0,$$

for $x = 1, 2$. By Proposition 4.13, we can see that $M_x^{(a)}|\psi\rangle = N_x^{(a)}|\psi\rangle$ for $x = 1, 2$ and $a = 0, 1$, and that $M_x|\psi\rangle = N_x|\psi\rangle$. Then,

$$O_A|\psi\rangle = M_1 M_2|\psi\rangle = N_2 M_1|\psi\rangle = N_2 N_1|\psi\rangle = O_B^{-1}|\psi\rangle.$$

Next, we prove that

$$O_A(U_A)^j|\psi\rangle = (U_A)^j O_A^{r^j}|\psi\rangle,$$
$$O_B(U_B)^j|\psi\rangle = (U_B)^j O_B^{r^j}|\psi\rangle$$

for $j \geq 1$ by induction. The base case is trivial as it is stated in the proposition. Assume $O_A(U_A)^n|\psi\rangle = (U_A)^n O_A^{r^n}|\psi\rangle$. By substitution and Lemma 4.15, we know

$$\begin{aligned} O_A(U_A)^{n+1}|\psi\rangle =& U_B O_A (U_A)^n|\psi\rangle \\ =& U_B U_A^n O_A^{r^n}|\psi\rangle \\ =& U_A^n O_A^{r^n} U_A|\psi\rangle \\ =& U_A^{n+1} O_A^{r^{n+1}}|\psi\rangle, \end{aligned}$$

where in the last line, we repeatedly use the relations: $O_A U_A|\psi\rangle = U_A(O_A)^r|\psi\rangle$ and $O_A|\psi\rangle = O_B^{-1}|\psi\rangle$, r^n times. By the principle of induction, the equality $O_A(U_A)^j|\psi\rangle = (U_A)^j O_A^{r^j}|\psi\rangle$ is true for all $j \geq 1$. The proof of $O_B(U_B)^j|\psi\rangle = (U_B)^j O_B^{r^j}|\psi\rangle$ is similar, so we omit it here.

Then,

$$O_A(U_A)^j|\psi_1\rangle = (U_A)^j O_A^{rj}|\psi_1\rangle = \omega_p^{-rj}(U_A^\dagger)^j|\psi_1\rangle,$$

$$O_B(U_B)^j|\psi_1\rangle = (U_B)^j O_B^{rj}|\psi_1\rangle = \omega_p^{rj}(U_B^\dagger)^j|\psi_1\rangle,$$

where we use the fact that $|\psi_1\rangle$ can be expressed using Alice's projectors and Bob's projectors and the proof is complete. □

5.4 The correlation $Q_{p,r}$

In this section, we first show that there exists a binary linear system such that a perfect correlation associated with it can enforce the relation $U^{-1}OU = O^r$ for two unitaries U and O, as summarized in the next proposition.

Proposition 5.10. *There exists a binary linear system $A_r\boldsymbol{x} = 0$ such that the following holds. If a quantum strategy $S = (|\psi\rangle \in \mathcal{H}, \{\{M_x^{(a)}\}\}, \{\{N_y^{(b)}\}\})$ can induce a perfect correlation of $A_r\boldsymbol{x} = 0$, then there exist two commuting sets of binary observables $\{M_{u_1}, M_{u_2}, M_{o_1}, M_{o_2}\}$ and $\{N_{u_1}, N_{u_2}, N_{o_1}, N_{o_2}\}$ on $\mathcal{H}$ such that*

$$M_{u_2}M_{u_1}(M_{o_1}M_{o_2})M_{u_1}M_{u_2}|\psi\rangle = (M_{o_1}M_{o_2})^r|\psi\rangle,$$

$$N_{u_2}N_{u_1}(N_{o_1}N_{o_2})N_{u_1}N_{u_2}|\psi\rangle = (N_{o_1}N_{o_2})^r|\psi\rangle.$$

Proof. The linear system $A_r\boldsymbol{x} = 0$ is constructed from a solution group, wherein the following group is embedded. For $r \geq 2$, define

$$\begin{aligned} G := \langle u_1, u_2, o_1, o_2 : & u_1^2 = u_2^2 = o_1^2 = o_2^2 = e, \\ & u_2 u_1 o_1 o_2 u_1 u_2 = (o_1 o_2)^r, u_1 o_2 u_1 = o_2 \rangle. \end{aligned} \tag{5.26}$$

By Proposition 3.55, G can be embedded into a linear-plus-conjugacy group $G_c = \langle S_c : R_c \rangle$ where S_c contains $\{u_1, u_2, o_1, o_2\}$. We also know that the embedding $\phi : G \to G_c$ maps u_i to u_i and o_i to o_i for $i = 1, 2$. By Proposition 3.56, G_c can be embedded into a solution group $\Gamma(A_r) := \langle S_\Gamma, R_\Gamma \rangle$. Moreover, $\{u_1, u_2, o_1, o_2\} \subseteq S_\Gamma$ and the embedding $\phi' : G_c \to \Gamma(A_r)$ maps s to s for each $s \in \{u_1, u_2, o_1, o_2\}$. Therefore, G is embedded in $\Gamma(A_r)$ and we get the binary linear system $A_r \boldsymbol{x} = 0$.

Since G is embedded in $\Gamma(A_r)$, we know that the relation $u_2 u_1 o_1 o_2 u_1 u_2 = (o_1 o_2)^r$ can be reconstructed by substituting in $r \in R_\Gamma$. Then, the statement of the proposition follows from Lemmas 4.15 and 4.19. $\square$

Note that $A_r \boldsymbol{x} = 0$ has $n(r) := 16r + 75$ variables and $m(r) := 14r + 62$ equations, where each equation has 3 variables. Let $\tau : [n(r)] \to S_\Gamma$ be the bijection between $[n(r)]$ and S_Γ. We assume that in this system $\tau(0) = o_1$ and $\tau(1) = o_2$.

Next we show that there exists a quantum strategy that can induce a perfect correlation of $A_r \boldsymbol{x} = 0$. The correlation is denoted by P_{A_r} and the strategy is denoted by S_{A_r}, which is based on a representation of $\Gamma(A_r)$.

We first give a representation of G. Let p be an odd prime number whose primitive root is r. Another basis of $\mathbb{C}^{p-1}$ is $\{|x_j\rangle \mid 1 \leq j \leq p-1\}$, where

$$|x_j\rangle = -\frac{1}{\sqrt{2}}(|j\rangle + i|p-j\rangle), \tag{5.27}$$

$$|x_{p-j}\rangle = \frac{-\omega_{2p}^{j}}{\sqrt{2}}(|j\rangle - i|p-j\rangle) \tag{5.28}$$

for $1 \leq j \leq \frac{p-1}{2}$. Note that another form of this basis is $\{|x_{r^j}\rangle \mid j \in [p-1]\}$, where the subscript r^j is taken modulo p implicitly. Based on the second basis, we define the third basis of $\mathbb{C}^{p-1}$, $\{|u_k\rangle \mid k \in [p-1]\}$ defined by

$$|u_k\rangle = \frac{1}{\sqrt{p-1}} \sum_{j=0}^{p-2} \omega_{p-1}^{jk} |x_{r^j}\rangle.$$

On $\mathbb{C}^{p-1}$, we define

$$O_1 = \sum_{j=1}^{(p-1)/2} \omega_p^{j} |x_j\rangle\langle x_{p-j}| + \omega_p^{-j} |x_{p-j}\rangle\langle x_j|, \tag{5.29}$$

$$O_2 = \sum_{j=1}^{(p-1)/2} |x_j\rangle\langle x_{p-j}| + |x_{p-j}\rangle\langle x_j|, \tag{5.30}$$

$$\begin{aligned} U_1 =& |u_0\rangle\langle u_0| + |u_{(p-1)/2}\rangle\langle u_{(p-1)/2}| \\ &+ \sum_{k=1}^{(p-3)/2} \left(|u_{p-1-k}\rangle\langle u_k| + |u_k\rangle\langle u_{p-1-k}|\right), \end{aligned} \tag{5.31}$$

$$\begin{aligned} U_2 =& |u_0\rangle\langle u_0| - |u_{(p-1)/2}\rangle\langle u_{(p-1)/2}| \\ &+ \sum_{k=1}^{(p-3)/2} \left(\omega_{p-1}^{k} |u_k\rangle\langle u_{p-1-k}| + \omega_{p-1}^{-k} |u_{p-1-k}\rangle\langle u_k|\right). \end{aligned} \tag{5.32}$$

It can be checked that

$$
\begin{aligned}
O_1O_2 &= \sum_{j\in[p-1]} \omega_p^{r^j} |x_{r^j}\rangle\langle x_{r^j}|, \\
U_1U_2 &= \sum_{j\in[p-1]} |x_{r^{j+1}}\rangle\langle x_{r^j}|, \\
U_2U_1(O_1O_2)U_1U_2 &= (O_1O_2)^r, \\
U_1O_2U_1 &= O_2.
\end{aligned}
$$

Hence, we can follow the proof of [7, Proposition 33] to extend $\rho : G_c \to \mathcal{U}(\mathbb{C}^{p-1})$ defined by $u_1 \mapsto U_1, u_2 \mapsto U_2, o_1 \mapsto O_1, o_2 \mapsto O_2$ to a representation of G_c, still denoted by ρ. Then, following the proofs of [7, Proposition 27 and Lemma 29], ρ can be extended to a representation of $\Gamma(A_r)$, $\rho' : \Gamma(A_r) \to \mathcal{U}(\mathbb{C}^{p-1} \otimes \mathbb{C}^2 \otimes \mathbb{C}^2)$. In particular, for any $s \in \{u_1, u_2, o_1, o_2\}$,

$$
\rho'(s) = \rho(s) \otimes \mathbb{1}_{\mathbb{C}^2} \otimes \mathbb{1}_{\mathbb{C}^2}.
$$

Define

$$
|\tilde{\psi}\rangle := \frac{1}{\sqrt{p-1}} \sum_{j=1}^{p-1} |x_j\rangle |x_{p-j}\rangle. \tag{5.33}
$$

Let $\pi_s^{(0)}, \pi_s^{(1)}$ be the projectors onto the $+1$ and -1-eigenspaces of $\rho'(s)$ for each

$s \in S_\Gamma$. Then we define projectors

$$M_i^{(x)} = N_i^{(x)} = \begin{cases} \prod_{k \in I_i} \pi_{\tau(k)}^{(x(k))} & \text{if } i \in [m(r)] \\ \pi_{\tau(i-m(r))}^{(x)} & \text{if } i \geq m(r) \text{ and } x < 2 \\ 0 & \text{otherwise.} \end{cases}$$

Definition 5.11. *The correlation $P_{A_r} : [m(r)+n(r)] \times [m(r)+n(r)] \times \mathbb{Z}_2^3 \times \mathbb{Z}_2^3 \to R_{\geq 0}$ is defined by the inducing strategy*

$$\begin{aligned} S_{A_r} = (|\tilde{\psi}\rangle \otimes |EPR\rangle^{\otimes 2}, &\{\{M_i^{(x)} \mid x \in \mathbb{Z}_2^3\} \mid i \in [m(r)+n(r)]\}, \\ &\{\{N_i^{(x)} \mid x \in \mathbb{Z}_2^3\} \mid i \in [m(r)+n(r)]\}). \end{aligned} \tag{5.34}$$

such that

$$P_{A_r}(x,y|i,j) = \left(\langle\tilde{\psi}| \otimes \langle EPR|^{\otimes 2}\right) M_i^{(x)} \otimes N_j^{(y)} \left(|\tilde{\psi}\rangle \otimes |EPR\rangle^{\otimes 2}\right).$$

It can be checked that P_{A_r} is a perfect strategy of $A_r \boldsymbol{x} = 0$.

In this section, we introduce $Q_{p,r}$, which can be thought of as the combination of P_{A_r} and $\hat{Q}_{-\pi/p}$. The correlation $Q_{p,r} : [m(r)+n(r)] \times [m(r)+n(r)] \times \mathbb{Z}_2^3 \times \mathbb{Z}_2^3 \to \mathbb{R}_{\geq 0}$ is defined by its inducing strategy.

Define

$$\tilde{M}_i^{(x)} = \begin{cases} M_i^{(x)} & \text{if } i \in [m(r)+n(r)] \\ \overline{M}_0^{(x)} \otimes \mathbb{1}_{\mathbb{C}^2} \otimes \mathbb{1}_{\mathbb{C}^2} & \text{if } i = m(r)+n(r) \text{ and } x \leq 2 \\ \overline{M}_{i-m(r)-n(r)+2}^{(x)} \otimes \mathbb{1}_{\mathbb{C}^2} \otimes \mathbb{1}_{\mathbb{C}^2} & \text{if } i > m(r)+n(r) \text{ and } x \leq 2 \\ 0 & \text{otherwise.} \end{cases}$$

$$\tilde{N}_i^{(x)} = \begin{cases} N_i^{(x)} & \text{if } i \in [m(r)+n(r)] \\ \overline{N}_0^{(x)} \otimes \mathbb{1}_{\mathbb{C}^2} \otimes \mathbb{1}_{\mathbb{C}^2} & \text{if } i = m(r)+n(r) \text{ and } x \leq 2 \\ \overline{N}_{i-m(r)-n(r)+2}^{(x)} \otimes \mathbb{1}_{\mathbb{C}^2} \otimes \mathbb{1}_{\mathbb{C}^2} & \text{if } i > m(r)+n(r) \text{ and } x \leq 2 \\ 0 & \text{otherwise,} \end{cases}$$

where $M_i^{(x)}$ and $N_i^{(x)}$ are obtained from strategy S_{A_r} (eq. (5.34)), and $\overline{M}_i^{(x)}$ and $\overline{N}_i^{(x)}$ are obtained from strategy $S_{-\pi/p}$ (eq. (5.22)).

Definition 5.12. *The correlation $Q_{p,r} : [n(r)+m(r)+3] \times [n(r)+m(r)+3] \times \mathbb{Z}_2^3 \times \mathbb{Z}_2^3 \to \mathbb{R}_{\geq 0}$ is induced by the strategy*

$$\tilde{S} = (|\tilde{\psi}\rangle \otimes |EPR\rangle^{\otimes 2}, \{\{\tilde{M}_x^{(a)} \mid a \in [8]\} \mid x \in [n(r)+m(r)+3]\}$$
$$\{\{\tilde{N}_y^{(b)} \mid b \in [8]\} \mid y \in [n(r)+m(r)+3]\}).$$

such that

$$Q_{p,r}(a,b|x,y) = \left(\langle\tilde{\psi}| \otimes \langle EPR|^{\otimes 2}\right) \tilde{M}_x^{(a)} \otimes \tilde{N}_y^{(b)} \left(|\tilde{\psi}\rangle \otimes |EPR\rangle^{\otimes 2}\right).$$

Theorem 5.13. *Let S be an inducing strategy of $Q_{p,r}$ with a shared state $|\psi\rangle$. Then there exist an isometry $\Phi_A \otimes \Phi_B$ and a state $|junk\rangle$ such that $\| |junk\rangle \| = 1$ and*

$$\Phi_A \otimes \Phi_B(|\psi\rangle) = |junk\rangle \otimes |\tilde{\psi}\rangle$$

where $|\tilde{\psi}\rangle$ is defined in eq. (5.33).

To prove this theorem, we first prove the following proposition.

Proposition 5.14. *If a strategy with shared state $|\psi\rangle \in \mathcal{H}$ can induce $Q_{p,r}$, then there exist sub-normalized states $\{|\psi_j\rangle \mid 1 \leq j \leq p-1\}$ such that*

$$\| |\psi_j\rangle \|^2 = \frac{1}{p-1} \text{ for } 1 \leq j \leq p-1,$$
$$|\psi\rangle = \sum_{j=1}^{p-1} |\psi_j\rangle.$$

Proof. First observe that when $x, y \in [m(r) + n(r)]$,

$$Q_{p,r}(a, b|x, y) = P_{A_r}(a, b|x, y).$$

Let $U_A = M_{\tau^{-1}(u_1)} M_{\tau^{-1}(u_2)}$ and $U_B = N_{\tau^{-1}(u_1)} N_{\tau^{-1}(u_2)}$. By Lemma 4.19, we know $U_A U_B |\psi\rangle = |\psi\rangle$. Let $O_A = M_{m(r)} M_{m(r)+1}$ and $O_B = N_{m(r)} N_{m(r)+1}$. By Proposition 5.10, we know that

$$O_A U_A |\psi\rangle = U_A O_A^r |\psi\rangle,$$

$$O_B U_B |\psi\rangle = U_B O_B^r |\psi\rangle.$$

Next, we observe that

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{p-1}} \sum_{j=1}^{(p-1)/2} \omega_{2p}^{j} (|j\rangle|j\rangle + |p-j\rangle|p-j\rangle).$$

Define $f : \{m(r), m(r)+1, n(r)+m(r), n(r)+m(r)+1, n(r)+m(r)+2\} \to [5]$ by

$$f(x) = \begin{cases} x+1-m(r) \text{ if } x = m(r), m(r)+1, \\ x-n(r)-m(r) \text{ if } x = n(r)+m(r), \\ x+2-n(r)-m(r) \text{ otherwise.} \end{cases}$$

Then, we can check that When $x, y \in \{m(r), m(r)+1, n(r)+m(r), n(r)+m(r)+1, n(r)+m(r)+2\}$, and $a, b \in [3]$

$$Q_{p,r}(a,b|x,y) = \hat{Q}_{-\pi/p}(a,b|f(x),f(y)).$$

It implies that the conditions of Proposition 5.9 are satisfied and we can define $|\psi_j\rangle = (U_A U_B)^{\log_r j} |\psi_1\rangle$. The conditions satisfied by $|\psi_j\rangle$ are $\| |\psi_j\rangle \|^2 = 1/(p-1)$ and $\langle \psi_j | \psi_{j'} \rangle = 0$ if $j \neq j'$. Therefore, $\| \sum_{j=1}^{p-1} |\psi_j\rangle \| = 1$. What remains is to show that $\sum_{j=1}^{p-1} \langle \psi | \psi_j \rangle = 1$. Since $U_A^\dagger U_B^\dagger |\psi\rangle = |\psi\rangle$, we know that $\sum_{j=1}^{p-1} \langle \psi | \psi_j \rangle =$

$(p-1)\langle\psi|\psi_1\rangle$ and

$$\begin{aligned}\langle\psi|\psi_1\rangle =&\frac{1}{2}\langle\psi|(M^{(0)}_{n(r)+m(r)+1}+M^{(1)}_{n(r)+m(r)+1}-iM_{n(r)+m(r)+2}M_{n(r)+m(r)+1})|\psi\rangle\\ =&\frac{1}{p-1}-\frac{i}{2}\langle\psi|N_{n(r)+m(r)+2}M_{n(r)+m(r)+1}|\psi\rangle\\ =&\frac{1}{p-1},\end{aligned}$$

where $\langle\psi|N_{n(r)+m(r)+2}M_{n(r)+m(r)+1}|\psi\rangle=0$ comes from the correlation. Then the proposition follows. □

Proof of Theorem 5.13. Propositions 5.9 and 5.14 tell us that $|\psi\rangle=\sum_{j=1}^{p-1}|\psi_j\rangle$ where

$$|\psi_j\rangle=(U_AU_B)^{\log_r j}|\psi_1\rangle$$

$$O_A|\psi_j\rangle=\omega_p^{p-j}|\psi_j\rangle$$

$$O_B|\psi_j\rangle=\omega_p^{j}|\psi_j\rangle.$$

Then this theorem follows from Theorem 5.6. □

The significance the implication of Theorem 5.13 is summarized in the next theorem.

Theorem 5.15. *There exists an infinit set D of prime numbers such that for each $p\in D$, there exists a constant-sized correlation that can self-test the maximally entangled state of local dimension $(p-1)$.*

Proof. There exists $r\in\{2,3,5\}$ such that r is a primitive root of infinitely many primes [27]. It suffices to choose D to be the set of primes whose primitive root is r. Then, by Theorem 5.13, for each $p \in D$, $Q_{p,r}$ of size $\Theta(r^2)$ can self-test a maximally entangled state of local dimension $p-1$. $\square$

This is the first result that shows that fixed-sized correlations can self-test maximally entangled states of unbounded dimension.

Chapter 6: Minsky machine and Kharlampovich-Myasnikov-Sapir group

In this chapter, we construct a group that is used in the main result of this dissertation. To construct this group, we first introduce the Minsky machine in Section 6.1, a semi-group that can simulate a Minsky machine in Section 6.2, and a group that can simulate a Minsky machine in Section 6.3, which is also known as the Kharlampovich-Myasnikov-Sapir group. In Section 6.4, we extend a Kharlampovich-Myasnikov-Sapir group in a particular way and prove various properties of this extended group.

6.1 Minsky machine

A *k-glass Minsky Machine* [30], denoted by MM_k, consists of k glasses, where each glass can hold arbitrarily many coins. Just like a Turing machine, a configuration of MM_k describes which state the machine is in and how many coins are in each of the glasses. A computation running on MM_k is a sequence of commands, where each command maps one configuration to another. Each command involves at most one of the two operations on each glass, which are adding a coin to a glass and removing a coin from a non-empty glass.

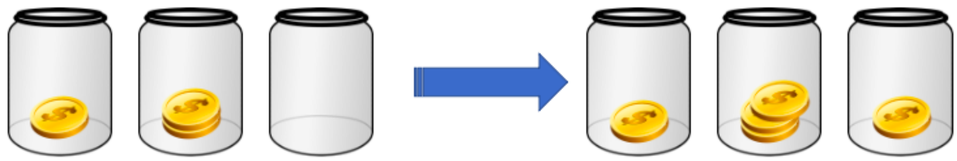

Figure 6.1: The visualization of a command that maps the configuration $(i;1,2,0)$ to $(j;1,3,1)$.

More formally, the states of MM_k are numbered from 0 to N where 0 is the final accept state and 1 is the starting state, so a *configuration of* MM_k is in $[N+1] \times (\mathbb{Z}_{\geq 0})^{\times k}$ and of the form $(i;n_1,n_2,\ldots n_k)$ where i is the current state number and each $n_j \geq 0$ represents the number of coins in the j-th glass. The *accept configuration* is $(0;0,0,\ldots 0)$ and the *starting configuration* with input m is $(1;m,0,\ldots 0)$.

Next, we formally introduce the commands of MM_k. A command may be of one of the following four forms.

1. When the state is i, add a coin to each of the glasses numbered $j_1, j_2 \ldots j_l$ where $l \leq k$, and go to state j. This command is encoded as

$$i; \to j; Add(j_1, j_2, \ldots j_l).$$

2. When the state is i, if the glasses numbered $j_1, j_2, \ldots j_l$ where $l \leq k$ are all nonempty, then remove a coin from each of the glasses numbered $j_1, j_2, \ldots j_l$,

and go to state j. This command is encoded as

$$i; n_{j_1} > 0, \dots n_{j_l} > 0 \to j; Sub(j_1, j_2, \dots j_l).$$

3. When the state is i, if the glasses numbered $j_1, j_2, \dots j_l$ where $l \leq k$ are empty, go to state j. This command is encoded as

$$i; n_{j_1} = 0, n_{j_2} = 0, \dots n_{j_l} = 0 \to j.$$

4. When the state is i, accept. This command is encoded as

$$i; \to 0.$$

If at any given state i, there is at most one command that can be applied, the Minsky machine is *deterministic*. Otherwise, the Minsky machine is *non-deterministic*.

The importance of Minsky machines is summarized in the next theorem. We first define what a *recursively enumerable* (RE) set is.

Definition 6.1. *A subset S of the set of natural numbers $(\mathbb{N})$ is **recursively enumerable** if there is an algorithm such that the algorithm accepts an input s if and only if $s \in S$.*

Theorem 6.2. *Let X be a recursively enumerable set of natural numbers. Then there exists a 3-glass deterministic Minsky machine MM_3 such that MM_3 takes the configuration $(1; n, 0, 0)$ to the accept configuration $(0; 0, 0, 0)$ if and only if $n \in X$.*

The proof can be found in the proof of [31, Theorem 2.7], so we omit it here. In the rest of the dissertation, we focus on 3-glass Minsky machines.

6.2 A semigroup to simulate MM_3

We first introduce concepts for semigroups that are necessary for this section, especially, the presentation of a semigroup.

Definition 6.3. *A **semigroup** is a set S with an operation $\cdot$, such that*

1. *for any $a, b \in S$, $a \cdot b \in S$;*

2. *for any $a, b, c \in S$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*

Definition 6.4. *A **semigroup with a zero element** is a semigroup S such that there exists an element 0, for which $0 \cdot a = a \cdot 0 = 0$ for any $a \in S$.*

The element 0 is also called an *absorbing element*.

Definition 6.5. *A **semigroup with an identity element** is a semigroup S such that there exists an element e, for which $e \cdot a = a \cdot e = a$ for any $a \in S$.*

To define the notion of a presentation of a semigroup, we first define notions related to congruence and then we define what a free semigroup is.

Definition 6.6. *For any semigroup S and $R \subseteq S \times S$, we define*

$$R^c = \{(a, b), (xa, xb), (ay, by), (xay, xby) \mid \text{ for all } (a, b) \in R \text{ and } x, y \in S\}.$$

Definition 6.7. *For any semigroup S and $R \subseteq S \times S$, let $R^{\#}$ be a subset of $S \times S$ such that $(a, b) \in R^{\#}$ if and only if $(a, b) \in R^c$, or there exist $\{z_i \mid i \in [n]\}$ such that $(a, z_0), (z_{n-1}, b) \in R^c$ and for each $0 \leq i \leq n-2$, $(z_i, z_{i+1}) \in R^c$ or $(z_{i+1}, z_i) \in R^c$. Them, $R^{\#}$ is called the* ***smallest congruence containing*** *R.*

Definition 6.8. *Let A be a non-empty set. The* ***free semigroup on*** *A, denoted by A^+, consists of all finite words $a_1 a_2 \ldots a_n$ where $a_i \in A$ and the binary operation is defined on A^+ by juxtaposition:*

$$(a_1 a_2 \ldots a_n)(b_1 b_2 \ldots b_m) = a_1 a_2 \ldots a_n b_1 b_2 \ldots b_m.$$

Definition 6.9. *Let A be a non-empty set, A^+ be the free semigroup on A and $R \subseteq A^+ \times A^+$. If there is a homomorphism ϕ from A^+ onto a semigroup S, such that $\{(x, y) \mid \phi(x) = \phi(y)\} = R^{\#}$, then we say a* ***presentation*** *of S is $\langle A : R \rangle$.*

If both A and R are finite, then we say S is *finitely-presented*. The relation $(a, b) \in R$ is written as $a = b$. Intuitively, S is the quotient of the free semigroup generated by A by the equivalence relations in R, which is an analogue of a group presentation (Definition 3.9). For more details about semigroup presentations, we refer to [39, Chapter 1.4 to 1.6].

Next, we define a finitely-presented semigroup with a zero element that can simulate a 3-glass Minsky machine.

Definition 6.10. *Let MM_3 be a 3-glass Minsky machine with states: $0, 1, \ldots N$. We define a semigroup $H(\mathsf{MM}_3)$ by giving the set of generators and the set of relations below.*

The set of generators of $H(\mathsf{MM}_3)$ *consists of* $\{q_i \mid 0 \le i \le N\}$ *and* $\{a_i, A_i \mid 1 \le i \le 3\}$.

The set of relations of $H(\mathsf{MM}_3)$ *consists of*

- $\{a_i a_j = a_j a_i, a_i A_j = A_j a_i, A_i A_j = A_j A_i \mid 1 \le i \ne j \le 3\}$;
- $a_i q_j = A_i q_j = 0$ *for all* $1 \le i \le 3$ *and* $0 \le j \le N$;
- $A_i a_i = 0$ *if* $1 \le i \le 3$;
- *for each command of the form* $i \to Add(k_1, \ldots k_m); j$, *the relation* $q_i = q_j a_{k_1} \ldots a_{k_m}$ *with* $m \le 3$;
- *for each command of the form* $i, n_{k_1} > 0, \ldots n_{k_m} > 0 \to j; Sub(n_{k_1}, \ldots n_{k_m})$, *the relation* $q_i a_{k_1} \ldots a_{k_m} = q_j$ *with* $m \le 3$; *and*
- *for each command of the form* $i, n_{k_1} = 0, \ldots n_{k_m} = 0 \to j$, *the relation* $q_i A_{k_1} \ldots A_{k_m} = q_j A_{k_1} \ldots A_{k_m}$ *with* $m \le 3$.

For the configuration $c = (i; n_1, n_2, n_3)$ of MM_3, the corresponding semigroup element is $w_H(c) = q_i a_1^{n_1} a_2^{n_2} a_3^{n_3} A_1 A_2 A_3$. Intuitively, q_j corresponds to the state j of MM_3; for $i = 1, 2, 3$, a_i represents a coin for the glass numbered i. Since a_i does not commute with A_i and $A_i a_i = 0$ for $1 \le i \le 3$, the A_i's are introduced to allow us to check if the glass-i is empty.

Theorem 6.11. *Let* MM_3 *be a 3-glass Minsky machine and* $H(\mathsf{MM}_3)$ *be defined as in Definition 6.10. Then, a configuration* c' *can be obtained from a configuration* c *of* MM_3 *by applying commands of* MM_3 *if and only if* $w_H(c') = w_H(c)$ *meaning that* $w_H(c')$ *can be obtained from* $w_H(c)$ *by applying the defining relations of* $H(\mathsf{MM}_3)$.

The proof can be found in [31, Property 3.1 and 3.2].

6.3 Kharlampovich-Myasnikov-Sapir group

For a 3-glass Minsky machine MM_3, the *Kharlampovich-Myasnikov-Sapir group* (KMS group) $G(\mathsf{MM}_3)$ is a finitely presented group with generator set $S(\mathsf{MM}_3)$ and relation set $R(\mathsf{MM}_3)$, where $S(\mathsf{MM}_3)$ and $R(\mathsf{MM}_3)$ are defined below. Note that the definitions are obtained from [31, Section 4.1].

Intuitively, $G(\mathsf{MM}_3)$ can simulate MM_3 because the semigroup $H(\mathsf{MM}_3)$ is embedded in $G(\mathsf{MM}_3)$. The image of $q_i a_1^{n_1} a_2^{n_2} a_3^{n_3} A_1 A_2 A_3$ in $G(\mathsf{MM}_3)$ is $x(q_i A_0) \circledast a_1^{\circledast n_1} \circledast a_2^{\circledast n_2} \circledast a_3^{\circledast n_3} \circledast A_1 \circledast A_2 \circledast A_3$, where the symbol $x(q_i A_0)$ and the operation $\circledast$ are defined below.

6.3.1 Baumslag-Remeslennikov-conjoint

We introduce a lemma, which tells us that certain solvable groups are finitely presented. This lemma gives us important intuitions behind the structure of $G(\mathsf{MM}_3)$. Since the lemma is first introduced by Baumslag [40] and Remeslennikov [41], the sets satisfying the conditions of the following lemma are called *Baumslag-Remeslennikov-conjoints* (BR-conjoints).

Lemma 6.12. *Suppose that a group H is generated by three sets X, $F = \{a_i \mid i \in [m]\}$ and $F' = \{a'_i \mid i \in [m]\}$ such that*

1. *$x^2 = e$ for each $x \in X$;*
2. *The subgroup generated by $F \cup F'$ is abelian;*
3. *For every $a_i \in F$ and $x \in X$, $x^{a_i} x^{-1} = x^{a'_i}$;*

4. $[x_1^{a_0^{\beta_0}\ldots a_{m-1}^{\beta_{m-1}}}, x_2] = e$ *for every* $x_1, x_2 \in X$ *and* $\beta_0, \beta_1, \ldots \beta_{m-1} \in \{0, 1, -1\}$.

Then, the normal subgroup generated by X in H is abelian, and H is solvable.

This lemma is based on Lemma 4.1 of [31], Before we prove Lemma 6.12, we first prove some facts about commutators, which will be used in the proof.

Proposition 6.13. *Let G be a group and $a, b, c \in G$. Then,*

1. $[a, b] = e \iff [a^c, b^c] = e$;

2. $[a, b] = [a, c] = e$ *implies that* $[a, bc] = e$; *and*

3. $[a, bc] = [a, b] = e$ *implies that* $[a, c] = e$.

Proof. We prove the three results one by one. The first result follows $[a^c, b^c] = [a, b]^c$.

The second result follows

$$a^{-1}(bc)^{-1}abc = a^{-1}c^{-1}b^{-1}abc = a^{-1}c^{-1}ac = e,$$

where we use the fact that $ab = ba$. The third result follows the same derivation.

□

Proof of Lemma 6.12. We first prove that the normal subgroups generated by X in H, denoted by $\langle X \rangle^H$, is abelian, then the second conclusion follows from $H / \langle X \rangle^H = \langle F \cup F' \rangle$.

Since $x^2 = e$ for all $x \in X$, then $x^{a'_i} = x^{a_i}x$ for $i \in [m]$. To show the normal subgroup generated by X in H is abelian, it suffices to show that

$$\left[x_1^{\prod_{i\in[m]} a_i^{n_i} \prod_{j\in[m]} a_j'^{\alpha_j}}, x_2^{\prod_{i\in[m]} a_i^{k_i} \prod_{j\in[m]} a_j'^{\beta_j}}\right] = e$$

for all $x_1, x_2 \in X$ and $n_i, \alpha_j, k_i, \beta_j \in \mathbb{Z}$. This is because every element of $\langle X\rangle^H$ can be expressed as a product of elements of the form $x^{\prod_{i\in[m]} a_i^{n_i} \prod_{j\in[m]} a_j'^{\alpha_j}}$. Then, for any $x \in X$, since $x^{a'_i} = x^{a_i}x$ for all $i \in [m]$ and $\langle F \cup F'\rangle$ is abelian, $x^{\prod_{i\in[m]} a_i^{n_i} \prod_{j\in[m]} a_j'^{\alpha_j}}$ can be expressed as a product of elements of the form $x^{\prod_{i\in[m]} a_i^{n'_i}}$ for some $n'_i \in \mathbb{Z}$. Hence, it suffices to show

$$\left[x_1^{\prod_{i\in[m]} a_i^{n_i}}, x_2^{\prod_{i\in[m]} a_i^{k_i}}\right] = e$$

for all $x_1, x_2 \in X$ and $n_i, k_i \in \mathbb{Z}$. Then, notice that

$$\left[x_1^{\prod_{i\in[m]} a_i^{n_i}}, x_2^{\prod_{i\in[m]} a_i^{k_i}}\right] = \left[x_1^{\prod_{i\in[m]} a_i^{n_i-k_i}}, x_2\right]^{\prod_{i\in[m]} a_i^{k_i}}.$$

It suffices to show

$$\left[x_1^{\prod_{i\in[m]} a_i^{n_i}}, x_2\right] = e \text{ for all } x_1, x_2 \in X \text{ and } n_i \in \mathbb{Z}. \tag{6.1}$$

We prove it by induction.

The base case that $|n_i| \leq 1$ for all $i \in [m]$ follows from the condition of the lemma. Suppose eq. (6.1) is true for all $|n_i| < N$ for all $i \in [m]$. Noticing that for any $S \subseteq [m]$

$$[x_1^{\prod_{i\in S} a_i^{-n_i-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2] = [x_1, x_2^{\prod_{i\in S} a_i^{n_i+1} \prod_{j\in[m]\setminus S} a_j^{-n_j}}]^{\prod_{i\in S} a_i^{-n_i-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}$$

where $n_i \geq 0$. Since the choices of x_1 and x_2 are arbitrary, it suffices to prove that for any index set $S \subseteq [m]$

$$[x_1^{\prod_{i\in S} a_i^{N} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2] = e. \tag{6.2}$$

In this step, we use induction on the size of $|S|$. In the base case that $|S| = 1$, we can assume $S = \{0\}$ without loss of generality. By the assumption of the outer induction, we know

$$\begin{aligned} e =& [x_1^{a_0^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2]^{a_0'} \\ =& [x_1^{a_0^{N} \prod_{j\in[m]\setminus S} a_j^{n_j}} x_1^{a_0^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2^{a_0} x_2]. \end{aligned}$$

Again by the assumption of the outer induction, we know

$$[x_1^{a_0^{N} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2^{a_0}] = [x_1^{a_0^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2^{a_0}] = e,$$

so, by Point (2) of Proposition 6.13,

$$[x_1^{a_0^{N} \prod_{j\in[m]\setminus S} a_j^{n_j}} x_1^{a_0^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2^{a_0}] = e.$$

Then, by Point (3) of Proposition 6.13,

$$[x_1^{a_0^N \prod_{j\in[m]\setminus S} a_j^{n_j}} x_1^{a_0^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2] = e.$$

Using the fact that $[x_1^{a_0^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2] = e$, we can use Point (3) of Proposition 6.13 to prove that

$$[x_1^{a_0^N \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2] = e,$$

which completes the base case of the inner induction.

Now, suppose eq. (6.2) is true for all $S \subseteq [m]$ with $|S| < k \leq m$. Consider the case that $|S| = k$. By the assumption, we know that

$$\begin{aligned} e =& [x_1^{\prod_{i\in S} a_i^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2]^{\prod_{i\in S} a_i'} \\ =& [x_1^{\prod_{i\in S} a_i' \prod_{i\in S} a_i^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2^{\prod_{i\in S} a_i'}] \\ =& [\prod_{S'\subseteq S} x_1^{(\prod_{i\in S'} a_i) \prod_{i\in S} a_i^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, \prod_{S'\subseteq S} x_2^{\prod_{i\in S'} a_i}]. \end{aligned}$$

Again, by the assumption of the inner induction, we know that for any $S'' \subseteq S$ with $|S''| \geq 1$,

$$[\prod_{S'\subseteq S} x_1^{(\prod_{i\in S'} a_i) \prod_{i\in S} a_i^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2^{\prod_{i\in S''} a_i}] = e.$$

Then, using Point (3) of Proposition 6.13 we can deduce that

$$[\prod_{S' \subseteq S} x_1^{(\prod_{i\in S'} a_i)\prod_{i\in S} a_i^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2] = e.$$

Since the assumption of the inner induction tells us that for any $S' \neq S$,

$$[x_1^{(\prod_{i\in S'} a_i)\prod_{i\in S} a_i^{N-1} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2] = e.$$

Using Point (3) of Proposition 6.13 we can deduce that

$$[x_1^{\prod_{i\in S} a_i^{N} \prod_{j\in[m]\setminus S} a_j^{n_j}}, x_2] = e.$$

By the principle of inductive proof, the inner and outer inductions are complete.

□

Definition 6.14. *Let sets F, F' and X be as defined in Lemma 6.12. If they satisfy the conditions of Lemma 6.12, then we say a_i' are **BR-conjoints** to a_i for $i \in [m]$ with respect to X.*

6.3.2 Definition of $G(\mathsf{MM}_3)$

Let U be the commutative semigroup with identity generated by $\{A_0, A_1, A_2, A_3\}$, and let

$$U' = \{u \in U \mid \text{ there exist } v \in U \text{ such that } vu = A_0A_1A_2A_3 \text{ in } U\},$$

be a subset of U.

We define the *generator set* $S(\mathsf{MM}_3)$ of $G(\mathsf{MM}_3)$ as the union of L_0, L_1 and L_2. Let L_0 be a finite set indexed by $(\{q_i \mid 0 \leq i \leq N\} \cdot U') \subseteq H(\mathsf{MM}_3)$ denoted by

$$L_0 = \{x(q_j u) \mid u \in U', 0 \leq j \leq N\}.$$

Let

$$L_1 = \{A_0, A_1, A_2, A_3\}, \text{ and}$$
$$L_2 = \{a_i, a_i', \tilde{a}_i, \tilde{a}_i' \mid i = 1,2,3\},$$

Note that the three sets L_0, L_1 and L_2 should be understood as disjoint sets with no predefined algebraic structure. Then, the generator set $S(\mathsf{MM}_3) = L_0 \sqcup L_1 \sqcup L_2$.

Let

$$M_0 = \{\tilde{a}_i, \tilde{a}_i', A_0 \mid i = 1,2,3\}$$
$$M_i = \{a_i, a_i', A_i\}$$

for $i = 1,2,3$. The *relation set* $R(\mathsf{MM}_3)$ contains

R.1 $\{x^2 = e \mid x \in L_0\} \cup \{[x_1, x_2] = e \mid x_1, x_2 \in L_0\}$ (these relations imply that L_0 generates an abelian 2-group);

R.2 $\{A_i^2 = e \mid i \in [4]\} \cup \{[A_i, A_j] = e \mid i, j \in [4]\}$ (these relations imply that L_1 generates an abelian 2-group);

R.3 $\{[a_i, a'_j] = [a_i, \tilde{a}_k] = [a_i, \tilde{a}'_l] = [a'_j, \tilde{a}_k] = [a'_j, \tilde{a}'_l] = [\tilde{a}_k, \tilde{a}'_l] = [a_i, a_j] = [a'_i, a'_j] = [\tilde{a}_i, \tilde{a}_j] = [\tilde{a}'_i, \tilde{a}'_j] = e \mid 1 \leq i, j, k, l \leq 3\}$ (these relations imply that L_2 generates an abelian group);

R.4 $\{[y, z] = e \mid y \in M_i, z \in M_j$ with $i \neq j \in [4]\}$;

R.5 $\{A_i^{a_i^{-1}} A_i^{-1} = A_i^{(a'_i)^{-1}} \mid i = 1, 2, 3\}$ (these relations imply that $\{a_i^{-1}\}$ and $\{a_i'^{-1}\}$ are BR-conjoints with respect to $\{A_i\}$);

R.6 $\{A_0^{\tilde{a}_i'^{-1}} = A_0^{\tilde{a}_i^{-1}} A_0^{-1} \mid i = 1, 2, 3\} \cup \{[A_0^{\tilde{a}_1^{\alpha_1} \tilde{a}_2^{\alpha_2} \tilde{a}_3^{\alpha_3}}, A_0] = e \mid \alpha_1, \alpha_2, \alpha_3 \in \{0, 1, -1\}\}$;

R.7 $\{[x(q_j u), A_i] = x(q_j u A_i) \mid j \in [N+1], i \in [4], u \in U'$ and u is generated by $\{e, A_0, A_1, A_2, A_3\} \setminus \{A_i\}\}$;

R.8 $\{x(q_j u)^{a_i} x(q_j u) = x(q_j u)^{a'_i} \mid j \in [N+1], 1 \leq i \leq 3, u \in U'$ and u is generated by $\{e, A_0, A_1, A_2, A_3\} \setminus \{A_i\}\}$;

R.9 $\{[x(q_j u), z] = e \mid j \in [N+1], z \in M_i, i \in [4], u \in U'$ and the generating set of u contains $A_i\}$;

R.10 $\{x(q_j)^{a_i} = x(q_j)^{\tilde{a}_i}, x(q_j)^{a'_i} = x(q_j)^{\tilde{a}'_i} \mid j \in [N], i = 1, 2, 3\}$;

R.11 $\{[x(q_i u)^{a_1^{\beta_1} a_2^{\beta_2} a_3^{\beta_3}}, x(q_j v)] = e \mid u, v \in U, \beta_1, \beta_2, \beta_3 \in \{0, 1, -1\}, i, j \in [N]\}$; and

R.12 The relations corresponding to the commands of MM_3 defined below. For every $f \in G(\mathsf{MM}_3)$, denote

$$f \circledast a_j = f^{-1} f^{a_j} (f^{-1})^{a_j^{-1}} f^{a_j'^{-1}},$$

and

$$f \circledast A_j = [f, A_j]$$

for $j = 1, 2, 3$. We denote $(\ldots(t_1 \circledast t_2) \circledast \ldots) \circledast t_m$ by $t_1 \circledast t_2 \ldots \circledast t_m$ and $t_1 \circledast \underbrace{t_2 \circledast \ldots \circledast t_2}_{\text{n times}}$ by $t_1 \circledast t_2^{\circledast n}$. The relations for the commands of MM_3 can be translated from the commands using the following rules:

- if the command is $i; \to j; Add(k_1, \ldots k_l)$, the relation is

$$x(q_i A_0) = x(q_j A_0) \circledast a_{k_1} \ldots \circledast a_{k_l};$$

- if the command is $i; n_{k_1} > 0 \ldots n_{k_l} > 0 \to j; Sub(k_1, \ldots k_l)$, the relation is

$$x(q_i A_0) \circledast a_{k_1} \ldots \circledast a_{k_l} = x(q_j A_0);$$

- if the command is $i; n_{k_1} = 0 \ldots n_{k_l} = 0 \to j$, the relation is

$$x(q_i A_0) \circledast A_{k_1} \circledast A_{k_2} \circledast \ldots A_{k_l} = x(q_j A_0) \circledast A_{k_1} \circledast A_{k_2} \circledast \ldots A_{k_l};$$

- if the command is $i; \to 0;$, the relation is $x(q_i A_0) = x(q_0 A_0)$.

Note that in the original definition [31], there is a parameter p. In the definition above, we choose $p = 2$. Relations **R.4** and **R.6** imply that $\{(\tilde{a}_i')^{-1} \mid i = 1,2,3\}$ are BR-conjoints of the set $\{\tilde{a}_i^{-1} \mid i = 1,2,3\}$ with respect to $\{A_0\}$.

We record the following lemmas from [31] about the structure of $G(\mathsf{MM}_3)$

Lemma 6.15 (Lemma 4.5 of [31])**.** *The normal subgroup T of $G(\mathsf{MM}_3)$ generated as a normal subgroup by all the elements $x(q_i u)$ for $u \in U'$ and $0 \le i \le N$ is abelian and of exponent 2.*

Lemma 6.16 (Lemma 4.4 of [31])**.** *The subgroup $\langle L_1 \cup L_2 \rangle$ is solvable. If we define $H_1 = \langle L_1 \rangle$ and $H_2 = \langle L_2 \rangle$, then*

$$\langle H_1 \cup H_2 \rangle = H_1^{H_2} \rtimes H_2,$$

where $H_1^{H_2}$ is an abelian normal subgroup of exponent 2 and H_2 is abelian.

Theorem 6.17. *The group $G(\mathsf{MM}_3)$ is solvable.*

Proof. From the presentation of $G(\mathsf{MM}_3)$ we know

$$G(\mathsf{MM}_3) = T \rtimes \langle H_1 \cup H_2 \rangle,$$

where T defined in Lemma 6.15 is an abelian normal subgroup and $\langle H_1 \cup H_2 \rangle$ is solvable following the proposition above, which completes the proof. □

Note that this theorem is independent of whether MM_3 is deterministic or not.

Next we explain why we say $G(\mathsf{MM}_3)$ can simulate MM_3. For each configuration $c = (i; n_1, n_2, n_3)$, the corresponding word is

$$w(c) = x(q_i A_0) \circledast a_1^{\circledast n_1} \circledast a_2^{\circledast n_2} \circledast a_3^{\circledast n_3} \circledast A_1 \circledast A_2 \circledast A_3.$$

Theorem 6.18 (Theorem 4.3 point (b) of [31])**.** *For a 3-glass Minsky machine* MM_3*, let* $G(\mathsf{MM}_3)$ *be the group defined above and* $H(\mathsf{MM}_3)$ *be the semigroup defined in the previous section. Then, the equality*

$$\begin{aligned}&x(q_i A_0) \circledast a_1^{\circledast n_1} \circledast a_2^{\circledast n_2} \circledast a_3^{\circledast n_3} \circledast A_1^{\circledast \alpha_1} \circledast A_2^{\circledast \alpha_2} \circledast A_3^{\circledast \alpha_3} \\ =&x(q_j A_0) \circledast a_1^{\circledast m_1} \circledast a_2^{\circledast m_2} \circledast a_3^{\circledast m_3} \circledast A_1^{\circledast \beta_1} \circledast A_2^{\circledast \beta_2} \circledast A_3^{\circledast \beta_3}\end{aligned}$$

for $\alpha_k, \beta_k \in \{0,1\}$*,* $n_k, m_k \in \mathbb{N}$ *and* $k \in \{1,2,3\}$ *is true in* $G(\mathsf{MM}_3)$ *if and only if the equality*

$$q_i a_1^{n_1} a_2^{n_2} a_3^{n_3} A_1^{\alpha_1} A_2^{\alpha_2} A_3^{\alpha_3} = q_j a_1^{m_1} a_2^{m_2} a_3^{m_3} A_1^{\beta_1} A_2^{\beta_2} A_3^{\beta_3}$$

is true in $H(\mathsf{MM}_3)$*.*

We omit the proof as it can be found in Section 4.1 of [31].

Among all such words, we are particularly interested in the word corresponding to the starting configuration of input n, which is defined by

$$w(n) := x(q_1 A_0) \circledast a_1^{\circledast n} \circledast A_1 \circledast A_2 \circledast A_3,$$

and In the word corresponding to the final accept configuration, which is defined by

$$w(a) := x(q_0 A_0) \circledast A_1 \circledast A_2 \circledast A_3.$$

When the input is 0, $w(0) = x(q_1 A_0) \circledast A_1 \circledast A_2 \circledast A_3$. Relations **R.1**, **R.8** and **R.12** imply that $w(a) = x(q_0 A_0 A_1 A_2 A_3)$, $w(0) = x(q_1 A_0 A_1 A_2 A_3)$, and $w(a)^2 = w(0)^2 = e$.

Corollary 6.19. *Let X be a recursively enumerable set. Then, there exist a Minsky machine MM_3 and a KMS group $G(\mathsf{MM}_3)$ such that in $G(\mathsf{MM}_3)$, $w(n) = w(a)$ if and only if $n \in X$.*

This corollary follows easily from Theorems 6.2, 6.11 and 6.18 by choosing MM_3 to be a deterministic Minsky machine that enumerates X.

Recall the definition of extended homogeneous linear-plus-conjugacy group (Definition 3.54).

Proposition 6.20. *Let MM_3 be a 3-glass Minsky machine. Then, there is a presentation of $G(\mathsf{MM}_3)$ as an extended homogeneous-linear-plus-conjugacy group in which $w(0)w(a)$ is equal in $G(\mathsf{MM}_3)$ to one of the involutary generators x_j.*

This proposition allows us to reduce the problem of determining if a correlation is quantum to the problem of determining if $w(0)w(a) = e$ in $G(\mathsf{MM}_3)$.

To prove Proposition 6.20, we use following lemma, which is first proved in [7].

Lemma 6.21 (Lemma 42 of [7])**.** *Suppose $K = \langle S : R \rangle$ is a finitely presented group satisfying the following properties:*

1. *The set S is divided into three subsets L_0, L_1, and L_2.*
2. *The relations in R come in three types:*
   (a) *R contains the relation $x^2 = e$ for all $x \in L_0 \cup L_1$.*
   (b) *R contains commuting relations of the form $xy = yx$, for certain pairs $x, y \in S$.*
   (c) *For every other relation $r \in R$, there are some subsets $S_1 \subseteq S$ and $S_0 \subseteq (L_0 \cup L_1) \cap S_1$ such that $r \in \langle S_0 \rangle^{\mathcal{F}(S_1)}$, and the image of $\langle S_0 \rangle^{\mathcal{F}(S_1)}$ in K is abelian, where $\langle S_0 \rangle^{\mathcal{F}(S_1)}$ denotes the normal subgroup generated by S_0 in $\mathcal{F}(S_1)$.*

Then K is an extended homogeneous-linear-plus-conjugacy group. Futhermore, if $S_0 \subseteq S_1 \subseteq S$ are two subsets such that $S_0 \subseteq L_0 \cup L_1$, and the image of $\langle S_0 \rangle^{\mathcal{F}(S_1)}$ in K is abelian, then for every $w \in \langle S_0 \rangle^{\mathcal{F}(S_1)}$, there is a presentation of K as an extended homogeneous-linear-plus-conjugacy group in which w is equal in K to one of the involutary generators x_j.

Proof of Proposition 6.20. By the definition of $G(\mathsf{MM}_3)$, Lemma 6.15 and Lemma 6.16, $G(\mathsf{MM}_3)$ satisfies the conditions of Lemma 6.21. Moreover,

$$w(0)w(a) = x(q_1 A_0 A_1 A_2 A_3)x(q_1 A_0 A_1 A_2 A_3) \in \langle L_0 \rangle,$$

and $\langle L_0 \rangle$ is abelian in $G(\mathsf{MM}_3)$, then this corollary follows from Lemma 6.21. $\square$

6.4 Extending a Kharlampovich-Myasnikov-Sapir group

This section is devoted to proving the following lemma.

Lemma 6.22. *Let $r \in \{2, 3, 5\}$ be an integer that is the primitive root of infinitely many primes, let $p(n)$ be the n-th prime whose primitive root is r, and let X be a recursively enumerable set of positive integers.*

Then, there exists a finitely presented group H, which has group elements t and x, such that $x^2 = e$ in H, $H/\langle t^{p(n)} = e \rangle$ is sofic, and

$$x = e \text{ in } H/\langle t^{p(n)} = e \rangle \iff n \in X. \tag{6.3}$$

Moreover, there is a finite presentation $\langle S : R \rangle$ of H as an extended homogeneous linear-plus-conjugacy group such that $t, x \in S$.

To prove Lemma 6.22, we first consider a 3-glass Minsky machine that can enumerate a specific recursively enumerable set.

Definition 6.23. *Let X be a recursively enumerable set and $r \in \{2, 3, 5\}$ be an integer that is the primitive root of infinitely many primes. Denote the n-th prime whose* *primitive root is r by $p(n)$. Then, let $P_{X,r}$ denote the set*

$$P_{X,r} := \{p(n) \mid n \in X\}.$$

Proposition 6.24. *The set $P_{X,r}$ is recursively enumerable.*

Proof. First notice that the set P of all the primes whose primitive root is r is infinite and computable. We show $P_{X,r}$ is recursively enumerable by constructing an algorithm A that accepts $q \in \mathbb{N}$ if and only if $q \in P_{X,r}$.

Let A_X be the algorithm that accepts $x \in \mathbb{N}$ if and only if $x \in X$. By the definition of recursively enumerable sets, when $n \notin X$, A_X may reject it or work indefinitely long. Given input q, A first checks if $q \in P$. If q is not in P, it rejects q. If q is in P, A also computes a positive integer n such that $q = p(n)$. Then A runs A_X with input n and accepts if and only if A_X accepts. Hence, A can accept each $q \in P_{X,r}$ in a finite amount of time. $\square$

Let $\mathbf{MM}_3$ be a 3-glass Minsky machine that accepts $n \in \mathbb{N}$ if and only if $n \in P_{X,r}$, whose existence follows from Theorem 6.2. Let $G(\mathbf{MM}_3) = \langle S_G : R_G \rangle$ be the KMS group of $\mathbf{MM}_3$. This section is devoted to studying the properties of

$$G := \frac{G(\mathbf{MM}_3) * \mathcal{F}(\{t\})}{\langle [t, a_1] = [t, a_1'] = e, t^{-1}x(q_1 A_0)t = x(q_1 A_0) \circledast a_1 \rangle}. \tag{6.4}$$

Note that

$$G \cong \langle S_G \cup \{t\} : R_G \cup \{[t, a_1] = [t, a_1'] = e, t^{-1}x(q_1 A_0)t = x(q_1 A_0) \circledast a_1\} \rangle.$$

The proof of Lemma 6.22 is divided into five propositions. The propositions involve two new related groups: $G_{p(n)}(\mathsf{MM}_3)$ and $\overline{G_{p(n)}(\mathsf{MM}_3)}$, defined by

$$\begin{aligned} G_{p(n)}(\mathsf{MM}_3) =& \frac{G(\mathsf{MM}_3)}{\langle x(q_1A_0) \circledast a_1^{\circledast p(n)} = x(q_1A_0)\rangle}, \\ \overline{G_{p(n)}(\mathsf{MM}_3)} =& \frac{G}{\langle x(q_1A_0) \circledast a_1^{\circledast p(n)} = x(q_1A_0), t^{p(n)} = e\rangle}. \end{aligned}$$

Proposition 6.25. $G_{p(n)}(\mathsf{MM}_3) \leq \overline{G_{p(n)}(\mathsf{MM}_3)}$.

Proof. Let H be the subgroup of $\overline{G_{p(n)}(\mathsf{MM}_3)}$ generated by $x(q_1A_0)$, a_1 and a_1'. The following relations hold in H:

$$\begin{aligned} & x(q_1A_0)^2 = [a_1, a_1'] = e, \\ & x(q_1A_0)^{a_1'} = x(q_1A_0)^{a_1} x(q_1A_0), \\ & [x(q_1A_0)^{a_1^{\alpha_1}}, x(q_1A_0)] = e \text{ for } \alpha_1 \in \{-1, 0, 1\}, \\ & x(q_1A_0) = x(q_1A_0) \circledast a_1^{\circledast p(n)}. \end{aligned}$$

Let K be the subgroup generated by a_1 and a_1' in H.

We first show that $K = \langle a_1, a_1' : [a_1, a_1'] = e\rangle$. Consider a homomorphism

$$\psi : \mathcal{F}(S(\mathsf{MM}_3)) \to \langle b_1, b_2 : [b_1, b_2] = e\rangle$$

defined by

$$\psi(a_1) = b_1$$

$$\psi(a_1') = b_2$$

$$\psi(s) = e \text{ for all } s \in S(\mathsf{MM}_3) \setminus \{a_1, a_1'\}.$$

It can be checked that for each r in the relation set of $G_{p(n)}(\mathbf{MM}_3)$, $\psi(r) = e$, for example,

$$\psi([a_1, a_1']) = \psi(a_1^{-1})\psi(a_1'^{-1})\psi(a_1)\psi(a_1') = [b_1, b_2] = e,$$

so ψ descends to a well-defined homomorphism $G_{p(n)}(\mathbf{MM}_3) \to \langle b_1, b_2 : [b_1, b_2] = e\rangle$. With a similar argument, we can get that ψ descends to a well-defined homomorphism on H. Note that, in H, $\ker(\psi) = \langle x(q_1 A_0)\rangle^H$. Also, notice that for every $n, m \in \mathbb{Z}$, $\psi(a_1^n a_1'^m) = b_1^n b_1'^m$, so ψ is surjective and $\mathrm{Im}(\psi) = \langle b_1, b_2 : [b_1, b_2] = e\rangle$. Since a_1 and a_1' commute, ψ gives us an isomorphism between K and $\langle b_1, b_2 : [b_1, b_2] = e\rangle$. We can conclude that K is abelian and write $K = \langle a_1, a_1' : [a_1, a_1'] = e\rangle$.

All the conditions of Lemma 6.12 are satisfied, so we know H is solvable, $\langle x(q_1 A_0)\rangle^H \cap K = \{e\}$, and

$$H / \langle x(q_1 A_0)\rangle^H = K.$$

Hence, every $h \in H$ can be written as $t a_1^n a_1'^m$ for some $t \in \langle x(q_1 A_0)\rangle^H$ and $n, m \in$

$\mathbb{Z}$. We can deduce that if $t_1 a_1^{n_1} a_1'^{m_1} = t_2 a_1^{n_2} a_1'^{m_2}$,

$$t_1 = t_2 a_1^{n_2 - n_1} a_1'^{m_2 - m_1} \iff n_2 = n_1, \quad m_1 = m_2, \text{ and } t_1 = t_2 \text{ in } \langle x(q_1 A_0) \rangle^H.$$

In other words, every element in H and be uniquely written as $t a_1^n a_1'^m$ for some $t \in \langle x(q_1 A_0) \rangle^H$ and $n, m \in \mathbb{Z}$.

We consider a homomorphism $\phi : \mathcal{F}(\{x(q_1 A_0), a_1, a_1'\}) \to H$ defined by

$$\begin{aligned}
&\phi(a_1) = a_1, \\
&\phi(a_1') = a_1', \\
&\phi(x(q_1 A_0)) = x(q_1 A_0) \circledast a_1.
\end{aligned}$$

It can be checked that

$$\begin{aligned}
&\phi(t a_1^n a_1'^m) = \phi(t) \phi(a_1)^n \phi(a_1')^m, \\
&\phi(t_1 t_2) = \phi(t_1) \phi(t_2),
\end{aligned}$$

for $t, t_1, t_2 \in \langle x(q_1 A_0) \rangle^H$. We first prove ϕ descends to a homomorphism $H \to H$. The fact ϕ is well-defined follows from the fact that each element of H can be uniquely written as $t a_1^n a_1'^m$ for some $t \in \langle x(q_1 A_0) \rangle^H$ and $n, m \in \mathbb{Z}$. To prove it is a homomorphism, first observe that

$$\phi(x(q_1 A_0)^{a_1^n a_1'^m}) = \phi(x(q_1 A_0))^{a_1^n a_1'^m} \text{ for all } n, m \in \mathbb{Z},$$

then for all $t \in \langle x(q_1A_0)\rangle^H$, $\phi(t^{a_1^n a_1'^m}) = \phi(t)^{a_1^n a_1'^m}$. Consider two elements $t_1 a_1^{r_1} a_1'^{s_1}$ and $t_2 a_1^{r_2} a_1'^{s_2}$ where $t_1, t_2 \in \langle x(q_1A_0)\rangle^H$, then

$$
\begin{aligned}
\phi(t_1 a_1^{r_1} a_1'^{s_1} t_2 a_1^{r_2} a_1'^{s_2}) &= \phi(t_1 t_2^{a_1^{-r_1} a_1'^{-s_1}} a_1^{r_1+r_2} a_1'^{s_1+s_2}) \\
&= \phi(t_1)\phi(t_2)^{a_1^{-r_1} a_1'^{-s_1}} \phi(a_1^{r_1+r_2} a_1'^{s_1+s_2}) \\
&= \phi(t_1) a_1^{r_1} a_1'^{s_1} \phi(t_2) a_1^{r_2} a_1'^{s_2} \\
&= \phi(t_1 a_1^{r_1} a_1'^{s_1}) \phi(t_2 a_1^{r_2} a_1'^{s_2}).
\end{aligned}
$$

Secondly, we will prove that $\phi^{p(n)} = \mathbb{1}$ so that it is invertible, and hence an isomorphism. Based on what we prove above, it suffices to make sure that $\phi^{p(n)} = \mathbb{1}$ on the generators. The fact that $\phi^{p(n)}(a_1) = a_1$ and $\phi^{p(n)}(a_1') = a_1'$ follows from the definition. What is left to prove is

$$
\phi^{p(n)}(x(q_1A_0)) = x(q_1A_0) \circledast a_1^{\circledast p(n)} = x(q_1A_0),
$$

where the second equality follows the relations.

We will prove that $\phi(x(q_1A_0) \circledast a_1^{\circledast m}) = x(q_1A_0) \circledast a_1^{\circledast (m+1)}$ for $m \geq 0$ by induction. The base case that $m = 0$ follows from the definition of ϕ. Assume it is true for $m \leq N$, then

$$\begin{aligned}
&\phi(x(q_1A_0) \circledast a_1^{\circledast N}) \\
=&\phi(\left(x(q_1A_0) \circledast a_1^{\circledast (N-1)}\right) \left(x(q_1A_0) \circledast a_1^{\circledast (N-1)}\right)^{a_1} \\
&\qquad \left(x(q_1A_0) \circledast a_1^{\circledast (N-1)}\right)^{a_1^{-1}} \left(x(q_1A_0) \circledast a_1^{\circledast (N-1)}\right)^{a_1'^{-1}}) \\
=&\phi\left(x(q_1A_0) \circledast a_1^{\circledast (N-1)}\right) \phi\left(x(q_1A_0) \circledast a_1^{\circledast (N-1)}\right)^{a_1} \\
&\qquad \phi\left(x(q_1A_0) \circledast a_1^{\circledast (N-1)}\right)^{a_1^{-1}} \phi\left(x(q_1A_0) \circledast a_1^{\circledast (N-1)}\right)^{a_1'^{-1}} \\
=&\left(x(q_1A_0) \circledast a_1^{\circledast N}\right) \left(x(q_1A_0) \circledast a_1^{\circledast N}\right)^{a_1} \left(x(q_1A_0) \circledast a_1^{\circledast N}\right)^{a_1^{-1}} \left(x(q_1A_0) \circledast a_1^{\circledast N}\right)^{a_1'^{-1}} \\
=&x(q_1A_0) \circledast a_1^{\circledast N+1},
\end{aligned}$$

where we use the fact that $x(q_1A_0) \circledast a_1^{\circledast n} \in T$ for all $n \geq 0$ and Lemma 6.15. The induction is complete by the principle of inductive proof.

Then, we prove $\phi^n(x(q_1A_0)) = x(q_1A_0) \circledast a_1^{\circledast n}$ for $n \geq 1$ by induction. The base case follows from the definition of ϕ. Assume it is true for $n \leq N$, then,

$$\phi^{N+1}(x(q_1A_0)) = \phi(\phi^N(x(q_1A_0))) = \phi(x(q_1A_0) \circledast a_1^{\circledast N}) = x(q_1A_0) \circledast a_1^{\circledast (N+1)},$$

and the induction is complete. Then we know that $\phi^{p(n)}(x(q_1A_0)) = x(q_1A_0) \circledast a_1^{\circledast p(n)} = x(q_1A_0)$ in $G_{p(n)}(\mathbf{MM}_3)$, and hence, $\phi^{p(n)} = \mathbb{1}$ on H. Note that

$$\overline{G_{p(n)}(\mathbf{MM}_3)} = \frac{G_{p(n)}(\mathbf{MM}_3) * \langle t : t^{p(n)} = e\rangle}{\langle [t, a_1] = [t, a_1'] = e, t^{-1}x(q_1A_0)t = x(q_1A_0) \circledast a_1\rangle},$$

and the proposition follows from Corollary 3.30. $\square$

We note that the previous proof showed that $\overline{G_{p(n)}(\mathsf{MM}_3)}$ is a $\mathbb{Z}_{p(n)}$-*HNN*-extension of $G_{p(n)}(\mathsf{MM}_3)$.

Proposition 6.26. *$G/\langle t^{p(n)} = e\rangle \cong \overline{G_{p(n)}(\mathsf{MM}_3)}$.*

Proof. Notice that the sets of generators of $G/\langle t^{p(n)} = e\rangle$ and $\overline{G_{p(n)}(\mathsf{MM}_3)}$ are the same. The only difference about the relations is that $\overline{G_{p(n)}(\mathsf{MM}_3)}$ has the relation $x(q_1A_0) \circledast a_1^{\circledast p(n)} = x(q_1A_0)$ and $G/\langle t^{p(n)} = e\rangle$ does not. We are going to show that $x(q_1A_0) \circledast a_1^{\circledast p(n)} = x(q_1A_0)$ holds in $G/\langle t^{p(n)} = e\rangle$ as well. Then it implies that the two groups are isomorphic.

To simplify the notation, we write $v(0) = x(q_1A_0)$ and $v(j) = x(q_1A_0) \circledast a_1^{\circledast j}$ for all $j \geq 1$. Since $v(j) \in T$ for all $j \geq 0$, by Lemma 6.15, we know that $v(j)^2 = e$. Next we are going to prove that $t^{-1}v(n)t = v(n+1)$ and $t^{-n}v(0)t^n = v(n)$ by induction. Assume $t^{-1}v(j)t = v(j+1)$ and $t^{-j}v(0)t^j = v(j)$ for all $1 \leq j \leq k$. Then

$$
\begin{aligned}
t^{-1}v(k)t =& t^{-1}v(k-1)v(k-1)^{a_1}v(k-1)^{a_1^{-1}}v(k-1)^{a_1'^{-1}}t \\
=& t^{-1}v(k-1)tt^{-1}v(k-1)^{a_1}tt^{-1}v(k-1)^{a_1^{-1}}tt^{-1}v(k-1)^{a_1'^{-1}}t \\
=& v(k)v(k)^{a_1}v(k)^{a_1^{-1}}v(k)^{a_1'^{-1}} \\
=& v(k+1)
\end{aligned}
$$

and

$$t^{-k-1}x(q_1A_0)t^{k+1} = t^{-1}t^{-k}v(0)t^kt = t^{-1}v(k)t = v(k+1),$$

where we use the fact that $[t, a_1] = [t, a_1'] = e$. Hence, we know $t^{p(n)} = e$ implies that

$$x(q_1 A_0) = t^{-p(n)} x(q_1 A_0) t^{p(n)} = x(q_1 A_0) \circledast a_1^{\circledast p(n)}$$

in $G / \langle t^{p(n)} = e \rangle$ and the proposition follows.

Moreover, we can also see that the identity homomorphism on the free group generated by the set of generators of G descends to an isomorphism between $G / \langle t^{p(n)} = e \rangle$ and $\overline{G_{p(n)}(\mathsf{MM}_3)}$. $\square$

For the next two propositions, we construct a non-deterministic version of MM_3, denoted by $\mathsf{MM}_3^{(p(n))}$. Comparing to MM_3, the machine $\mathsf{MM}_3^{(p(n))}$ has additional states $1', 2', 3', \ldots p(n)'$. Every command of MM_3 that starts with state 1 or goes to state 1 is replaced by a command starting from state $1'$ or going to state $1'$ respectively with the same action. The other commands of MM_3 are unchanged. In addition to the commands obtained from MM_3, the new commands are

$$1; \to 1'$$

$$1; Add(1) \to 2'$$

$$i'; Add(1) \to (i+1)' \text{ for } 2 \leq i < p(n)$$

$$p(n)'; Add(1) \to 1.$$

Proposition 6.27. *Every computation θ of $\mathsf{MM}_3^{(p(n))}$ satisfies the condition that*

$$\theta = (\theta_l)^k(1; \to 1')\theta_0$$

where $(\theta_l)^k$ represents k loops on the states $1 \to 2' \to \ldots \to p(n)' \to 1$ for $k \geq 0$ and θ_0 is some computation of MM_3 starting at the state 1.

Proof. First observe that $\mathsf{MM}_3^{(p(n))}$ simulates MM_3 in the sense that any computation of $\mathsf{MM}_3^{(p(n))}$ that starts with state $1'$ has a corresponding computation of MM_3 starting at state 1. Since θ_l does not modify the second and third counters and neither does the command $(1; \to 1')$, effectively, the configuration $(1' : m, 0, 0)$ of $\mathsf{MM}_3^{(p(n))}$ can be viewed as the input configuration of MM_3 simulated by $\mathsf{MM}_3^{(p(n))}$. Then, this proposition follows from the observation that $\mathsf{MM}_3^{(p(n))}$ does not have commands going from $1'$ back to 1. $\square$

Proposition 6.28. *In $G_{p(n)}(\mathsf{MM}_3)$, $w(0) = w(a)$ if and only if $n \in X$.*

Proof. Let the set of generators of $G_{p(n)}(\mathsf{MM}_3)$ be $S(\mathsf{MM}_3)$, and let the set of relations of $G_{p(n)}(\mathsf{MM}_3)$ be $R_{p(n)}(\mathsf{MM}_3)$. If $n \in X$, notice that in $G_{p(n)}(\mathsf{MM}_3)$,

$$\begin{aligned} w(0) &= x(q_1 A_0) \circledast A_1 \circledast A_2 \circledast A_3 \\ &= x(q_1 A_0) \circledast a_1^{\circledast p(n)} \circledast A_1 \circledast A_2 \circledast A_3. \end{aligned}$$

Also, notice that $x(q_1 A_0) \circledast a_1^{\circledast p(n)} \circledast A_1 \circledast A_2 \circledast A_3 = w(a)$ in $G(\mathsf{MM}_3)$, which follows from the fact that $p(n)$ is accepted by MM_3. Therefore, $w(0)w(a)$ is in $R_{p(n)}(\mathsf{MM}_3)$ and is trivial in $G_{p(n)}(\mathsf{MM}_3)$.

If $n \notin X$, we consider $G(\mathbf{MM}_3^{(p(n))})$, which is the KMS group of $\mathbf{MM}_3^{(p(n))}$. Let the set of generators and the set of relations of $G(\mathbf{MM}_3^{p(n)})$ be $S(\mathbf{MM}_3^{p(n)})$ and $R(\mathbf{MM}_3^{p(n)})$. Let $L_0' = L_0 \cup \{x(q_{i'}u) \mid 1 \leq i \leq p(n) \text{ and } u \in U'\}$, where L_0 and U' are defined in Section 6.3.2. It can be seen that

$$S(\mathbf{MM}_3) = L_0 \sqcup L_1 \sqcup L_2$$

$$S(\mathbf{MM}_3^{p(n)}) = L_0' \sqcup L_1 \sqcup L_2,$$

where L_1 and L_2 are defined in Section 6.3.2. Based on the relations for the commands in **R.12**, we know that in $G(\mathbf{MM}_3^{(p(n))})$ the relations involving $x(q_1 A_0)$ are

$$x(q_1 A_0) = x(q_{2'} A_0) \circledast a_1,$$

$$x(q_{p(n)'} A_0) \circledast a_1 = x(q_1 A_0),$$

$$x(q_1 A_0) = x(q_{1'} A_0).$$

From the relations involving states $2', 3' \ldots (p(n)-1)'$, we can further deduce that in $G(\mathbf{MM}_3^{(p(n))})$

$$x(q_1 A_0) \circledast a_1^{\circledast p(n)} = x(q_1 A_0). \tag{6.5}$$

Therefore, every $r \in R_{p(n)}(\mathbf{MM}_3)$ is trivial in $G(\mathbf{MM}_3^{(p(n))})$ and the identity homomorphism $\psi : \mathcal{F}(S(\mathbf{MM}_3)) \to \mathcal{F}(S(\mathbf{MM}_3^{p(n)}))$ descends to a homomorphism $\psi : G_{p(n)}(\mathbf{MM}_3) \to G(\mathbf{MM}_3^{p(n)})$. Then if $w(0)w(a) \neq e$ in $G(\mathbf{MM}_3^{p(n)})$, its preimage

$w(0)w(a)$ is also nontrivial in $G_{p(n)}(\mathsf{MM}_3)$.

Since $w(0) = x(q_1A_0) \circledast a_1^{\circledast p(n)} \circledast A_1 \circledast A_2 \circledast A_3$ in $G(\mathsf{MM}_3^{p(n)})$, it suffices to prove $x(q_1A_0) \circledast a_1^{\circledast p(n)} \circledast A_1 \circledast A_2 \circledast A_3 \neq w(a)$ in $G(\mathsf{MM}_3^{p(n)})$. We can prove it by contradiction. Suppose, on the contrary, that $x(q_1A_0) \circledast a_1^{\circledast p(n)} \circledast A_1 \circledast A_2 \circledast A_3 = w(a)$, which implies that there exists a computation of $\mathsf{MM}_3^{(p(n))}$ that will bring the configuration $(1; p(n), 0, 0)$ to the accept configuration. Following Proposition 6.27, θ_0 starts with an input configuration $(1'; (k+1)p(n), 0, 0)$. Our assumption is equivalent to that there exists a $k \geq 0$ such that $(1; (k+1)p(n), 0, 0)$ is accepted by MM_3, which is a contradiction. This is because if $k = 0$, $(1; (k+1)p(n), 0, 0)$ is not accepted because $n \notin X$, and if $k > 0$, $(1; (k+1)p(n), 0, 0)$ is not accepted because $(k+1)p(n)$ is not a prime. So, in $G(\mathsf{MM}_3^{p(n)})$, If $n \notin X$, $x(q_1A_0) \circledast a_1^{\circledast p(n)} \circledast A_1 \circledast A_2 \circledast A_3 \neq w(a)$. We can conclude that $w(0)w(a) \neq e$ in $G(\mathsf{MM}_3^{p(n)})$ and the preimage of $w(0)w(a)$ under the homomorphism ψ in $G_{p(n)}(\mathsf{MM}_3)$, which equals $w(0)w(a)$, is also nontrivial.

In summary, we can see that in $G_{p(n)}(\mathsf{MM}_3)$

$$w(0)w(a) = e \iff n \in X,$$

which completes the proof. □

Proposition 6.29. *The group $\overline{G_{p(n)}(\mathsf{MM}_3)}$ is sofic.*

Proof. We first prove that $G_{p(n)}(\mathsf{MM}_3)$ is solvable. Let $X = \langle L_0 \rangle^{G_{p(n)}(\mathsf{MM}_3)}$ and let H be the subgroup generated by L_1 and L_2 in $G_{p(n)}(\mathsf{MM}_3)$. Comparing to T, which is the normal subgroup generated by L_0 in $G(\mathbf{MM}_3)$,

$$X = T/\langle x(q_1 A_0) \circledast a_1^{\circledast p(n)} = x(q_1 A_0)\rangle.$$

Since T is abelian (Lemma 6.15), X is also abelian. We also know that H is solvable following Lemma 6.16. Then $G_{p(n)}(\mathbf{MM}_3) = X \rtimes H$ is also solvable. Since $\overline{G_{p(n)}(\mathbf{MM}_3)}$ is a $\mathbb{Z}_{p(n)}$-HNN-extension of $G_{p(n)}(\mathbf{MM}_3)$ (Proposition 6.25) and a $\mathbb{Z}_{p(n)}$-HNN-extension of a solvable group is sofic (Proposition 3.52), $\overline{G_{p(n)}(\mathbf{MM}_3)}$ is sofic. $\square$

In summary, the relations between $G/\langle t^{p(n)} = e\rangle$, $G_{p(n)}(\mathbf{MM}_3)$, $\overline{G_{p(n)}(\mathbf{MM}_3)}$ and $G(\mathbf{MM}_3^{(p(n))})$ are given in the figure below.

$$\begin{tikzcd}
G/\langle t^{p(n)} = e\rangle \arrow[r, leftrightarrow] & \overline{G_{p(n)}(\mathbf{MM}_3)} & G(\mathbf{MM}_3^{(p(n))}) \\
& G_{p(n)}(\mathbf{MM}_3) \arrow[u, hook] \arrow[ur] &
\end{tikzcd}$$

Figure 6.2: Figure for the relations between $G/\langle t^{p(n)} = e\rangle$, $\overline{G_{p(n)}(\mathbf{MM}_3)}$, $G(\mathbf{MM}_3^{(p(n))})$ and $G_{p(n)}(\mathbf{MM}_3)$.

Proof of Lemma 6.22. It suffices to choose $H = G$, which is defined in eq. (6.4), $t = t$ and $x = w(0)w(a)$. By Lemma 6.15, $x^2 = e$. Since $G_{p(n)}(\mathbf{MM}_3)$ is embedded in $\overline{G_{p(n)}(\mathbf{MM}_3)}$ (Proposition 6.25), following Proposition 6.28, we know $w(0)w(a) = e$ in $\overline{G_{p(n)}(\mathbf{MM}_3)}$ if and only if $n \in X$. By Proposition 6.26, we can further deduce that $w(0)w(a) = e$ in $G/\langle t^{p(n)} = e\rangle$ if and only if $n \in X$. Also, by Proposition 6.26 and Proposition 6.29, we know $G/\langle t^{p(n)} = e\rangle$ is sofic. For the presentation of H it suffices to apply Proposition 6.20 to $G(\mathsf{MM}_3)$ and $w(0)w(a)$. $\square$

Chapter 7: Main results

In this chapter, we state and prove our main result of this dissertation. Specifically, in Section 7.1, we state a our main theorem (Theorem 7.1) and explain its implication on the decidability of the membership problems of constant-sized C_{qa} and C_{qc} correlations. In Section 7.2, we introduce a correlation that can certify the relation $(t_1t_2)^p = e$, which is used in the proof of Theorem 7.1. In Section 7.3, we construct the family of sets of correlation $\{F_n\}$, which is the central object of Theorem 7.1. In the proof of Theorem 7.1, we need some approximation results to construct approximating strategies of a quantum correlation based on approximating representations. We present such results in Section 7.4. Finally, we prove $\{F_n\}$ satisfy the conclusion of Theorem 7.1 in Section 7.5.

7.1 Membership problems of constant-sized quantum correlations

In this chapter, we let $\mathbb{K}$ be the subfield of $\mathbb{C}$ generated by $\mathbb{Q}$ and the roots of unity ω_n for $n \in \mathbb{Z}$, and we work with correlations with entries in $\mathbb{K}$.

The main result of this chapter is given in the theorem below.

Theorem 7.1. *Let $r \in \{2, 3, 5\}$ be an integer such that there are infinitely many primes whose primitive root is r, let $p(n)$ be the n-th prime whose primitive root is r, and let X*

be a recursively enumerable set of positive integers.

Suppose $G = \langle S : R \rangle$ is an extended homogeneous linear-plus-conjugacy group, which has generators t and x such that $x^2 = e$ in G, $G/\langle t^{p(n)} = e \rangle$ is sofic, and

$$x = e \text{ in } G/\langle t^{p(n)} = e \rangle \iff n \in X, \tag{7.1}$$

for all $n \geq 0$. Then, there exist constants N and K, which only depend on the presentation of G and r, and a family of sets of correlations $\{F_n \mid n > 0\}$ where

$$F_n = \{C_{n,i} \mid i \in [K]\} \subset \mathbb{K}^{N^2 \times 8^2},$$

such that

$$F_n \cap C_{qc}(N, N, 8, 8) = \emptyset \text{ if } n \in X,$$

$$F_n \cap C_{qa}(N, N, 8, 8) \neq \emptyset \text{ if } n \notin X.$$

Note that the set of correlations F_n can be computed by an algorithm for all $n \geq 0$, and we will show it in the proof of Theorem 7.1. Before we prove it, we first prove its consequences on the hardness of membership problem of constant-sized quantum correlations.

For $t \in \{q, qs, qa, qc\}$, we define the membership problem of $C_t(n_A, n_B, m_A, m_B)$ as follows.

Problem (Membership$(n_A, n_B, m_A, m_B)_t$). *Given a correlation $P \in \mathbb{K}^{n_A n_B m_A m_B}$ for* *some constants n_A, n_B, m_A and m_B, decide if $P \in C_t(n_A, n_B, m_A, m_B)$.*

We study the hardness of the membership problems of $C_t(n_A, n_B, m_A, m_B)$ by studying the hardness of a related problem.

Problem (Intersection$(n_A, n_B, m_A, m_B)_t$)**.** *Given a set of correlations $F \subset \mathbb{K}^{n_A n_B m_A m_B}$ such that $|F| \leq K$ for some constants K, n_A, n_B, m_A and m_B, decide if $F \cap C_t(n_A, n_B, m_A, m_B) \neq \emptyset$.*

Proposition 7.2. *For fixed constants n_A, n_B, m_A, m_B and K, and $t \in \{q, qs, qa, qc\}$, (Intersection$(n_A, n_B, m_A, m_B)_t$) is as hard as (Membership$(n_A, n_B, m_A, m_B)_t$).*

Proof. If we have a decider D_m for (Membership$(n_A, n_B, m_A, m_B)_t$), we can use it to construct a decider D_i for (Intersection$(n_A, n_B, m_A, m_B)_t$) in the following way. Given a set of correlations F, D_i runs D_m in parallel for each member of F and accepts only if one of the members of F is in $C_t(n_A, n_B, m_A, m_B)$. Since there are only a constant-number of members of F, the overhead is constant.

If we have a decider D'_i for (Intersection$(n_A, n_B, m_A, m_B)_t$), we can use it to construct a decider D'_m for (Membership$(n_A, n_B, m_A, m_B)_t$) in the following way. Given a correlation P, D'_m passes $\{P\}$ as the input to D'_i and accepts P only if D'_i accepts. Again, the overhead is constant. Hence, under Karp reduction, the two problems have equivalent hardness. $\square$

The first consequence of Theorem 7.1 is on the hardness of the membership problem of constant-sized C_{qa} correlations.

Corollary 7.3. *There exist constants N and M such that, for any integer n_A, $n_B \geq N$ and m_A, $m_B \geq M$, (Membership$(n_A, n_B, m_A, m_B)_{qa}$) is* coRE*-hard.*

Proof. By Lemma 6.22, the group G defined in eq. (6.4) satisfies the conditions of Theorem 7.1. Since $C_{qa}(n,\ n,\ m,\ m) \subseteq C_{qc}(n,\ n,\ m,\ m)$ for any $n, m \geq 2$, Theorem 7.1 implies that there exist constants N and K, and a family of sets of correlations $\{F_n\}$ where $F_n \subseteq \mathbb{K}^{N^2 \times 8^2}$ and $|F_n| = K$, such that

$$F_n \cap C_{qa}(N, N, 8, 8) = \emptyset \text{ if and only if } n \in X.$$

Hence, the problem of deciding if $F_n \cap C_{qa}(N, N, 8, 8) \neq \emptyset$ is coRE-complete, and (Intersection$(n_A, n_B, m_A, m_B)_{qa}$) is coRE-hard for $n_A, n_B \geq N$ and $m_A, m_B \geq 8$. By Proposition 7.2, (Membership$(n_A, n_B, m_A, m_B)_{qa}$) for $n_A, n_B \geq N$ and $m_A, m_B \geq 8$ is also coRE-hard. □

Corollary 7.4. *There exist constants N and M such that, for any n_A, $n_B \geq N$ and m_A, $m_B \geq M$, (Membership$(n_A, n_B, m_A, m_B)_{qc}$)is* coRE*-complete.*

Proof. By Lemma 6.22, the group G defined in eq. (6.4) satisfies the conditions of Theorem 7.1. Since $C_{qa}(n,\ n,\ m,\ m) \subseteq C_{qc}(n,\ n,\ m,\ m)$ for any $n, m \geq 2$, Theorem 7.1 implies that there exist constants N and K, and a family of sets of correlations $\{F_n\}$ where $F_n \subseteq \mathbb{K}^{N^2 \times 8^2}$ and $|F_n| = K$, such that

$$F_n \cap C_{qc}(N, N, 8, 8) = \emptyset \text{ if and only if } n \in X.$$

Hence, the problem of deciding if $F_n \cap C_{qc}(N, N, 8, 8) \neq \emptyset$ is coRE-complete, and (Intersection$(n_A, n_B, m_A, m_B)_{qc}$) is coRE-hard for $n_A, n_B \geq N$ and $m_A, m_B \geq 8$.

On the other hand, it has been shown that (Membership$(n_A, n_B, m_A, m_B)_{qc}$)

is in coRE [42]. Hence, (Membership$(n_A, n_B, m_A, m_B)_{qc}$) is coRE-complete for $n_A, n_B \geq N$ and $m_A, m_B \geq 8$. $\square$

In the proof of Theorem 7.1, we follow the fa^*-embedding procedure and embed the group $G/\langle t^p = e\rangle$ from the statement of Theorem 7.1 into a group of the form $\Gamma/\langle (t_1t_2)^p = e\rangle$, where Γ is a solution group associated with a linear system. To construct a correlation that certifies the relations of $\Gamma/\langle (t_1t_2)^p = e\rangle$, we first show that there exists a constant-sized correlation that can certify the relation $(t_1t_2)^p = e$ for any prime p. More precisely, we mean that the size of this correlation is independent of p.

7.2 The correlation $\overline{Q}_{-\pi/p}$

Recall that, for a prime p, $D_p = \langle t_1, t_2 : t_1^2 = t_2^2 = (t_1t_2)^p = e\rangle$. In this section, we introduce a correlation $\overline{Q}_{-\pi/p}$ that can certify the relation $(t_1t_2)^p = e$ under some condition. Note that $\overline{Q}_{-\pi/p}$ is very similar to $\hat{Q}_{-\pi/p}$ as $\hat{Q}_{-\pi/p}$ can also certify the relation $(t_1t_2)^p = e$. The difference is that $\overline{Q}_{-\pi/p}$ is induced by a strategy based on the regular representation of D_p, but $\hat{Q}_{-\pi/p}$ is not.

To stress the fact that $\overline{Q}_{-\pi/p}$ can certify the relation $(t_1t_2)^p = e$, we include symbols t_1 and t_2 in the question set of $\overline{Q}_{-\pi/p}$, where the question set is

$$I := \{0, 1, 2, t_1, t_2, (0, t_1), (0, t_2)\}.$$

Note that the input set can be chosen to be [7]. Instead, we make the bijection between I and $[7]$ implicit to help understand Theorem 7.10 introduced later. The questions $(0, t_1)$ and $(0, t_2)$ are introduced to make sure the measurement for question 0 commutes with the measurements for questions t_1 and t_2 respectively following Proposition 4.14. When Alice and Bob receive the question $(0, t_1)$ and $(0, t_2)$, they return two symbols (a_0, a_1) where $a_0 \in [3]$ and $a_1 \in [2]$. The answer $(a_0, a_1) \in [3] \times [2]$ is mapped to $2a_0 + a_1 \in [6]$. Instead of using such a bijection between $[3] \times [2]$ and $[6]$, we keep the answer pair (a_0, a_1) to match the question pair $(0, t_1)$ or $(0, t_2)$.

The correlation $\overline{Q}_{-\pi/p} : I \times I \times [6] \times [6] \to \mathbb{K}$ is defined in the next subsection.

7.2.1 An inducing strategy of $\overline{Q}_{-\pi/p}$

In this subsection, we present a commuting-operator strategy inducing $\overline{Q}_{-\pi/p}$, denoted by

$$\tilde{S} = (|\tilde{\psi}\rangle, \{\{\tilde{M}_x^{(a)} \mid x \in I\} \mid a \in [6]\}, \{\{\tilde{N}_y^{(b)} \mid y \in I\} \mid b \in [6]\}),$$

based on the left and right regular representations of D_p. The definitions of $|\tilde{\psi}\rangle$, $\tilde{M}_x^a$ and $\tilde{N}_y^b$ are given below.

First, we introduce the notion of *group algebra* over $\mathbb{C}$ and the notion of an idempotent element of $\mathbb{C}[G]$.

Definition 7.5. *Let G be a group. The **group algebra** $\mathbb{C}[G]$ is the set of all linear combinations of finitely many elements of G with coefficients in $\mathbb{C}$ with two operations*

$+$ and $\cdot$ defined in the following way. Let $\sum_{g \in G} \alpha_g g$ and $\sum_{g \in G} \beta_g g$, where α_g and β_g are nonzero on finitely many g, be two elements of $\mathbb{C}[G]$. Then,

$$(\sum_{g \in G} \alpha_g g) + (\sum_{g \in G} \beta_g g) = \sum_{g \in G} (\alpha_g + \beta_g) g,$$

$$(\sum_{g \in G} \alpha_g g) \cdot (\sum_{g' \in G} \beta_{g'} g') = \sum_{h \in G} (\sum_{g, g' \in G : gg' = h} \alpha_g \beta_{g'}) h.$$

Definition 7.6. *Let G be a group and let $\mathbb{C}[G]$ be the group algebra over $\mathbb{C}$. An element $x \in \mathbb{C}[G]$ is* ***idempotent*** *if $x \cdot x = x$.*

Definition 7.7. *Let G be a group, let $\mathbb{C}[G]$ be the group algebra over $\mathbb{C}$, and let $x = \sum_{g \in G} \alpha_g g$ be an element of $\mathbb{C}[G]$. The support of x, denoted by $\mathrm{supp}(x)$, is*

$$\{g \in G \mid \alpha_g \neq 0\}.$$

Recall the vector space

$$L^2 D_p = \mathrm{span}(\{|(t_1 t_2)^j\rangle, |t_2 (t_1 t_2)^j\rangle \mid j \in [p]\}).$$

We first define $|\tilde{\psi}\rangle := |e\rangle$.

Next we define some idempotent elements of $\mathbb{C}[D_p]$.

$$\pi_0^{(0)} = \frac{1}{p} \sum_{j \in [p]} (t_1 t_2)^j, \tag{7.2}$$

$$\pi_0^{(1)} = \frac{2}{p} \sum_{j \in [p]} \cos(\frac{2j\pi}{p})(t_1 t_2)^j, \tag{7.3}$$

$$\pi_0^{(2)} = e - \pi_0^{(0)} - \pi_0^{(1)}, \tag{7.4}$$

$$\pi_1^{(0)} = \frac{1}{2}\pi_0^{(1)} + \frac{1}{p} \sum_{j \in [p]} \cos(\frac{(2j+1)\pi}{p}) t_2 (t_1 t_2)^j, \tag{7.5}$$

$$\pi_1^{(1)} = \pi_0^{(1)} - \pi_1^{(0)}, \tag{7.6}$$

$$\pi_1^{(2)} = e - \pi_0^{(1)}, \tag{7.7}$$

$$\pi_2^{(0)} = \frac{1}{2}\pi_0^{(1)} + \frac{1}{p} \sum_{j \in [p]} \sin(\frac{(2j+1)\pi}{p}) t_2 (t_1 t_2)^j, \tag{7.8}$$

$$\pi_2^{(1)} = \pi_0^{(1)} - \pi_2^{(0)}, \tag{7.9}$$

$$\pi_2^{(2)} = e - \pi_0^{(1)}. \tag{7.10}$$

From the definition of group algebra, we can see that representations of G can be extended to representations of $\mathbb{C}[G]$ linearly. We denote the left and right regular representations of $\mathbb{C}[D_p]$ on $L^2 D_p$ by L and R. Then we define the projectors used by Alice and Bob.

- For the input $x, y \in \{0, 1, 2\}$

$$\tilde{M}_x^{(a)} = \begin{cases} L(\pi_x^{(a)}) & \text{if } a \in [3], \\ 0 & \text{otherwise;} \end{cases}$$

$$\tilde{N}_y^{(b)} = \begin{cases} R(\pi_y^{(b)}) & \text{if } b \in [3], \\ 0 & \text{otherwise.} \end{cases}$$

- For the inputs $x, y \in \{t_1, t_2\}$

$$\tilde{M}_x^{(a)} = \begin{cases} \frac{L(e)+(-1)^a L(x)}{2} & \text{if } a \in [2], \\ 0 & \text{otherwise;} \end{cases}$$

$$\tilde{N}_y^{(b)} = \begin{cases} \frac{R(e)+(-1)^b R(y)}{2} & \text{if } b \in [2], \\ 0 & \text{otherwise.} \end{cases}$$

- For the inputs $(0, x)$ and $(0, y)$ with $x, y \in \{t_1, t_2\}$

$$\tilde{M}_{(0,x)}^{(a_0,a_1)} = \tilde{M}_0^{(a_0)} \tilde{M}_x^{(a_1)} \qquad \text{with } a_0 \in [3], a_1 \in [2],$$

$$\tilde{N}_{(0,y)}^{(b_0,b_1)} = \tilde{N}_0^{(b_0)} \tilde{N}_y^{(b_1)} \qquad \text{with } b_0 \in [3], b_1 \in [2].$$

Note that the fact that $\tilde{M}_0^{(a)}$ commutes with $\tilde{M}_x^{(a)}$ for $x \in \{t_1, t_2\}$ follows from the observation that

$$L(t_1)L((t_1t_2)^j)L(t_1) = L((t_1t_2)^{-j}) \qquad L(t_2)L((t_1t_2)^j)L(t_2) = L((t_1t_2)^{-j})$$

for each $j \in [p]$. With similar reasoning, we get that $\tilde{N}_0^{(b)}$ commutes with $\tilde{N}_y^{(b)}$ for $y \in \{t_1, t_2\}$.

Definition 7.8. *The correlation $\overline{Q}_{-\pi/p} : I \times I \times [6] \times [6] \to \mathbb{K}$, is defined by*

$$\overline{Q}_{-\pi/p}(a, b|x, y) = \langle \tilde{\psi}|\tilde{M}_x^{(a)}\tilde{N}_y^{(b)}|\tilde{\psi}\rangle.$$

Since $\overline{Q}_{-\pi/p}$ is induced by $\tilde{S}$, the next claim is immediate.

Claim 7.9. *The correlation $\overline{Q}_{-\pi/p}$ is in $C_{qc}^s(7, 6)$.*

7.2.2 Implication of $\overline{Q}_{-\pi/p}$

This subsection is devoted to the following theorem.

Theorem 7.10. *If a commuting-operator strategy $S = (|\psi\rangle, \{M_x^{(a)}\}, \{N_y^{(b)}\})$ can induce $\overline{Q}_{-\pi/p}$ and there exist unitaries U_A and U_B such that U_A commutes with U_B and all of Bob's projectors, U_B commutes with all of Alice's projectors, and*

$$U_AU_B|\psi\rangle = |\psi\rangle,$$

$$(N_{t_1}N_{t_2})U_B|\psi\rangle = U_B(N_{t_1}N_{t_2})^r|\psi\rangle,$$

$$(M_{t_1}M_{t_2})U_A|\psi\rangle = U_A(M_{t_1}M_{t_2})^r|\psi\rangle,$$

where $M_x = M_x^{(0)} - M_x^{(1)}$ *and* $N_y = N_y^{(0)} - N_y^{(1)}$ *for* $x, y \in \{t_1, t_2\}$ *and* r *is a primitive root of* p*, then*

$$(M_{t_1} M_{t_2})^p |\psi\rangle = |\psi\rangle.$$

This proof is very similar to the proof of Proposition 5.8. As, in that proof, the basic idea is to find a decomposition of $|\psi\rangle : |\psi\rangle = \sum_{j=0}^{p} |\psi_j\rangle$, where $|\psi_j\rangle$ is an eigenvector of $M_{t_1} M_{t_2}$ with eigenvalue ω_p^j. Intuitively, $|\psi_0\rangle$ and $|\psi_p\rangle$ are in the 1-dimensional irreducible representation of D_p, and $|\psi_j\rangle$ and $|\psi_{p-j}\rangle$ are in the 2-dimensional irreducible representation of D_p, in which

$$t_1 t_2 \mapsto \begin{pmatrix} \omega_p^j & 0 \\ 0 & \omega_p^{-j} \end{pmatrix}$$

for $1 \leq j \leq (p-1)/2$.

Comparing to $\hat{Q}_{-\pi/p}$, the two new questions are $(0, t_1)$ and $(0, t_2)$. As mentioned in the start of this section, we introduce questions $(0, t_1)$ and $(0, t_2)$ to make sure the measurement for question 0 commutes with the measurements of t_1 and t_2. Such tests of commutation relations between measurements are not necessary for the proof of Proposition 5.8.

The full proof along with entries of $\overline{Q}_{-\pi/p}$ can be found in Appendix C.1.

7.3 The set of correlations F_n

The idea behind how we construct the set of correlations F_n in the statement of Theorem 7.1 is the following. We first extend the given group G and embed it into a solution group Γ. Then, the correlations in F_n are designed to certify the relations of $\Gamma/\langle (t_1 t_2)^{p(n)} = e\rangle$. More specifically, we identify the projector of each question-answer pair as an idempotent element of $\mathbb{C}[\Gamma]$, and the correlations values are function values of products of such idempotent elements for a family of functions on $\mathbb{C}[\Gamma]$ to be defined later.

We first extend the group G and embed the extended group in Γ. Let

$$D := \langle u, t_D : u^{-1} t_D u = t_D^r \rangle$$

$$K := (G * D)/\langle t = t_D \rangle.$$

Proposition 7.11. *$K/\langle t^{p(n)} = e\rangle$ is sofic and $G/\langle t^{p(n)} = e\rangle$ is embedded in $K/\langle t^{p(n)} = e\rangle$ such that*

$$x = e \text{ in } K/\langle t^{p(n)} = e\rangle \iff n \in X.$$

Proof. We first prove that D is sofic. First note that $\langle t_D \rangle \cong \mathbb{Z}$ and it is abelian. Next, we show that D is an HNN-extension of $\mathbb{Z}$. Define $\phi : \mathbb{Z} \to \mathbb{Z} : t_D \to t_D^r$. Then ϕ is an injective endomorphism on $\langle t_D \rangle$ and D is an HNN-extension of $\mathbb{Z}$. By Proposition 3.51, we know D is sofic. Because $G/\langle t^{p(n)} = e\rangle$ is sofic, by

Proposition 3.50, we know $K/\langle t^{p(n)} = e\rangle \cong (G/\langle t^{p(n)} = e\rangle * D)/\langle t = t_D\rangle$ is also sofic.

Again, because $K/\langle t^{p(n)} = e\rangle$ is the free product $G/\langle t^{p(n)} = e\rangle$ and D with amalgamation, by Theorem 3.22, we know $G/\langle t^{p(n)} = e\rangle$ is embedded in $K/\langle t^{p(n)} = e\rangle$. Hence, $x = e$ in $K/\langle t^{p(n)} = e\rangle$ if and only if $n \in X$. $\square$

We know that G is an extended homogeneous linear-plus-conjugacy group. If the presentation of G is $\langle S : R\rangle$, then the presentation of K is $\langle S \cup \{u\} : R \cup \{u^{-1}tu = t^r\}\rangle$. We can see that K is also an extended homogeneous linear-plus-conjugacy group following Definition 3.54. Therefore, the fa^*-embedding procedure (Propositions 3.55 and 3.56) can be applied to K.

By applying the fa^*-embedding procedure to the group K , we can construct an $m \times n$ binary linear system $A\boldsymbol{x} = 0$ and a solution group Γ associated with $A\boldsymbol{x} = 0$ wherein K is embedded.

$$\Gamma = \Gamma'(A) = \frac{G_0 * G_1 * \ldots * G_{m-1}}{\langle P_\Gamma\rangle},$$

where

$$G_i = \langle \{g_{i,k} \mid k \in I_i\} : \{g_{i,k}^2 = [g_{i,k}, g_{i,l}] = \prod_{k\in I_i} g_{i,k} = e \mid k,l \in I_i\}\rangle, \tag{7.11}$$

$$P_\Gamma = \{g_{i,k}g_{j,k} \mid i,j \in [m],\ k \in I_i \cap I_j\}. \tag{7.12}$$

Denote the fa^*-embedding of K into Γ by ϕ. Then there exist $i_0, i_1, i_2 \in [m]$ and

$k_0 \in I_{i_0}, k_1 \in I_{i_1}, k_2 \in I_{i_2}$ [1] such that

$$\phi(x) = g_{i_0,k_0} \qquad\qquad \phi(t) = g_{i_1,k_1} g_{i_2,k_2}.$$

For simplicity, from now on, we write $\phi(x) = x$ and $\phi(t) = t_1 t_2$.

Proposition 7.12. *Let $\phi' : K/\langle t^{p(n)} = e\rangle \to \Gamma/\langle \phi(t)^{p(n)} = e\rangle$ be the homomorphism induced by ϕ. Then ϕ' is also an fa^*-embedding. In particular,*

$$\phi'(x) = e \text{ in } \Gamma/\langle \phi(t)^{p(n)} = e\rangle \iff n \in X.$$

Proof. If ρ is also an ϵ-representation of $K/\langle t^{p(n)} = e\rangle$ meaning that $\|\rho(t)^{p(n)} - \mathbb{1}\| \leq \epsilon$, then following the steps of the fa^*-embedding procedure in Appendix B, we can construct an approximate representation σ of $\Gamma/\langle \phi(t)^{p(n)} = e\rangle$ such that

$$\sigma(\phi'(t)) = (\rho(t) \oplus \rho(t)) \otimes \mathbb{1}_{\mathbb{C}^{k_0}} \oplus (\rho(t) \oplus \overline{\rho(t)}) \oplus \mathbb{1}_{\mathbb{C}^{k_1}}$$

where $\overline{\rho(t)}$ is the complex conjugate of $\rho(t)$ and for some constants k_0 and k_1 depending on the presentation of G. Hence, $\|\sigma(\phi'(t))^{p(n)} - \mathbb{1}\| \leq \epsilon$ and σ is an ϵ-approximate representation of $\Gamma/\langle \phi(t)^{p(n)} = e\rangle$. By Lemma 3.41, we know ϕ' is an fa^*-embedding and the proposition follows. □

Next, we are going to define F_n based on $\Gamma/\langle (t_1 t_2)^{p(n)} = e\rangle$. Let $O_\Gamma = \{g_{i,k} \mid$

[1] This is because the fa^*-embedding procedure reuses generators of G that squares to identity and introduce two more generators for each generator of G that does not square to identity, as demonstrated in Appendix B.

$i \in [m], k \in I_i\}$, which are the generators of Γ, and let

$$O = O_\Gamma \cup \{g_m, g_{m+1}, g_{m+2}, (g_m, t_1), (g_m, t_2)\}.$$

The symbols g_m, g_{m+1} and g_{m+2} correspond to questions 0, 1 and 2 from the question set of $\overline{Q}_{-\pi/p(n)}$ respectively. The symbols (g_m, t_1) and (g_m, t_2) correspond to questions $(0, t_1)$ and $(0, t_2)$ from the question set of $\overline{Q}_{-\pi/p(n)}$ respectively. Then the set of questions for each correlation in F_n is $O \cup [m]$. The constant M in the statement of Theorem 7.1 equals $|O| + m$. [2]

It takes two steps to define correlations in F_n. We first define a mapping $\sigma : (O \cup [m]) \times [8] \to \mathbb{C}[\Gamma]$, which gives us the idempotent element for each question-answer pair.

- When $g \in O_\Gamma$

$$\sigma(g, a) = \begin{cases} \frac{e+(-1)^a g}{2} & \text{if } a < 2, \\ 0 & \text{otherwise.} \end{cases}$$

- When $i \in [m]$, [3]

$$\sigma(i, \boldsymbol{a}) = \prod_{k \in I_i} \frac{e + (-1)^{\boldsymbol{a}(k)} g_{i,k}}{2}.$$

[2] As in the case of $\overline{Q}_{-\pi/p(n)}$, we use $O \cup [m]$ instead of $[M]$ as the question set to better distinguish between different types of questions.

[3] The bijection between $[2] \times [2] \times [2]$ and $[8]$ is implicit here.

- When $g \in \{g_m, g_{m+1}, g_{m+2}\}$,

$$\sigma(g, a) = \begin{cases} 0 & \text{if } a > 2 \\ \pi_0^{(a)} & \text{if } g = g_m, \\ \pi_1^{(a)} & \text{if } g = g_{m+1}, \\ \pi_2^{(a)} & \text{otherwise,} \end{cases}$$

where $\pi_i^{(a)}$ are defined in eq. (7.2) to eq. (7.10).

- Lastly, [4]

$$\sigma((g_m, t_1), (a_1, a_2)) = \begin{cases} \pi_0^{(a_1)} \frac{e+(-1)^{a_2} t_1}{2} & \text{if } a_1 < 3, a_2 < 2 \\ 0 & \text{otherwise.} \end{cases}$$

$$\sigma((g_m, t_2), (a_1, a_2)) = \begin{cases} \pi_0^{(a_1)} \frac{e+(-1)^{a_2} t_2}{2} & \text{if } a_1 < 3, a_2 < 2 \\ 0 & \text{otherwise.} \end{cases}$$

If $\sigma(x, a) = \sum_g \alpha_g g$ for some coefficients α_g, we define a notation

$$\sigma(x, a)^- = \sum_g \alpha_g g^{-1}.$$

Note that $\sigma(x, a)^-$ is different from the inverse of $\sigma(x, a)$ in $\mathbb{C}[\Gamma]$.

In the second step, we will define a set of functions $\{f_{n,\mathbf{z}} : \mathbb{C}[\Gamma] \to \mathbb{K}\}$. We

[4] The bijection between $[3] \times [2]$ and $[6]$ is implicit here.

first introduce the index set of $\boldsymbol{z}$. Let

$$W^+ = \bigcup_{x,y \in O \cup [m], a,b \in [8]} \operatorname{supp}(\sigma(x,a)\sigma(y,b)^-), \tag{7.13}$$

which is the set of all the elements of Γ that appears in the expression of $\sigma(x,a)\sigma(y,b)^-$ for any $x, y \in O \cup [m]$ and $a, b \in [8]$. Note that W^+ is a finite union of finite sets, so W^+ is also a finite set.

Recall that $x \in O_\Gamma$ and eq. (7.12). Let

$$\begin{aligned} S &= \{t_1, t_2, g_m, g_{m+1}, g_{m+2}, (g_m, t_1), (g_m, t_2)\}, \\ W &= W^+ \setminus \left[\{x\} \bigcup \left(\bigcup_{x,y \in S, a,b \in [8]} \operatorname{supp}(\sigma(x,a)\sigma(y,b)^-) \right) \right]. \end{aligned}$$

The triviality of $w \in W$ in $\Gamma / \langle (t_1 t_2)^{p(n)} = e \rangle$ depends on G and n and cannot be determined from the fa^*-embedding procedure. Then, W is a finite set and $|W|$ is independent of n. In addition, we can fix a bijection between W and $[|W|]$, so for each $w \in W$ we can talk about the w-th bit of $\boldsymbol{z} \in \mathbb{Z}_2^{|W|}$. Hence, we can define a function $h_{n,\boldsymbol{z}} : \Gamma \to \mathbb{K}$ for each $\boldsymbol{z} \in \mathbb{Z}_2^{|W|}$.

$$h_{n,\boldsymbol{z}}(g) = \begin{cases} 1 & \text{if } g = e \text{ or } g = (t_1 t_2)^{p(n)}, \\ 0 & \text{if } g = x, \\ \boldsymbol{z}(g) & \text{if } g \in W, \\ 0 & \text{otherwise.} \end{cases}$$

Then, $f_{n,\boldsymbol{z}} : \mathbb{C}[\Gamma] \to \mathbb{K}$ is defined by

$$f_{n,\boldsymbol{z}}(\sum_{g\in\Gamma} \alpha_g g) = \sum_{g\in\Gamma} \alpha_g h_{n,\boldsymbol{z}}(g).$$

Given the functions $\{f_{n,\boldsymbol{z}} \mid \boldsymbol{z} \in \mathbb{Z}_2^W\}$ and σ, a correlation $C_{n,\boldsymbol{z}} : (O \cup [m]) \times (O \cup [m]) \times [8] \times [8] \to \mathbb{K}$ is defined by

$$C_{n,\boldsymbol{z}}(a, b|x, y) = f_{n,\boldsymbol{z}}(\sigma(x, a)\sigma(y, b)^{-}).$$

We say a correlation $C_{n,\boldsymbol{z}}$ induces a perfect correlation of $A\boldsymbol{x} = 0$ if $C_{n,\boldsymbol{z}}$ restricted to the domain $([m] \cup O_\Gamma) \times ([m] \cup O_\Gamma) \times [8] \times [8]$ is a perfect correlation of $A\boldsymbol{x} = 0$. Define

$$F_n = \{C_{n,\boldsymbol{z}} \mid C_{n,\boldsymbol{z}} \text{ induces a perfect correlation of } A\boldsymbol{x} = 0\},$$

and the constant $K := |F_n| \leq 2^{|W|}$, which is mentioned in the statement of Theorem 7.1.

7.4 Approximation tools

A key step in the proof of Theorem 7.1 is to construct an approximate strategy of a quantum correlation based on some approximation representation of a group. In this section, we present these techniques used in this step.

In the next proposition, we first show that any unitary can be approximated by another unitary of an integer order.

Proposition 7.13. *For any integer $n \geq 2$ and any diagonal unitary matrix U, there is a diagonal matrix D such that $D^n = \mathbb{1}$ and*

$$\|U - D\|^2 \leq (\frac{1}{n} + \frac{1}{n^2})\|U^n - \mathbb{1}\|^2.$$

Proof. Suppose the i-th entry on the diagonal of U is $e^{i\theta}$ with $\theta \in [0, 2\pi)$. Choose an integer k such that $|\theta - 2k\pi/n| = \mu \leq \pi/n$. We will first show that

$$\|e^{i\theta} - \omega_n^k\|^2 \leq (\frac{1}{n} + \frac{1}{n^2})\|e^{in\theta} - 1\|^2.$$

By the definition of the normalized Hilbert-Schmidt norm, the proposition follows.

It can be calculated that

$$\begin{aligned}
\|e^{i\theta} - e^{i2k\pi/n}\|^2 &= (\cos(\theta) - \cos(2k\pi/n))^2 + (\sin(\theta) - \sin(2k\pi/n)))^2 \\
&= 2 - 2\cos(\theta - 2k\pi/n) = 2 - 2\cos(\mu), \\
\|e^{in\theta} - 1\|^2 &= (\cos(n\theta) - 1)^2 + \sin(n\theta)^2 \\
&= 2 - 2\cos(n\mu).
\end{aligned}$$

Define a function

$$f(x) = (\frac{1}{n} + \frac{1}{n^2})(1 - \cos(nx)) - (1 - \cos(x)).$$

We will show that $f(x) \geq 0$ when $x \in [0, \pi/n]$. Taking its first and second derivatives, we get

$$f'(x) = (1 + \frac{1}{n}) \sin(nx) - \sin(x),$$
$$f''(x) = (n+1)\cos(nx) - \cos(x).$$

First notice that

$$f'(x) = \frac{1}{n}\sin(nx) + 2\cos(\frac{(n+1)x}{2})\sin(\frac{(n-1)x}{2}),$$

so $f'(x) \geq 0$ when $x \in [0, \pi/(n+1)]$ and we need to study the behaviour of $f''(x)$ on $[\pi/(n+1), \pi/n]$. When $x \in [\pi/(n+1), \pi/n]$, $\cos(nx) < 0$ but $\cos(x) > 0$ so $f''(x) < 0$. and $f'(x)$ is monotonically decreasing on $[\pi/(n+1), \pi/n]$. Since,

$$f'(\frac{\pi}{n}) = -\sin(\pi/n) < 0.$$

we know $f(x)$ is increasing on $[0, x_0)$ and decreasing on $[x_0, \pi/n]$ for some $x_0 \in (\pi/(n+1), \pi/n)$. Hence, to show $f(x) \geq 0$, it suffices to check $f(0)$ and $f(\pi/n)$:

$$f(0) = 0,$$
$$f(\pi/n) = 2(\frac{1}{n} + \frac{1}{n^2}) - (1 - \cos(\pi/n)) \geq \frac{2n+2}{n^2} - \frac{\pi^2}{2n^2} \geq 0,$$

which is because $2n + 2 \geq 6$ and $\pi^2/2 < 5$, and we complete the proof. $\square$

Proposition 7.14. *Let $\{P_i \mid i \in [n]\} \subset \mathcal{L}(\mathbb{C}^d)$ be a set of matrices such that*

$$\|P_i\|_{op} \leq c, \qquad \|P_i^2 - P_i\| \leq \epsilon, \qquad \|P_i P_j\| \leq \epsilon, \qquad \sum_{i\in[n]} P_i = \mathbb{1},$$

for $i \neq j \in [n]$ and a constant $c > 1$. Then, there is a projective measurement $\{\Pi_i \mid i \in [n]\} \subset \mathcal{L}(\mathbb{C}^d)$ such that $\|\Pi_i - P_i\| \leq (cn)^{2n-1}\epsilon$ for all $i \in [n]$.

Proof. From the conditions, we know that

$$\|P_i^n - P_i\| \leq \sum_{j=1}^{n-1} \|P_i^{j+1} - P_i^j\| \leq \sum_{j=1}^{n-1} \|P_i^2 - P_i\| \|P_i^{j-1}\|_{op} \leq c^{n-1}\epsilon,$$

for any $i \in [n]$, and for any sequence $(j_0, j_1, \ldots, j_{n-1})$ where there exists $l \in [n-1]$ such that $j_l \neq j_{l+1}$,

$$\|\prod_{k\in[n]} P_{j_k}\| \leq \prod_{k\in[l]} \|P_{j_k}\|_{op} \|P_{j_l} P_{j_{l+1}}\| \prod_{l+1<k<n} \|P_{j_k}\|_{op} \leq c^{n-2}\epsilon.$$

Let $O = \sum_{i\in[n]} \omega_n^i P_i$, then

$$\begin{aligned}
&\|O\|_{op} \leq \sum_{i\in[n]} |\omega_n^i| \|P_i\|_{op} \leq cn, \\
&\|O^j - \sum_{i\in[n]} \omega_n^{ji} P_i\| \\
=&\| \sum_{i_0,\ldots i_{j-1}\in[n]} \left(\omega_n^{\sum_{k\in[j]} i_k} \prod_{k\in[j]} P_{i_k} \right) - \sum_{i\in[n]} \omega_n^{ji} P_i\| \\
\leq&[(n^j - n)c^{n-2} + nc^{n-1}]\epsilon \leq n^j c^{n-1}\epsilon,
\end{aligned}$$

and in particular

$$\|O^n - \mathbb{1}\| \leq n^n c^{n-1} \epsilon.$$

By the previous proposition, we can construct a unitary $\hat{O}$ such that $\hat{O}^n = \mathbb{1}$ and

$$\|\hat{O} - O\| \leq \frac{\sqrt{n+1}}{n} \|O^n - \mathbb{1}\| \leq \sqrt{n+1}(cn)^{n-1}\epsilon.$$

Then it can be checked that

$$\|\hat{O}^j - O^j\| \leq \sum_{k \in [j-1]} \|\hat{O}\|_{op}^k \|\hat{O} - O\| \|O\|_{op}^{j-k-1} \leq (cn)^j \|\hat{O} - O\|.$$

Define

$$\Pi_i = \frac{1}{n} \sum_{j \in [n]} \omega_n^{-ij} \hat{O}^j$$

for each $i \in [n]$. Then, by the definition of $\hat{O}$, we know $\{\Pi_i \mid i \in [n]\}$ is a projective measurement. We can further calculate that

$$\begin{aligned}
\|\Pi_i - P_i\| \leq & \frac{1}{n} \| \sum_{j \in [n]} \omega_n^{-ij} (\hat{O}^j - O^j) \| + \frac{1}{n} \| \sum_{j \in [n]} \omega_n^{-ij} (O^j - \sum_{k \in [n]} \omega_n^{jk} P_k) \| \\
\leq & \frac{1}{n} \sum_{j \in [n]} (cn)^j \|\hat{O} - O\| + \frac{1}{n} \sum_{j \in [n]} n^j c^{n-1} \epsilon \\
\leq & (cn)^{2n-1} \epsilon,
\end{aligned}$$

for each $i \in [n]$. $\square$

We also use the following lemma first proved by Slofstra to handle approximate representations of the group $\mathbb{Z}_2^k$ for some $k \geq 1$.

Lemma 7.15 (Lemma 24 of [7]). *Consider $\mathbb{Z}_2^k$ as a finitely presented group with presentation*

$$\langle x_1, \ldots, x_k : x_i^2 = e, [x_i, x_j] = e \text{ for all } i \neq j \rangle.$$

Then, there is a constant $C > 0$, depending only on k, such that if ρ is an ϵ-approximate representation of $\mathbb{Z}_2^k$ on a Hilbert space $\mathcal{H}$, then there is a representation σ of $\mathbb{Z}_2^k$ on $\mathcal{H}$ with

$$\|\sigma(x_i) - \rho(x_i)\| \leq C\epsilon$$

for all $1 \leq i \leq k$.

From Slofstra's proof of this lemma, we can see that when $k = 3$,

$$C = (4(1 + \frac{1}{\sqrt{2}}) + 1)(1 + \frac{1}{2\sqrt{2}}) + (1 + \frac{1}{\sqrt{2}}) \approx 12.3 < 13.$$

7.5 Proof of Theorem 7.1

The proof of Theorem 7.1 covers two cases: $n \in X$ and $n \notin X$. When $n \in X$, we prove $F_n \cap C_{qc}(N, N, 8, 8) = \emptyset$ by contradiction. When $n \notin X$, we show that we can construct an approximating strategy of a particular correlation in F_n based on any approximate representations of $\Gamma / \langle (t_1 t_2)^{p(n)} = e \rangle$. It implies that this correlation is in $C_{qa}(N, N, 8, 8)$ and $F_n \cap C_{qa}(N, N, 8, 8) \neq \emptyset$.

Proof of Theorem 7.1. When $n \in X$, we prove by contradiction. Assume $C_{n,\boldsymbol{z}} \in C_{qc}(N, N, 8, 8)$ for some $\boldsymbol{z}$. Then there exists an inducing commuting-operator strategy

$$S = (|\psi\rangle, \{\{M_g^{(x)} \mid x \in [8]\} \mid g \in O \cup [m]\}, \{\{N_g^{(x)} \mid x \in [8]\} \mid g \in O \cup [m]\}).$$

From the correlation, we know that for each $g \in O_\Gamma$ and $x, y > 1$,

$$M_g^{(x)} |\psi\rangle = N_g^{(y)} |\psi\rangle = 0.$$

We can construct a binary observable for each $g \in O_\Gamma$. Define $M(g) := M_g^{(0)} - M_g^{(1)}$ and $N(g) := N_g^{(0)} - N_g^{(1)}$ for each $g \in O_\Gamma$, then

$$M(g)^2 |\psi\rangle = (M_g^{(0)} + M_g^{(1)}) |\psi\rangle = \sum_{j \in [8]} M_g^{(j)} |\psi\rangle = |\psi\rangle,$$
$$N(g)^2 |\psi\rangle = (N_g^{(0)} + N_g^{(1)}) |\psi\rangle = \sum_{j \in [8]} N_g^{(j)} |\psi\rangle = |\psi\rangle.$$

From the correlation, we also know that

$$\langle \psi | M(x) | \psi \rangle = 0. \tag{7.14}$$

Since D is embedded in K and K is embedded in Γ, assuming the image of u in Γ is u_1u_2, we know

$$(M(t_1)M(t_2))(M(u_1)M(u_2))|\psi\rangle = (M(u_1)M(u_2))(M(t_1)M(t_2))^r|\psi\rangle,$$
$$(N(t_1)N(t_2))(N(u_1)N(u_2))|\psi\rangle = (N(u_1)N(u_2))(N(t_1)N(t_2))^r|\psi\rangle.$$

Let $U_A = M(u_1)M(u_2)$ and $U_B = N(u_1)N(u_2)$, then these two unitaries satisfy the conditions of Theorem 7.10. Since S can induce $\overline{Q}_{-\pi/p(n)}$, we can use Theorem 7.10 to conclude that

$$\langle\psi|(M(t_1)M(t_2))^{p(n)}|\psi\rangle = 1.$$

By [43, Lemma 8], we know that there exists a Hilbert space $\mathcal{H}_0$, such that for $g, g' \in O_\Gamma$,

$$(M(g)|_{\mathcal{H}_0})^2 = \mathbb{1}_{\mathcal{H}_0},$$
$$M(g)|_{\mathcal{H}_0}M(g')|_{\mathcal{H}_0} = \mathbb{1}_{\mathcal{H}_0} \text{ if } gg' = e \text{ in } \Gamma,$$

where $M(g)|_{\mathcal{H}_0}$ denotes the linear operator for the actions of $M(g)$ restricted to $\mathcal{H}_0$, and that

$$(M(t_1)|_{\mathcal{H}_0}M(t_2)|_{\mathcal{H}_0})^{p(n)} = \mathbb{1}_{\mathcal{H}_0}.$$

Hence, $\phi : \Gamma/\langle(t_1t_2)^{2p(n)} = e\rangle \to \mathcal{U}(\mathcal{H}_0)$ induced by $\phi(g) = M(g)|_{\mathcal{H}_0}$ for each

$g \in O_\Gamma$ is a representation of $\Gamma/\langle (t_1t_2)^{p(n)} = e\rangle$.

By Proposition 7.12, when $n \in X$, $x = e$ in $\Gamma/\langle (t_1t_2)^{p(n)} = e\rangle$. On the other hand, eq. (7.14) implies that $M(x)|\psi\rangle \neq |\psi\rangle$, so $\phi(x) = M(x)|_{\mathcal{H}_0} \neq \mathbb{1}_{\mathcal{H}_0}$, which contradicts the fact that ϕ is a homomorphism. Hence, $C_{n,\boldsymbol{z}}$ is not in $C_{qc}(N, N, 8, 8)$ and $F_n \cap C_{qc}(N, N, 8, 8) = \emptyset$.

When $n \notin X$, we define $\hat{\boldsymbol{z}} \in \mathbb{Z}_2^{|W|}$ by

$$\hat{\boldsymbol{z}}(w) = 1 \iff w = e \in \Gamma/\langle \phi(t)^{p(n)} = e\rangle$$

for all $w \in W$.

Proposition 7.16. $C_{n,\hat{\boldsymbol{z}}} \in F_n$.

It suffices to show that $C_{n,\hat{\boldsymbol{z}}}$ induces a perfect correlation of $A\boldsymbol{x} = 0$. We prove it in Appendix C.2.

Next, we give a series of finite-dimensional quantum strategies inducing quantum correlations approaching $C_{n,\hat{\boldsymbol{z}}}$.

Recall that W^+ defined in eq. (7.13) is the set of elements of Γ that appears in the expression of $\sigma(x,a)\sigma(y,b)^-$ for some $x, y \in O \cup [m]$ and $a, b \in [8]$. Let

$$W' = W^+ \cap \{g \neq e \mid g \in \Gamma/\langle (t_1t_2)^{p(n)} = e\rangle\}.$$

Since $K/\langle t^{p(n)} = e\rangle$ is sofic and can be fa^*-embedded in $\Gamma/\langle (t_1t_2)^{p(n)} = e\rangle$, by Propositions 3.55 to 3.57 and [7, Lemma 25], we know that for any $\epsilon, \zeta > 0$, there is an ϵ-approximate representation $\rho : \Gamma/\langle (t_1t_2)^{p(n)} = e\rangle \to \mathcal{U}(\mathbb{C}^d)$, where d

depends on ϵ and ζ, such that, for each $w \in W'$,

$$0 \leq \widetilde{\mathrm{Tr}}(\rho(w)) \leq \zeta,$$

and for any $g \in O_\Gamma$, $\rho(g)^2 = \mathbb{1}$. Moreover, for any $r \in P_\Gamma$,

$$|\widetilde{\mathrm{Tr}}(\rho(r)) - 1| \leq \|\rho(r) - \rho(e)\| \leq \epsilon.$$

By Lemma 7.15, for each $i \in [m]$, there is a representation $\rho_i : G_i \to \mathcal{U}(\mathbb{C}^d)$ such that

$$\|\rho_i(g_{i,k}) - \rho(g_{i,k})\| \leq 13\epsilon \text{ for } k \in I_i.$$

To apply Proposition 7.14 in the construction of an approximation strategy of $C_{n,\hat{z}}$, we need the following proposition, which is proved in Appendix C.3.

Proposition 7.17. *Let ρ be an ϵ-approximate representation of $\Gamma/\langle t^{p(n)} = e\rangle$. Then, $\|\rho(\pi_i^{(a)})\|_{op} \leq 4$ for $i \in [3]$ and $a \in [3]$.*

Then we can define Alice and Bob's projectors based on the approximate representation ρ of $\Gamma/\langle (t_1t_2)^{p(n)} = e\rangle$, the representation ρ_i of G_i for all $i \in [m]$, where G_i is defined in eq. (7.11), and the function σ introduced in Section 7.3.

- For question $g_{i,k} \in O_\Gamma$, Alice and Bob's projectors are

$$\tilde{P}_{g_{i,k}}^{(a)} = \rho(\sigma(g_{i,k}, a)),$$
$$\tilde{Q}_{g_{i,k}}^{(b)} = \rho(\sigma(g_{i,k}, b)^-)^\intercal.$$

- For question $i \in [m]$, Alice and Bob's projectors are

$$\tilde{P}_i^{(\boldsymbol{a})} = \rho_i(\sigma(i, \boldsymbol{a})),$$
$$\tilde{Q}_i^{(\boldsymbol{a})} = \rho_i(\sigma(i, \boldsymbol{a})^-)^\intercal,$$

  where $\boldsymbol{a} \in \mathbb{Z}_2^3$ represents the assignments to the three variables of an equation and the bijection between $\mathbb{Z}_2^3$ and $[8]$ is implicit.

- For question $g \in \{g_m, g_{m+1}, g_{m+2}\}$, we define $\{\tilde{P}_g^{(a)} \mid a \in [3]\}$ to be the projective measurements obtained by applying Proposition 7.14 to $\{\rho(\sigma(g, a)) \mid a \in [3]\}$; and we define $\{\tilde{Q}_g^{(a)} \mid a \in [3]\}$ to be the conjugate of the projective measurements obtained by applying Proposition 7.14 to $\{\rho(\sigma(g, a)^-) \mid a \in [3]\}$. For answers $a, b > 2$, $\tilde{P}_g^{(a)} = \tilde{Q}_g^{(b)} = 0$.

- For questions (g_m, t_1) and (g_m, t_2), we define $\{\tilde{P}_{(g_m,t_1)}^{(a_0,a_1)} \mid a_0 \in [4], a_1 \in [2]\}$

and $\{\tilde{P}^{(a_0,a_1)}_{(g_m,t_2)} \mid a_0 \in [4], a_1 \in [2]\}$ [5] by

$$\tilde{P}^{(a_0,a_1)}_{(g_m,t)} = \begin{cases} \tilde{P}^{(a_0)}_{g_m} \tilde{P}^{(a_1)}_{t_1} & \text{if } a_0 \in [3], \\ 0 & \text{otherwise,} \end{cases}$$

for $t \in \{t_1, t_2\}$. Note that by Proposition 7.14 $\tilde{P}^{(a_0)}_{g_m}$ commutes with $\rho(\pi_0^{(a_0)})$, which commutes with $\rho(t_1)$ and $\rho(t_2)$. So $\tilde{P}^{(a_0,a_1)}_{(g_m,t_1)}$ and $\tilde{P}^{(a_0,a_1)}_{(g_m,t_2)}$ are well defined projectors. In this case, Bob's projectors are defined by

$$\tilde{Q}^{(b_0,b_1)}_{(g_m,t)} = \begin{cases} \left(\tilde{P}^{(a_0)}_{g_m} \tilde{P}^{(a_1)}_{t_1}\right)^{\mathsf{T}} & \text{if } b_0 \in [3] \\ 0 & \text{otherwise} \end{cases}$$

for $t \in \{t_1, t_2\}$.

In summary, the strategy we construct is

$$S_{\epsilon,\zeta} = (|\mathsf{EPR}_d\rangle, \{\{\tilde{P}^{(a)}_x \mid a \in [8]\} \mid x \in O \cup [m]\}, \{\{\tilde{Q}^{(b)}_y \mid b \in [8]\} \mid y \in O \cup [m]\}).$$

We are going to show that there exist constants Δ_1 and Δ_2 independent of d such that

$$|\langle \mathsf{EPR}_d | \tilde{P}^{(a)}_x \otimes \tilde{Q}^{(b)}_y | \mathsf{EPR}_d \rangle - C_{n,\hat{z}}(a,b|x,y)| \le \Delta_1 \epsilon + \Delta_2 \zeta \tag{7.15}$$

for all $x, y \in O \cup [m]$ and $a, b \in [8]$.

[5] The bijection between $[4] \times [2]$ and $[8]$ is implicit.

To prove eq. (7.15), we use the following relations:

$$|\widetilde{\mathrm{Tr}}(\rho(g)) - f_{n,\hat{\boldsymbol{z}}}(g)| \leq \begin{cases} \epsilon & \text{if } g = e \text{ in } \Gamma / \langle (t_1 t_2)^{p(n)} = e \rangle \\ \\ \zeta & \text{if } g \neq e \text{ in } \Gamma / \langle (t_1 t_2)^{p(n)} = e \rangle \end{cases} \leq \epsilon + \zeta \tag{7.16}$$

for any $g \in W^+$;

$$\|\rho_i(g_{i,k}) - \rho(g_{i,k})\| \leq 13\epsilon \tag{7.17}$$

for all $g_{i,k} \in O_\Gamma$; and

$$\|\tilde{P}_g^{(a)} - \rho(\sigma(g,a))\| \leq 12^5\epsilon, \tag{7.18}$$

$$\|\tilde{Q}_g^{(a)\mathsf{T}} - \rho(\sigma(g,a)^-)\| \leq 12^5\epsilon, \tag{7.19}$$

for all $g \in \{g_m, g_{m+1}, g_{m+2}\}$, which follows Proposition 7.14 with $n = 3$ and $c = 4$. In particular, we know

$$|\langle \mathsf{EPR}_d|\rho(x)|\mathsf{EPR}_d\rangle - f_{n,\hat{\boldsymbol{z}}}(x)| \leq \zeta.$$

Based on these relations, we can also prove the following proposition.

Proposition 7.18. *For $x \in \{g_m, g_{m+1}, g_{m+2}\}$, $g \in O_\Gamma \cup \{e\}$ and $a, b \in [8]$*

$$|\widetilde{\mathrm{Tr}}(\rho(\sigma(x,a)\sigma(g,b)^-)) - f_{n,\hat{\mathbf{z}}}(\sigma(x,a)\sigma(g,b)^-)| \leq 4(\epsilon+\zeta), \tag{7.20}$$

$$|\widetilde{\mathrm{Tr}}(\rho(\sigma(g,b)\sigma(x,a)^-)) - f_{n,\hat{\mathbf{z}}}(\sigma(g,b)\sigma(x,a)^-)| \leq 4(\epsilon+\zeta). \tag{7.21}$$

For $x, y \in \{g_m, g_{m+1}, g_{m+2}\}$, $g \in O_\Gamma \cup \{e\}$ and $a, b \in [8]$,

$$|\widetilde{\mathrm{Tr}}(\rho(g)\rho(\sigma(x,a)\sigma(y,b)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(x,a)\sigma(y,b)^-)| \leq 15(\epsilon+\zeta), \tag{7.22}$$

$$|\widetilde{\mathrm{Tr}}(\rho(\sigma(x,a)\sigma(y,b)^-)\rho(g)) - f_{n,\hat{\mathbf{z}}}(\sigma(x,a)\sigma(y,b)^- g)| \leq 15(\epsilon+\zeta). \tag{7.23}$$

The proof of this proposition can be found in Appendix C.

Then, we can prove eq. (7.15) by examining all the different combinations of questions. When the questions are $g_{i,k}, g_{j,l} \in O_\Gamma$,

$$\begin{aligned}
&|C_{n,\hat{\mathbf{z}}}(a,b|g_{i,k},g_{j,l}) - \langle \mathsf{EPR}_d|\tilde{P}^{(a)}_{g_{i,k}} \otimes \tilde{Q}^{(b)}_{g_{j,l}}|\mathsf{EPR}_d\rangle| \\
\leq &\frac{1}{4}\Big[|f_{n,\hat{\mathbf{z}}}(e) - \widetilde{\mathrm{Tr}}(\rho(e))| + |f_{n,\hat{\mathbf{z}}}(g_{i,k}) - \widetilde{\mathrm{Tr}}(\rho(g_{i,k}))| \\
&\qquad + |f_{n,\hat{\mathbf{z}}}(g_{j,l}) - \widetilde{\mathrm{Tr}}(\rho(g_{j,l}))| + |f_{n,\hat{\mathbf{z}}}(g_{i,k}g_{j,l}) - \widetilde{\mathrm{Tr}}(\rho(g_{i,k}g_{j,l}))|\Big] \\
\leq &\epsilon + \zeta,
\end{aligned}$$

where we use eq. (7.16).

When the questions are $i, j \in [m]$, first notice that

$$\langle \mathsf{EPR}_d|\tilde{P}^{(\boldsymbol{a})}_i \otimes \tilde{Q}^{(\boldsymbol{b})}_j|\psi\rangle = \widetilde{\mathrm{Tr}}\left(\prod_{k\in I_i}\frac{\mathbb{1}+(-1)^{\boldsymbol{a}(k)}\rho_i(g_{i,k})}{2}\prod_{l\in I_j}\frac{\mathbb{1}+(-1)^{\boldsymbol{b}(l)}\rho_j(g_{j,l})}{2}\right).$$

If we write

$$\Pi_{i,j}^{(\boldsymbol{a},\boldsymbol{b})} = (\prod_{k\in I_i} \frac{\mathbb{1} + (-1)^{\boldsymbol{a}(k)}\rho(g_{i,k})}{2})(\prod_{l\in I_j} \frac{\mathbb{1} + (-1)^{\boldsymbol{b}(l)}\rho(g_{j,l})}{2}),$$

then

$$\begin{aligned}
&|C_{n,\hat{\boldsymbol{z}}}(\boldsymbol{a},\boldsymbol{b}|i,j) - \langle \mathsf{EPR}_d|\tilde{P}_i^{(\boldsymbol{a})} \otimes \tilde{Q}_j^{(\boldsymbol{b})}|\mathsf{EPR}_d\rangle| \\
\leq &|C_{n,\hat{\boldsymbol{z}}}(\boldsymbol{a},\boldsymbol{b}|i,j) - \widetilde{\mathrm{Tr}}(\Pi_{i,j}^{(\boldsymbol{a},\boldsymbol{b})})| + |\widetilde{\mathrm{Tr}}\left[\tilde{P}_i^{(\boldsymbol{a})}\tilde{Q}_j^{(\boldsymbol{b})\mathsf{T}} - \Pi_{i,j}^{(\boldsymbol{a},\boldsymbol{b})}\right]|,
\end{aligned}$$

and we can bound the two absolute values on the last line separately. For the first absolute value,

$$\begin{aligned}
&|C_{n,\hat{\boldsymbol{z}}}(\boldsymbol{a},\boldsymbol{b}|i,j) - \widetilde{\mathrm{Tr}}(\Pi_{i,j}^{(\boldsymbol{a},\boldsymbol{b})})| \\
\leq &\frac{1}{16}\Big[|f_{n,\hat{\boldsymbol{z}}}(e) - 1| + \sum_{k\in I_i}|f_{n,\hat{\boldsymbol{z}}}(g_{i,k}) - \widetilde{\mathrm{Tr}}(\rho(g_{i,k}))| \\
&\quad + \sum_{l\in I_j}|f_{n,\hat{\boldsymbol{z}}}(g_{j,l}) - \widetilde{\mathrm{Tr}}(\rho(g_{j,l}))| + \sum_{k\in I_i}\sum_{l\in I_j}|f_{n,\hat{\boldsymbol{z}}}(g_{i,k}g_{j,l}) - \widetilde{\mathrm{Tr}}(\rho(g_{i,k}g_{j,l}))|\Big] \\
\leq &\ \epsilon + \zeta,
\end{aligned}$$

which follows eq. (7.16). For the second absolute value,

$$
\begin{aligned}
&|\widetilde{\mathrm{Tr}}\left[\tilde{P}_i^{(\boldsymbol{a})}\tilde{Q}_j^{(\boldsymbol{b})\intercal} - \Pi_{i,j}^{(\boldsymbol{a},\boldsymbol{b})}\right]| \\
\leq &\frac{1}{16}\Big[|\widetilde{\mathrm{Tr}}(\rho_i(e)\rho_j(e) - \rho(e))| + \sum_{k\in I_i}|\widetilde{\mathrm{Tr}}(\rho(g_{i,k}) - \rho_i(g_{i,k}))| \\
&\quad + \sum_{l\in I_j}|\widetilde{\mathrm{Tr}}(\rho(g_{j,l}) - \rho_j(g_{j,l}))| + \sum_{k\in I_i}\sum_{l\in I_j}|\widetilde{\mathrm{Tr}}(\rho(g_{i,k}g_{j,l}) - \rho_i(g_{i,k})\rho_j(g_{j,l}))|\Big] \\
\leq &\frac{1}{16}\Big[0 + \sum_{k\in I_i}\|\rho(g_{i,k}) - \rho_i(g_{i,k})\| + \sum_{l\in I_j}\|\rho(g_{j,l}) - \rho_j(g_{j,l})\| \\
&\quad + \sum_{k\in I_i}\sum_{l\in I_j}|\widetilde{\mathrm{Tr}}(\rho(g_{i,k}g_{j,l}) - \rho_i(g_{i,k})\rho(g_{j,l}))| + |\widetilde{\mathrm{Tr}}(\rho_i(g_{i,k})\rho(g_{j,l}) - \rho_i(g_{i,k})\rho_j(g_{j,l}))|\Big] \\
\leq &\frac{1}{16}\Big[0 + 6\cdot 13\epsilon \\
&\quad + \sum_{k\in I_i}\sum_{l\in I_j}\|\rho(g_{j,l})\|_{op}\|\rho(g_{i,k}) - \rho_i(g_{i,k})\| + \|\rho_i(g_{i,k})\|_{op}\|\rho(g_{j,l}) - \rho_j(g_{j,l})\|\Big] \\
\leq &\frac{1}{16}\left(0 + 78\epsilon + 9\cdot 26\epsilon\right) \\
\leq &20\epsilon,
\end{aligned}
$$

which follows eq. (7.17). Overall,

$$|C_{n,\hat{\mathbf{z}}}(\boldsymbol{a},\boldsymbol{b}|i,j) - \langle \mathsf{EPR}_d|\tilde{P}_i^{(\boldsymbol{a})}\otimes\tilde{Q}_j^{(\boldsymbol{b})}|\mathsf{EPR}_d\rangle| \leq \zeta + 21\epsilon.$$

When one question is $g_{i,k}$ and the other question is $i \in [m]$, without loss of generality, we can assume Alice's question is $g_{i,k}$ and Bob's question is i. First notice that

$$
\begin{aligned}
&|C_{n,\hat{\boldsymbol{z}}}(a,\boldsymbol{b}|g_{i,k},i) - \langle \mathsf{EPR}_d|\tilde{P}^{(a)}_{g_{i,k}} \otimes \tilde{Q}^{(\boldsymbol{b})}_i|\mathsf{EPR}_d\rangle|\\
\leq &|C_{n,\hat{\boldsymbol{z}}}(a,\boldsymbol{b}|g_{i,k},i) - \widetilde{\mathrm{Tr}}(\rho(\frac{e+(-1)^a g_{i,k}}{2}\prod_{l\in I_i}\frac{e+(-1)^{\boldsymbol{b}(l)}g_{i,l}}{2}))|\\
&\quad + |\widetilde{\mathrm{Tr}}(\rho(\frac{e+(-1)^a g_{i,k}}{2})\Big[\rho(\prod_{l\in I_i}\frac{e+(-1)^{\boldsymbol{b}(l)}g_{i,l}}{2}) - \rho_i(\prod_{l\in I_i}\frac{e+(-1)^{\boldsymbol{b}(l)}g_{i,l}}{2})\Big])|.
\end{aligned}
$$

We first bound

$$
\begin{aligned}
&|C_{n,\hat{\boldsymbol{z}}}(a,\boldsymbol{b}|g_{i,k},i) - \widetilde{\mathrm{Tr}}(\rho(\frac{e+(-1)^a g_{i,k}}{2}\prod_{l\in I_i}\frac{e+(-1)^{\boldsymbol{b}(l)}g_{i,l}}{2}))|\\
\leq &\frac{1}{4}\left[|f_{n,\hat{\boldsymbol{z}}}(e) - \widetilde{\mathrm{Tr}}(\rho(e))| + \sum_{l\in I_i}|f_{n,\hat{\boldsymbol{z}}}(g_{i,l}) - \widetilde{\mathrm{Tr}}(\rho(g_{i,l}))|\right]\\
\leq &\epsilon + \zeta,
\end{aligned}
$$

where we use eq. (7.16). Next, we bound

$$
\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(\frac{e+(-1)^a g_{i,k}}{2})\Big[\rho(\prod_{l\in I_i}\frac{e+(-1)^{\boldsymbol{b}(l)}g_{i,l}}{2}) - \rho_i(\prod_{l\in I_i}\frac{e+(-1)^{\boldsymbol{b}(l)}g_{i,l}}{2})\Big])|\\
\leq &\|\rho(\frac{e+(-1)^a g_{i,k}}{2})\Big[\rho(\prod_{l\in I_i}\frac{e+(-1)^{\boldsymbol{b}(l)}g_{i,l}}{2}) - \rho_i(\prod_{l\in I_i}\frac{e+(-1)^{\boldsymbol{b}(l)}g_{i,l}}{2})\Big]\|\\
\leq &\frac{1}{4}\|\rho(\frac{e+(-1)^a g_{i,k}}{2})\|_{op}\|\sum_{l\in I_i}\rho(g_{i,l}) - \rho_i(g_{i,l})\|\\
\leq &13\epsilon,
\end{aligned}
$$

where we use eq. (7.17). Therefore,

$$|C_{n,\hat{\boldsymbol{z}}}(a,\boldsymbol{b}|g_{i,k},i) - \langle \mathsf{EPR}_d|\tilde{P}_{g_{i,k}}^{(a)} \otimes \tilde{Q}_i^{(\boldsymbol{b})}|\mathsf{EPR}_d\rangle| \leq 14\epsilon + \zeta.$$

When the questions are $g \in \{g_m, g_{m+1}, g_{m+2}\}$ and $g' \in O_\Gamma$, First notice that

$$\begin{aligned}
&|\langle \mathsf{EPR}_d|\tilde{P}_g^{(a)} \otimes \tilde{Q}_{g'}^{(b)}|\mathsf{EPR}_d\rangle - C_{n,\boldsymbol{z}}(a,b|g,g')| \\
\leq &|\widetilde{\mathrm{Tr}}(\tilde{P}_g^{(a)}\rho(\sigma(g',b)) - \rho(\sigma(g,a))\rho(\sigma(g',b)))| \\
&\qquad + |\widetilde{\mathrm{Tr}}(\rho(\sigma(g,a))\rho(\sigma(g',b))) - f_{n,\boldsymbol{z}}(\sigma(g,a)\sigma(g',b))| \\
\leq &\|(\tilde{P}_g^{(a)} - \rho(\sigma(g,a)))\rho(\sigma(g',b))\| + 4(\epsilon+\zeta) \\
\leq &\|\rho(\sigma(g',b))\|_{op}\|\tilde{P}_g^{(a)} - \rho(\sigma(g,a))\| + 4(\epsilon+\zeta) \\
\leq &(12^5+4)\epsilon + 4\zeta,
\end{aligned}$$

where we use $\|\rho(\sigma(g',b))\|_{op} = 1$ and Proposition 7.18.

When one questions is $g \in \{g_m, g_{m+1}, g_{m+2}\}$ and the other question is $i \in [m]$, without loss of generality, we can assume Alice's question is g and Bob's question is i. Then,

$$
\begin{aligned}
&|\langle \mathsf{EPR}_d|\tilde{P}_g^{(a)} \otimes \tilde{Q}_i^{(\boldsymbol{b})}|\mathsf{EPR}_d\rangle - C_{n,\hat{\boldsymbol{z}}}(a,\boldsymbol{b}|g,i)| \\
=&|\widetilde{\mathrm{Tr}}(\tilde{P}_g^{(a)}\frac{1}{4}(\rho_i(e) + \sum_{k\in I_i}\rho_i(g_{i,k}))) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g,a)\frac{1}{4}(e + \sum_{k\in I_i} g_{i,k}))| \\
\leq&\frac{1}{4}\Big[|\widetilde{\mathrm{Tr}}(\tilde{P}_g^{(a)}) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g,a))| + \sum_{k\in I_i}|\widetilde{\mathrm{Tr}}(\tilde{P}_g^{(a)}\rho_i(g_{i,k})) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g,a)g_{i,k})|\Big] \\
\leq&\frac{1}{4}\Big[|\widetilde{\mathrm{Tr}}(\tilde{P}_g^{(a)} - \rho(\sigma(g,a)))| + |\widetilde{\mathrm{Tr}}(\rho(\sigma(g,a))) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g,a))| \\
&\quad + \sum_{k\in I_i}\Big(|\widetilde{\mathrm{Tr}}(\tilde{P}_g^{(a)}\rho_i(g_{i,k})) - \tilde{P}_g^{(a)}\rho(g_{i,k})| + |\widetilde{\mathrm{Tr}}(\tilde{P}_g^{(a)}\rho(g_{i,k})) - \rho(\sigma(g,a)\rho(g_{i,k}))| \\
&\qquad + |\widetilde{\mathrm{Tr}}(\rho(\sigma(g,a)\rho(g_{i,k}))) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g,a)g_{i,k})|\Big) \\
\leq&\frac{1}{4}\Big[12^5\epsilon + 4(\epsilon+\zeta) + 3(13\epsilon + 12^5\epsilon + 4(\epsilon+\zeta))\Big] \\
\leq&(12^5+14)\epsilon + 4\zeta,
\end{aligned}
$$

where we apply Proposition 7.18. Similar derivations can be applied to the case that one question is $x \in \{(g_m, t_1), (g_m, t_2)\}$ and the other question is $y \in O_\Gamma$ to show that

$$
\begin{aligned}
|\langle \mathsf{EPR}_d|\tilde{P}_x^{(a)} \otimes \tilde{Q}_y^{(b)}|\mathsf{EPR}_d\rangle - C_{n,\hat{\boldsymbol{z}}}(a,b|x,y)| &\leq (12^5+4)\epsilon + 4\zeta \\
|\langle \mathsf{EPR}_d|\tilde{P}_y^{(b)} \otimes \tilde{Q}_x^{(a)}|\mathsf{EPR}_d\rangle - C_{n,\hat{\boldsymbol{z}}}(b,a|y,x)| &\leq (12^5+4)\epsilon + 4\zeta.
\end{aligned}
$$

Similar derivations can also be applied to the case that one question is $x \in \{(g_m, t_1),$

$(g_m, t_2)\}$ and the other question is $y \in [m]$ to show that

$$|\langle \mathsf{EPR}_d|\tilde{P}_x^{(a)} \otimes \tilde{Q}_y^{(\boldsymbol{b})}|\mathsf{EPR}_d\rangle - C_{n,\hat{\boldsymbol{z}}}(a,\boldsymbol{b}|x,y)| \leq (12^5 + 14)\epsilon + 4\zeta$$

$$|\langle \mathsf{EPR}_d|\tilde{P}_y^{(\boldsymbol{b})} \otimes \tilde{Q}_x^{(a)}|\mathsf{EPR}_d\rangle - C_{n,\hat{\boldsymbol{z}}}(\boldsymbol{b},a|y,x)| \leq (12^5 + 14)\epsilon + 4\zeta.$$

The next case is when $x, y \in \{g_m, g_{m+1}, g_{m+2}\}$. We can use Proposition 7.18 to see that

$$\begin{aligned}
&|\langle \mathsf{EPR}_d|\tilde{P}_x^{(a)} \otimes \tilde{Q}_y^{(b)}|\mathsf{EPR}_d\rangle - C_{n,\hat{\boldsymbol{z}}}(a,b|x,y)| \\
=&|\widetilde{\mathrm{Tr}}(\tilde{P}_x^{(a)}\tilde{Q}_y^{(b)\mathsf{T}}) - f_{n,\hat{\boldsymbol{z}}}(\sigma(x,a)\sigma(y,b)^-)| \\
\leq&|\widetilde{\mathrm{Tr}}((\tilde{P}_x^{(a)} - \rho(\sigma(x,a)))\tilde{Q}_y^{(b)\mathsf{T}})| + |\widetilde{\mathrm{Tr}}(\rho(\sigma(x,a))(\tilde{Q}_y^{(b)} - \rho(\sigma(y,b)^-)))| \\
&\qquad + |\widetilde{\mathrm{Tr}}(\rho(\sigma(x,a)\sigma(y,b)^-)) - f_{n,\hat{\boldsymbol{z}}}(\sigma(x,a)\sigma(y,b)^-)| \\
\leq&\|\tilde{Q}_y^{(b)\mathsf{T}}\|_{op}\|\tilde{P}_x^{(a)} - \rho(\sigma(x,a))\| + \|\rho(\sigma(x,a))\|_{op}\|\rho(\sigma(y,b)^-) - \tilde{Q}_y^{(b)}\| \\
&\qquad + |\widetilde{\mathrm{Tr}}(\rho(\sigma(x,a)\sigma(y,b)^-)) - f_{n,\hat{\boldsymbol{z}}}(\sigma(x,a)\sigma(y,b)^-)| \\
\leq&12^5\epsilon + 4 \cdot 12^5\epsilon + 15(\epsilon + \zeta) \\
=&5 \cdot 12^5\epsilon + 15\epsilon + 15\zeta
\end{aligned}$$

where we use eqs. (7.18) and (7.19) and Proposition 7.17 to bound $\|\rho(\sigma(x,a))\|_{op}$ by 4.

The last case is when $x \in \{g_m, g_{m+1}, g_{m+2}\}$ and $(g_m, t) \in \{(g_m, t_1), (g_m, t_2)\}$.

$$
\begin{aligned}
&|\langle \mathsf{EPR}_d|\tilde{P}_x^{(a)} \otimes \tilde{Q}_{(g_m,t)}^{(\boldsymbol{b})}|\mathsf{EPR}_d\rangle - C_{n,\hat{\boldsymbol{z}}}(a,\boldsymbol{b}|x,(g_m,t))| \\
=&|\widetilde{\mathrm{Tr}}(\tilde{P}_x^{(a)}\tilde{Q}_{g_m}^{(\boldsymbol{b}(0))\mathsf{T}}\rho(\sigma(t,\boldsymbol{b}(1))^-)) - C_{n,\hat{\boldsymbol{z}}}(a,\boldsymbol{b}|x,(g_m,t))| \\
\leq&\|\rho(\sigma(t,\boldsymbol{b}(1))^-)\|_{op}\|\tilde{Q}_{g_m}^{(\boldsymbol{b}(0))\mathsf{T}}\|_{op}\|\tilde{P}_x^{(a)} - \rho(\sigma(x,a))\| \\
&\quad + \|\rho(\sigma(t,\boldsymbol{b}(1))^-)\|_{op}\|\rho(\sigma(x,a))\|_{op}\|\tilde{Q}_{g_m}^{(\boldsymbol{b}(0))} - \rho(\sigma(g_m,\boldsymbol{b}(0))^-)\| \\
&\quad\quad + |\widetilde{\mathrm{Tr}}(\rho(\sigma(x,a)\sigma(g_m,\boldsymbol{b}(0))^-\sigma(t,\boldsymbol{b}(1))^-)) - f_{n,\hat{\boldsymbol{z}}}(\sigma(x,a)\sigma(g_m,\boldsymbol{b}(0))^-\sigma(t,\boldsymbol{b}(1))^-)| \\
\leq&12^5\epsilon + 4\cdot 12^5\epsilon + 15(\epsilon+\zeta).
\end{aligned}
$$

In summary, we can take $\Delta_1 = 5\cdot 12^5 + 15$ and $\Delta_2 = 15$ in eq. (7.15), and it implies that

$$
\lim_{\max(\zeta,\epsilon)\to 0^+} \langle \mathsf{EPR}_d|\tilde{P}_x^{(a)} \otimes \tilde{Q}_y^{(b)}|\mathsf{EPR}_d\rangle = C_{n,\hat{\boldsymbol{z}}}(a,b|x,y).
$$

Therefore, by Definition 4.8, $C_{n,\hat{\boldsymbol{z}}} \in C_{qa}(N,N,8,8)$ and $F_n \cap C_{qa}(N,N,8,8) \neq \emptyset$.

$\square$

Chapter 8: Conclusion and future work

In this dissertation, we proved that there exists an integer N such that when n_A, $n_B \geq N$ and $m_A, m_B \geq 8$, the decision problem (Membership$(n_A, n_B, m_A, m_B)_{qa}$) is coRE-hard, and the decision problem (Membership$(n_A, n_B, m_A, m_B)_{qc}$) is coRE-complete.

Leading to this result, we first proved a self-testing result in chapter 5. We showed that for any prime p with a primitive root r, there exists a correlation of size $\Theta(r^2)$ that can self-test a maximally entangled state of dimension $(p-1)$. Since there exists $r \in \{2, 3, 5\}$ that is a primitive root of infinitely many primes, we got a family of constant-sized correlations that can self-test maximally entangled states of unbounded dimension.

In chapters 6 and 7, we showed that for any recursively enumerable set X, there exists a family of sets of correlations $\{F_n | n \geq 0\}$ and a constant N such that the sizes of F_n's are the same, each correlation in F_n are in $\mathbb{K}^{N^2 \cdot 8^2}$, and

$$F_n \cap C_{qc}(N, N, 8, 8) = \emptyset \text{ if } n \in X,$$

$$F_n \cap C_{qa}(N, N, 8, 8) \neq \emptyset \text{ if } n \notin X.$$

Since $C_{qa}(N,N,8,8) \subseteq C_{qc}(N,N,8,8)$, we can determine that

$$F_n \cap C_{qc}(N,N,8,8) = \emptyset \text{ if and only if } n \in X,$$
$$F_n \cap C_{qa}(N,N,8,8) = \emptyset \text{ if and only if } n \in X.$$

The decision problem of determining if a fixed-sized set of correlations has non-trivial intersection with $C_t(n_A, n_B, m_A, m_B)$ is as hard as (Membership$(n_A, n_B, m_A, m_B)_t$), for $t \in \{q, qs, qa, qc\}$. Then, we concluded that (Membership$(n_A, n_B, m_A, m_B)_{qa}$) is coRE-hard, and the decision problem (Membership$(n_A, n_B, m_A, m_B)_{qc}$) is coRE-complete for $n_A, n_B \geq N$ and $m_A, m_B \geq 8$.

Next, we discuss open problems related to self-testing and membership problems of quantum correlations.

The nonlocal assumption of self-tests is a simple theoretical assumption, but it is hard to enforce in practice. It is natural ask if it is possible to replace the nonlocal assumption with a more practical assumption, for example, some computational assumption. Building on Urmila Mahadev's seminal work [44], Tony Metger and Thomas Vidick first proposed a protocol to self-test the EPR pair with a single computational assumption [45]. It will be interesting to see what other states can be self-tested with this computational assumption and if it is possible to convert existing self-tests under the nonlocal assumption to self-tests under this computational assumption systematically.

In this dissertation, we only proved the existence of the constant N but we did not estimate how big N is. It is natural to ask how small N can be. A recent result by Laura Mančinska, Jitendra Prakash and Christopher Schafhauser shows that correlations in $C_{qs}(4, 4, 2, 2)$ can robustly self-test maximally entangled states of unbounded dimension [46]. It is interesting to see if the new constant-sized self-tests can yield new proof of the same undecidability result with smaller correlations.

In this dissertation, we did not answer the hardness of (Membership$(n_A, n_B, m_A, m_B)_t$) for $t = q, qs$. We conjecture these problems are RE-complete for sufficiently large n_A, n_B, m_A and m_B. Our lower bound of (Membership$(n_A, n_B, m_A, m_B)_{qa}$) is not tight either. Hamoon Mousavi, Seyed Sajjed Nezhadi and Henry Yuen has proved that (Membership$(n_A, n_B, m_A, m_B)_{qa}$) is in Π_2^0 [47], which is one level above coRE in the arithmatical hierarchy. We also conjecture that (Membership$(n_A, n_B, m_A, m_B)_{qa}$) is Π_2^0-complete for sufficiently large n_A, n_B, m_A and m_B. To prove these conjectures, we need deeper understandings of techniques used in [8]. For example, one can try to investigate the implication of the compression scheme used in [8] on group presentation and approximate representations of groups. If we can prove (Membership$(n_A, n_B, m_A, m_B)_t$) for $t = q, qs$ are RE-complete, we expect the techniques can also allow us to prove (Membership$(n_A, n_B, m_A, m_B)_{qa}$) is Π_2^0-complete.

Appendix A: A few results about $\mathbb{Z}_p$-HNN extension

We first prove Theorem 3.29. This proof is based on the proof of Theorem 2.1 of Chapter IV in [36].

Proof of Theorem 3.29. Let W be the set of all normal forms from $\hat{G}$, and let $S(W)$ denote the group of all permutations of W. In order to define a homomorphism $\Psi : \hat{G} \to S(W)$, it suffices to define Ψ on G and t, and then show that all defining relations go to 1.

If $g \in G$, define $\Psi(g)$ by

$$\Psi(g)(g_0, t^{\epsilon_1}, \dots, t^{\epsilon_n}, g_n) = gg_0, t^{\epsilon_1}, \dots, t^{\epsilon_n}, g_n.$$

Clearly, $\Psi(g'g) = \Psi(g)\Psi(g')$. In particular, $\Psi(g)\Psi(g^{-1}) = \mathbb{1}_W = \Psi(g^{-1})\Psi(g)$, meaning that for all $w \in W$,

$$\Psi(g)\Psi(g^{-1})(w) = \Psi(g^{-1})\Psi(g)(w) = w.$$

Moreover, if $r = e$ in G, $\Psi(r) = \mathbb{1}_W$.

Next, we define the action of $\Psi(t)$. Let g_0, t^{ϵ_1}, g_1, …, t^{ϵ_n}, g_n be a normal form.

$$\Psi(t)(g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n)$$

$$= \begin{cases} \phi^{-1}(g_0)g_1, t^{\epsilon_2}, \ldots, t^{\epsilon_n}, g_n & \text{if } \epsilon_1 = -1 \text{ and } g_0 \in H, \\ \phi^{-1}(g_0), t, e, t, g_1, \ldots, t^{\epsilon_n}, g_n & \text{if } \epsilon_1 = 1, g_0 \in H, \\ & \text{and } t, g_1, \ldots t^{\epsilon_{(p-1)/2}} \neq t, e, t, \ldots, t \\ \phi^{-1}(g_0), \overbrace{t^{-1}, e, \ldots, e, t^{-1}}^{(p-1)/2 \text{ of } t^{-1}}, g_{\frac{p+1}{2}}, \ldots, t^{\epsilon_n}, g_n & \text{if } \epsilon_1 = -1, g_0 \in H, g_i = e, \epsilon_i = 1 \\ & \text{for } i = 1 \ldots (p-1)/2 \\ \phi^{-1}(h), t, \hat{g_0}, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n & \text{otherwise,} \end{cases}$$

where $\hat{g_0}$ is the representative of Hg_0 and $h\hat{g_0} = g_0$ with $h \in H$.

Then we can check $\Psi(t)^p = \mathbb{1}_W$. Let g_0, t^{ϵ_1}, g_1, ..., t^{ϵ_n}, g_n be a normal form. There are three cases. The first case is that $g_0 \notin H$. We can assume $h\hat{g_0} = g_0$

where $\hat{g_0}$ is the representative of Hg_0.

$$
\begin{aligned}
&\Psi(t)^p(g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n)\\
=&\Psi(t)^{p-1}(\phi^{-1}(h), t, \hat{g_0}, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n)\\
&\ldots\\
=&\Psi(t)^{(p-1)/2+1}(\phi^{-(p-1)/2}(h), \overbrace{t, e, t, \ldots, t}^{(p-1)/2 \text{ of } t}, \hat{g_0}, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n)\\
=&\Psi(t)^{(p-1)/2}(\phi^{-(p+1)/2}(h), \overbrace{t^{-1}, e, t^{-1}, \ldots, t^{-1}}^{(p-1)/2 \text{ of } t^{-1}}, \hat{g_0}, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n)\\
&\ldots\\
=&\phi^{-p}(h)\hat{g_0}, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n\\
=&h\hat{g_0}, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n\\
=&g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n,
\end{aligned}
$$

where, in the first part of the skipped steps, we apply case 2 of $\Psi(t)$ $\frac{p-3}{2}$ times, and, in the second part of the skipped steps, we apply case 1 of $\Psi(t)$ $\frac{p-1}{2}$ times.

The second case is that $g_0 \in H$ and $\epsilon_1 = 1$.

$$\begin{aligned}
&\Psi(t)^p(g_0, t, \ldots, t^{\epsilon_n}, g_n)\\
=&\Psi(t)^{(p+3)/2}(\phi^{-(p-3)/2}(g_0), \overbrace{t, e, \ldots, t}^{(p-1)/2 \text{ of } t}, g_1, \ldots, t^{\epsilon_n}, g_n)\\
=&\Psi(t)^{(p+1)/2}(\phi^{-(p-1)/2}(g_0), \overbrace{t^{-1}, e, \ldots, t^{-1}}^{(p-1)/2 \text{ of } t^{-1}}, g_1, \ldots, t^{\epsilon_n}, g_n)\\
=&\Psi(t)(\phi^{-p+1}(g_0)g_1, t^{\epsilon_2}, \ldots, t^{\epsilon_n}, g_n)\\
=&\phi^{-p}(g_0), t, g_1, t^{\epsilon_2}, \ldots, t^{\epsilon_n}, g_n\\
=&g_0, t, g_1, \ldots, t^{\epsilon_n}, g_n,
\end{aligned}$$

where we use the fact that $g_1 \notin H$. The last case is that $g_0 \in H$ and $\epsilon_1 = -1$.

$$\begin{aligned}
&\Psi(t)^p(g_0, t^{-1}, \ldots, t^{\epsilon_n}, g_n)\\
=&\Psi(t)^{p-1}(\phi^{-1}(g_0)g_1, t^{\epsilon_2}, \ldots, t^{\epsilon_n}, g_n)\\
=&\Psi(t)^{p-2}(\phi^{-2}(g_0), t, g_1, t^{\epsilon_2}, \ldots, t^{\epsilon_n}, g_n)\\
=&\Psi(t)^{(p-1)/2}(\phi^{-(p+1)/2}(g_0), \overbrace{t, e, \ldots, t}^{(p-1)/2 \text{ of } t}, g_1, \ldots, g_n)\\
=&\Psi(t)^{(p-3)/2}(\phi^{-(p+3)/2}(g_0), \overbrace{t^{-1}, e, \ldots, t^{-1}}^{(p-1)/2 \text{ of } t^{-1}}, g_1, \ldots, g_n)\\
=&\phi^{-p}(g_0), t^{-1}, g_1, t^{\epsilon_2}, \ldots, t^{\epsilon_n}, g_n\\
=&g_0, t^{-1}, g_1, \ldots, t^{\epsilon_n}, g_n.
\end{aligned}$$

Therefore, $\Psi(t)^p = \mathbb{1}_W$. Then, $\Psi(\phi(h)) = \Psi(t^{-1})\Psi(h)\Psi(t)$. We can see that Ψ is a well-defined homomorphism from $\hat{G}$ into $S(W)$.

We can also see that if $g_0 \notin H$ and $g_0 = h\hat{g_0}$

$$\Psi(t^{-1})(g_0, t^{\epsilon_1}, \dots, t^{\epsilon_n}, g_n) = \phi(h), t^{-1}, \hat{g_0}, t^{\epsilon_1}, \dots, t^{\epsilon_n}, g_n.$$

and if $g_0 \in H$, $\epsilon_1 = -1$ and the subsequence

$$t^{\epsilon_1}, g_1, t^{\epsilon_2}, \dots, t^{\epsilon_{(p-1)/2}} \neq \overbrace{t^{-1}, e, \dots, t^{-1}}^{(p-1)/2 \text{ of } t^{-1}},$$

then

$$\Psi(t^{-1})(g_0, t^{-1}, \dots, t^{\epsilon_n}, g_n) = \phi(g_0), t^{-1}, e, t^{-1}, \dots, t^{\epsilon_n}, g_n.$$

We can see that if g_0, t^{ϵ_1}, g_1, ..., t^{ϵ_n}, g_n is a normal form,

$$\Psi(g_0 t^{\epsilon_1} g_1 \dots t^{\epsilon_n} g_n)(e) = g_0, t^{\epsilon_1}, g_1, \dots, t^{\epsilon_n}, g_n.$$

Thus the products of the elements in distinct normal forms represent distinct elements of $\hat{G}$, otherwise, Ψ would not be well-defined. □

Next, we prove Proposition 3.52, which follows a similar line of argument as the proof of [37, Property 8 of Proposition 2.4.1].

Proof of Proposition 3.52. By Theorem 3.31 and Proposition 3.49, to prove $\hat{G}$ is sofic, it suffices to prove K is sofic, where K is the subgroup of $\hat{G}$ generated by $t^{-i}Gt^i$ for $i = 0, 1, \dots, p-1$.

Let K_j be the subgroup of $\hat{G}$ generated by $t^{-i}Gt^i$ for $0 \leq i \leq j$. Then, $K_{p-1} = K$ and we will prove K_{p-1} is sofic by induction on j. The base case is $j = 0$, and $K_0 = G$ is sofic follows from the condition of the proposition.

Assume K_n is sofic for some $0 \leq n < p-1$. Then, we will show that

$$K_{n+1} \cong K^* := \frac{K_n * G}{\langle \phi^{n+1}(h) = h | h \in H \rangle},$$

where $\phi^{n+1}(h) \in K_{n+1}$ and $h \in G$. Consider $\Psi : K_{n+1} \to K^*$ induced by

$$\Psi(k) = \begin{cases} k & \text{if } k \in K_n; \\ t^{n+1}kt^{-n-1} & \text{otherwise.} \end{cases}$$

It is immediate that Ψ is surjective. On the other hand, $k = e$ in K_{n+1} if and only if k is in the normal subgroup generated by $t^{-i}ht^i\phi^{-i}(h)$ for all $h \in H$ and $1 \leq i \leq n+1$. For relations of the form $t^{-i}ht^i = \phi^i(h)$ for all $h \in H$ and $1 \leq i \leq n$, $\Psi(t^{-i}ht^i\phi^{-i}(h)) = t^{-i}ht^i\phi^{-i}(h) = e$ as this relation is also in K_n. For relations of the form $t^{-n-1}ht^{n+1} = \phi^{n+1}(h)$,

$$\Psi(t^{-n-1}ht^{n+1}\phi^{n+1}(h)) = \Psi(t^{-n-1}ht^{n+1})\Psi(\phi^{-n-1}(h)) = h\phi^{-n-1}(h) = e,$$

which follows the added relations. Therefore, Ψ descends to an isomorphism between the normal subgroup generated by $t^{-i}ht^i\phi^{-i}(h)$ for all $h \in H$ and $1 \leq i \leq n+1$ in K_{n+1} and the normal subgroup generated by $t^{-i}ht^i\phi^{-i}(h)$ and $h^{-1}\phi^{n+1}(h)$ for all $h \in H$ and $1 \leq i \leq n$ in K^*. It implies that $\Psi(k) = e$ in K^* if and only if

$k = e$ in K_{n+1} and Ψ is injective. Hence, Ψ is an isomorphism.

Then, by Proposition 3.50 and the induction assumption, K_{n+1} is also sofic.

By the principle of induction, K_{p-1} is sofic and the proof is complete. $\square$

Appendix B: Steps of the fa^*-embedding procedure

In this section, we describe the steps of the fa^*-embedding procedure summarized in Propositions 3.55 and 3.56.

Let l, m and n be some positive integer, and let $G = E\Gamma(A, C_0, C_1, L)$ be an extended homogeneous linear-plus-conjugacy group, where A is an m-by-n matrix over $\mathbb{Z}_2$, $C_0 \subseteq [n] \times [n] \times [n]$, $C_1 \subseteq [l] \times [n] \times [n]$ and L is an $l \times l$ lower-triangular matrix with non-negative integer entries, as in Definition 3.54. The generators of G are $\{x_i \mid i \in [n]\}$ and $\{y_i \mid i \in [l]\}$. The relations are

$$
\begin{aligned}
&x_i^2 = e && \text{for all } i \in [n]; \\
&\prod_{k \in I_j} x_k = e && \text{for all } j \in [m]; \\
&x_i x_j x_i = x_k && \text{for all } (i,j,k) \in C_0; \\
&y_i^{-1} x_j y_i = x_k && \text{for all } (i,j,k) \in C_1; \\
&y_i^{-1} y_j y_i = y_j^{L(i,j)} && \text{for all } i > j \text{ with } L(i,j) > 0.
\end{aligned}
$$

In the first step of the embedding procedure, we embed G into a linear-plus-conjugacy group. Let $G' = \langle G, z, w : z^2 = w^2 = e, y_0 = zw, wy_iw = y_i \text{ for all } i > 0\rangle$. Then G' is also an extended homogeneous linear plus conjugacy group. This is because for any relation of the form $y_0^{-1}x_jy_0 = x_k$, we know

$$zx_jz = wx_kw \text{ and } (zx_jz)^2 = (wx_kw)^2 = e.$$

If we let $Z_{jk} = zx_jz$, then

$$Z_{jk} = wx_kw.$$

In addition, for any relation of the form $y_j^{-1}y_0y_j = y_k$, we know

$$y_j^{-1}zy_j = (zw)^{L(0,j)-1}z \text{ and } \left((zw)^{L(0,j)-1}z\right)^2 = e.$$

Then, we can replace the relation $y_j^{-1}zy_j = (zw)^{L(0,j)-1}z$ with a sequence of conjugacy relations of generators of order 2. Moreover, G is fa^*-embedded in G', as proved in [7, Proposition 33].

By embedding G into G', we remove y_0 from the set of generators of G and introduce more generators of order 2 and more conjugacy relations. We can repeat this process for each y_i with $i > 0$ to embed G into a linear-plus-conjugacy group H where $\{x_i \mid i \in [n]\}$ is a subset of the set of generators of H. We can assume $H = \Gamma(A', C)$ where A' is an m'-by-n' matrix over $\mathbb{Z}_2$ and $C \subseteq [n'] \times [n'] \times [n']$ for some positive integer $m' > m$ and $n' > n$.

In the second step, we embed H into a linear-plus-conjugacy group $H' = \Gamma(B, D)$ where B is an M-by-N matrix over $\mathbb{Z}_2$ and $D \subseteq [N] \times [N] \times [N]$ for some $M > m'$ and $N > n'$. Moreover, in H', $x_ix_jx_i = x_k$ if and only if $x_jx_kx_j = x_k$ for all

$(i, j, k) \in D$. Here,

$$H' = \langle H, u, w_i, y_i, z_i \text{ for } i \in [n'] : u^2 = w_i^2 = y_i^2 = z_i^2 = e \text{ for } i \in [n'],$$
$$x_i = y_i z_i = u w_i \text{ and } u y_i u = z_i \text{ for } i \in [n'],$$
$$z_k y_j z_k = y_j, w_i y_j w_i = z_k \text{ for all } (i, j, k) \in C\rangle$$

An injective homomorphism $\phi : H \to H'$ is defined by $x_i \mapsto x_i$ for all $i \in [n']$. Moreover, ϕ is a fa^*-embedding as proved in [7, Lemma 29].

In the last step, we embed the group H' into a solution group K. We extend the linear system $B\boldsymbol{x} = 0$ by adding variables $v_{I,l}$ for all $I \in D$ and $1 \le l \le 7$, and adding equations

$$x_i + v_{I,1} + v_{I,2} = 0, \qquad x_j + v_{I,2} + v_{I,3} = 0, \qquad v_{I,3} + v_{I,4} + v_{I,5} = 0,$$
$$x_i + v_{I,5} + v_{I,6} = 0, \qquad x_k + v_{I,6} + v_{I,7} = 0, \qquad v_{I,1} + v_{I,4} + v_{I,7} = 0.$$

if $I = (i, j, k) \in D$. If we denote the new linear system by $B_{ext}\boldsymbol{x} = 0$, then $K := \Gamma(B_{ext})$. The embedding of H' into K maps x_i to x_i for each $i \in [N]$, which is also an fa^*-embedding as proved in [7, Proposition 27].

Overall, we can see that G is embedded in K and, under this embedding, the image of x_i is x_i for each $i \in [n]$ and the image of y_j is a product of two order-2 generators for each $j \in [l]$.

Appendix C: Proof of some results in chapter 7

C.1 Proof of Theorem 7.10

To help the proof, we first present certain nonzero values of $\overline{Q}_{-\pi/p}$. When $x = y = 0$,

$$\overline{Q}_{-\pi/p}(a,b|0,0) = \begin{cases} \frac{1}{p} & \text{if } a = b = 0, \\ \frac{2}{p} & \text{if } a = b = 1, \\ \frac{p-3}{p} & \text{if } a = b = 2, \\ 0 & \text{otherwise.} \end{cases}$$

When $x \in \{t_1, t_2\}$ and $y \in \{1, 2\}$, some of the values of $\overline{Q}_{-\pi/p}(a,b|x,y)$ are summarized in the following table.

		$y=1$		$y=2$	
		$b=0$	$b=1$	$b=0$	$b=1$
$x=t_1$	$a=0$	$\frac{\cos^2(\pi/2p)}{p}$	$\frac{\sin^2(\pi/2p)}{p}$	$\frac{1-\sin(\pi/p)}{2p}$	$\frac{1+\sin(\pi/p)}{2p}$
	$a=1$	$\frac{\sin^2(\pi/2p)}{p}$	$\frac{\cos^2(\pi/2p)}{p}$	$\frac{1+\sin(\pi/p)}{2p}$	$\frac{1-\sin(\pi/p)}{2p}$
$x=t_2$	$a=0$	$\frac{\cos^2(\pi/2p)}{p}$	$\frac{\sin^2(\pi/2p)}{p}$	$\frac{1+\sin(\pi/p)}{2p}$	$\frac{1-\sin(\pi/p)}{2p}$
	$a=1$	$\frac{\sin^2(\pi/2p)}{p}$	$\frac{\cos^2(\pi/2p)}{p}$	$\frac{1-\sin(\pi/p)}{2p}$	$\frac{1+\sin(\pi/p)}{2p}$

Table C.1: $\overline{Q}_{-\pi/p}$: the correlation values for $x \in \{t_1, t_2\}$ and $y \in \{1, 2\}$.

When $x, y \in \{0,1,2\}$, some of the values of $\overline{Q}_{-\pi/p}(a,b|x,y)$ is summarized in the following table.

		$x=1$			$x=2$			$x=0$	
		$a=0$	$a=1$	$a=2$	$a=0$	$a=1$	$a=2$	$a=1$	$a\neq 1$
$y=1$	$b=0$	$\frac{1}{p}$	0	0	$\frac{1}{2p}$	$\frac{1}{2p}$	0	$\frac{1}{p}$	0
	$b=1$	0	$\frac{1}{p}$	0	$\frac{1}{2p}$	$\frac{1}{2p}$	0	$\frac{1}{p}$	0
	$b=2$	0	0	$\frac{p-2}{p}$	0	0	$\frac{p-2}{p}$	0	$\frac{p-2}{p}$
$y=2$	$b=0$	$\frac{1}{2p}$	$\frac{1}{2p}$	0	$\frac{1}{p}$	0	0	$\frac{1}{p}$	0
	$b=1$	$\frac{1}{2p}$	$\frac{1}{2p}$	0	0	$\frac{1}{p}$	0	$\frac{1}{p}$	0
	$b=2$	0	0	$\frac{p-2}{p}$	0	0	$\frac{p-2}{p}$	0	$\frac{p-2}{p}$
$y=0$	$b=1$	$\frac{1}{p}$	$\frac{1}{p}$	0	$\frac{1}{p}$	$\frac{1}{p}$	0	$\frac{2}{p}$	0
	$b\neq 1$	0	0	$\frac{p-2}{p}$	0	0	$\frac{p-2}{p}$	0	$\frac{p-2}{p}$

Table C.2: $\overline{Q}_{-\pi/p}$: the correlation values for $x, y \in \{0,1,2\}$.

When $x \in \{0, t_1\}$ and $y = (0, t_1)$ the commutation test is conducted and the correlation is given in the table below.

		$y=(0,t_1)$					
		$b=(0,0)$	$b=(0,1)$	$b=(1,0)$	$b=(1,1)$	$b=(2,0)$	$b=(2,1)$
$x=0$	$a=0$	$\frac{1}{2p}$	$\frac{1}{2p}$	0	0	0	0
	$a=1$	0	0	$\frac{1}{p}$	$\frac{1}{p}$	0	0
	$a=2$	0	0	0	0	$\frac{p-3}{2p}$	$\frac{p-3}{2p}$
$x=t_1$	$a=0$	$\frac{1}{2p}$	0	$\frac{1}{p}$	0	$\frac{p-3}{2p}$	0
	$a=1$	0	$\frac{1}{2p}$	0	$\frac{1}{p}$	0	$\frac{p-3}{2p}$

Table C.3: $\overline{Q}_{-\pi/p}$: the correlation values for the commutation test for Alice's questions 0 and t_1.

When $x = (0, t_1)$ and $y = (0, t_2)$, for $a, b \in [2]$,

$$\overline{Q}_{-\pi/p}((0,a),(0,b)|(0,t_1),(0,t_2)) = \begin{cases} 1/p & \text{if } a = b = 0, \\ 1/p & \text{if } a = b = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{C.1}$$

Proof of Theorem 7.10. To prove this theorem, we need to find a decomposition of $|\psi\rangle$ as $|\psi\rangle = \sum_{j\in[p+1]} |\psi_j\rangle$ such that $\{|\psi_i\rangle\}$ is an orthogonal set and each $|\psi_i\rangle$ is an eigenvector of $M_{t_1}M_{t_2}$ with an eigenvalue that equals some power of ω_p.

Applying Proposition 4.14 to the values given in Table C.3, we can get that

$$M_x^{(a_x)} M_0^{(a_0)} |\psi\rangle = N_{(0,x)}^{(a_0,a_x)} |\psi\rangle = M_0^{(a_0)} M_x^{(a_x)} |\psi\rangle$$

for $a_0 \in [3]$, $x \in \{t_1, t_2\}$ and $a_x \in [2]$.

Applying Proposition 4.13 to given in eq. (C.1), we can get that

$$M_{(0,t_1)}^{(0,a_1)} |\psi\rangle = N_{(0,t_2)}^{(0,a_1)} |\psi\rangle$$

for each $a_1 \in [2]$. Then, we can further deduce that

$$M_{t_1}^{(a_1)} M_0^{(0)} |\psi\rangle = N_{(0,t_2)}^{(0,a_1)} |\psi\rangle = M_{t_2}^{a_1} M_0^{(0)} |\psi\rangle. \tag{C.2}$$

Let $M_x := M_x^{(0)} - M_x^{(1)}$ and $N_y := N_y^{(0)} - N_y^{(1)}$ for $x, y = t_1, t_2$, and let

$$|\psi_0\rangle = M_{t_1}^{(0)} M_0^{(0)} |\psi\rangle,$$
$$|\psi_p\rangle = M_{t_1}^{(1)} M_0^{(0)} |\psi\rangle.$$

Then we know from the correlation in Table C.2 and the definitions of $|\psi_0\rangle$ and $|\psi_p\rangle$ that

$$\||\psi_0\rangle\|^2 = \||\psi_p\rangle\|^2 = \frac{1}{2p},$$
$$M_{t_1}|\psi_0\rangle = |\psi_0\rangle,$$
$$M_{t_1}|\psi_p\rangle = -|\psi_p\rangle,$$

and hence $\langle\psi_0|\psi_p\rangle = 0$. By eq. (C.2), we know

$$|\psi_0\rangle = M_2^0 M_0^0 |\psi\rangle,$$
$$|\psi_p\rangle = M_2^1 M_0^0 |\psi\rangle.$$

The definition of M_2 implies that

$$M_2|\psi_0\rangle = |\psi_0\rangle,$$
$$M_2|\psi_p\rangle = -|\psi_p\rangle.$$

Following the proof of Proposition 5.8, we can conclude from Tables C.1

and C.2 that

$$S = (\frac{M_0^{(1)}|\psi\rangle}{\|M_0^{(1)}|\psi\rangle\|}, \{\{M_x^{(0)}, M_x^{(1)}\} \mid x = 1,2\}, \{\{N_y^{(0)}, N_y^{(1)}\} \mid y = t_1, t_2\})$$

induces the correlation $Q_{-\pi/p}$; and that

$$S_f = (\frac{M_0^{(1)}|\psi\rangle}{\|M_0^{(1)}|\psi\rangle\|}, \{\{M_x^{(0)}, M_x^{(1)}\} \mid x = t_1, t_2\}, \{\{N_y^{(0)}, N_y^{(1)}\} \mid y = 1,2\})$$

induces the correlation of $Q_{-\pi/p}$ with Alice and Bob's roles flipped. Then we can define $M_2 := M_2^{(0)} - M_2^{(1)}$ and

$$|\psi_1\rangle = \frac{1}{2}(M_1^{(0)} - iM_2M_1^{(1)} + iM_2M_1^{(0)} + M_1^{(1)})|\psi\rangle.$$

Following the proof of Proposition 5.8, we can conclude that

$$\begin{aligned}
\||\psi_1\rangle\|^2 &= \frac{1}{p}, \\
M_{t_1}M_{t_2}|\psi_1\rangle &= \omega_p|\psi_1\rangle, \\
N_{t_1}N_{t_2}|\psi_1\rangle &= \omega_p^{-1}|\psi_1\rangle.
\end{aligned}$$

Recall the conditions satisfied by U_A and U_B in the statement of the theorem. Define

$$|\psi_j\rangle = (U_AU_B)^{\log_r j}|\psi_1\rangle$$

for $j = 1, \ldots, p-1$. Note that $\log_r j = a$ implies that $r^a \equiv j \pmod{p}$. It is easy to see that $\||\psi_j\rangle\|^2 = 1/p$. Following the proof of Proposition 5.8, we can get that

$$(M_{t_1} M_{t_2})|\psi_j\rangle = \omega_p^j |\psi_j\rangle,$$
$$(N_{t_1} N_{t_2})|\psi_j\rangle = \omega_p^{-j} |\psi_j\rangle.$$

By the orthogonality between eigenvectors of different eigenvalues, we know that

$$\langle \psi_j | \psi_k \rangle = 0$$

for each $1 \leq j \neq k \leq p-1$.

Define

$$|\psi'\rangle = |\psi_0\rangle + |\psi_p\rangle + \sum_{j=1}^{p-1} |\psi_j\rangle. \tag{C.3}$$

By the orthogonality relations and the norms of each subnormalized state, we can calculate that $\||\psi'\rangle\| = 1$. Moreover,

$$\begin{aligned}\langle \psi | \psi' \rangle =& \langle \psi | \psi_0 \rangle + \langle \psi | \psi_p \rangle + \sum_{j=1}^{p-1} \langle \psi | \psi_j \rangle \\ =& \||\psi_0\rangle\|^2 + \||\psi_p\rangle\|^2 + (p-1)\langle \psi | \psi_1 \rangle \\ =& \frac{1}{p} + (p-1)\frac{1}{p} = 1,\end{aligned}$$

where we use $(U_A U_B)|\psi\rangle = |\psi\rangle$. The derivation of $\langle\psi|\psi_1\rangle = 1/p$ follows the similar derivation in the proof of Proposition 5.8.

With the decomposition of $|\psi\rangle$, we can conclude that

$$
\begin{aligned}
&(M_{t_1}M_{t_2})^p|\psi\rangle \\
=&(M_{t_1}M_{t_2})^p(|\psi_0\rangle + |\psi_p\rangle + \sum_{j=1}^{p-1}|\psi_j\rangle) \\
=&1^p(|\psi_0\rangle + |\psi_p\rangle) + \sum_{j=1}^{p-1}\omega_p^{jp}|\psi_j\rangle \\
=&|\psi\rangle,
\end{aligned}
$$

which completes the proof. □

C.2 Proof of Proposition 7.16

Proof. The first case to check is that when the questions are $g_{i,k}$ and $g_{j,k}$ where $k \in I_i \cap I_j$.

$$
\begin{aligned}
&C_{n,\hat{\mathbf{z}}}(0,0|g_{i,k},g_{j,k}) + C_{n,\hat{\mathbf{z}}}(1,1|g_{i,k},g_{j,k}) \\
=&f_{n,\hat{\mathbf{z}}}\left(\frac{(e+g_{i,k})(e+g_{j,k})}{4} + \frac{(e-g_{i,k})(e-g_{j,k})}{4}\right) \\
=&f_{n,\hat{\mathbf{z}}}\left(\frac{e+g_{i,k}g_{j,k}}{2}\right) \\
=&1,
\end{aligned}
$$

which satisfies **P.6** of Definition 4.16.

The second case is that one question is $i \in [m]$ and the other question is $g_{i,k}$ with $k \in I_i$. Assuming $I_i = \{k, l, m\}$,

$$\begin{aligned}
&\sum_{\boldsymbol{a} \in S_i} C_{n,\hat{\boldsymbol{z}}}(\boldsymbol{a}, \boldsymbol{a}(k)|i, g_{j,k}) \\
=&\frac{1}{16} f_{n,\hat{\boldsymbol{z}}}\Big((e - g_{i,k})^2 \left[(e + g_{i,l})(e - g_{i,m}) + (e - g_{i,l})(e + g_{i,m})\right] \\
&\qquad + (1 + g_{i,k})^2 \left[(e - g_{i,l})(e - g_{i,m}) + (e + g_{i,l})(e + g_{i,m})\right]\Big) \\
=&\frac{1}{8} f_{n,\hat{\boldsymbol{z}}}\Big((e - g_{i,k})^3 + (e + g_{i,k})^3\Big) \\
=&\frac{1}{2} f_{n,\hat{\boldsymbol{z}}}\Big(e - g_{i,k} + e + g_{i,k}\Big) \\
=&1,
\end{aligned}$$

which satisfies **P.5** of Definition 4.16. Property **P.4** can be checked similarly.

The last case is that the questions are $i, j \in [m]$. First notice that if $\boldsymbol{a} \notin S_i$,

$$\prod_{k \in I_i} \frac{e + (-1)^{\boldsymbol{a}(k)} g_{i,k}}{2} = 0.$$

Secondly, notice that if $\boldsymbol{a} \in S_i$ and $\boldsymbol{b} \in S_j$ but $\boldsymbol{a}(k) \neq \boldsymbol{b}(k)$, the expansion of

$$\prod_{l \in I_i} \prod_{m \in I_j} \frac{e + (-1)^{\boldsymbol{a}(l)} g_{i,l}}{2} \frac{e + (-1)^{\boldsymbol{b}(m)} g_{j,m}}{2}$$

contains a term $(1 - g_{i,k})(1 + g_{j,k}) = 0$. Therefore, $C_{n,\hat{\boldsymbol{z}}}(\boldsymbol{a}, \boldsymbol{b}|i, j)$ satisfies **P.3** of Definition 4.16. The other three properties of Definition 4.16 are enforced in the function σ introduced in Section 7.3. $\square$

C.3 Proof of Proposition 7.17

Proof. Recall the expressions in eq. (7.2) to eq. (7.10). To bound the operator norms of $\rho(\pi_i^{(a)})$, because $\rho(t_1t_2)$ is a unitary, it suffices to consider the action of the operators on an eigenvector of $\rho(t_1t_2)$. Let $|\psi\rangle$ be an eigenvector of $\rho(t_1t_2)$ such that $\rho(t_1t_2)|\psi\rangle = e^{i\theta}|\psi\rangle$.

$$\|\rho(\pi_0^{(0)})|\psi\rangle\| = \frac{1}{p(n)}\|\sum_{j\in[p(n)]}\rho(t_1t_2)^j|\psi\rangle\| \leq \frac{1}{p(n)}\sum_{j\in[p(n)]}\|e^{ij\theta}|\psi\rangle\| \leq 1,$$

$$\|\rho(\pi_0^{(1)})|\psi\rangle\| \leq \frac{2}{p(n)}\sum_{j\in[p(n)]}|\cos(\frac{2j\pi}{p(n)})|\|e^{ij\theta}|\psi\rangle\| \leq 2,$$

$$\|\rho(\pi_0^{(2)})|\psi\rangle\| \leq \||\psi\rangle\| + \|\rho(\pi_0^{(0)})|\psi\rangle\| + \|\rho(\pi_0^{(1)})|\psi\rangle\| \leq 4,$$

where we use $|\cos(\frac{2j\pi}{p(n)})| \leq 1$. Recall that

$$\pi_1^{(0)} = \pi_0^{(1)}/2 + \frac{1}{p(n)}\sum_{j\in[p(n)]}\cos(\frac{(2j+1)\pi}{p(n)})t_2(t_1t_2)^j,$$

$$\pi_2^{(0)} = \pi_0^{(1)}/2 + \frac{1}{p(n)}\sum_{j\in[p(n)]}\sin(\frac{(2j+1)\pi}{p(n)})t_2(t_1t_2)^j.$$

Then,

$$\|\rho(\pi_1^{(0)})|\psi\rangle\| \leq \frac{1}{2}\|\rho(\pi_0^{(1)})|\psi\rangle\| + \frac{1}{p(n)}\sum_{j\in[p(n)]}|\cos(\frac{(2j+1)\pi}{p(n)})|\|\rho(t_2)e^{ij\theta}|\psi\rangle\|$$

$$\leq 1+1 = 2,$$

where we use the fact that $\rho(t_2)$ is a unitary. With similar reasoning, we can get that

$$
\begin{aligned}
\|\rho(\pi_1^{(1)})|\psi\rangle\| \leq& 2, \\
\|\rho(\pi_1^{(2)})|\psi\rangle\| \leq& \||\psi\rangle\| + \|\rho(\pi_0^{(1)})|\psi\rangle\| \leq 3, \\
\|\rho(\pi_2^{(0)})|\psi\rangle\| \leq& 2, \\
\|\rho(\pi_2^{(1)})|\psi\rangle\| \leq& 2, \\
\|\rho(\pi_2^{(2)})|\psi\rangle\| \leq& \||\psi\rangle\| + \|\rho(\pi_0^{(1)})|\psi\rangle\| \leq 3,
\end{aligned}
$$

which completes the proof. □

C.4 Proof of Proposition 7.18

Proof. We first prove eq. (7.20), then eq. (7.21) follows analogously. By the definitions of $\sigma(x, a)$ and $\sigma(g, b)^{-}$, we can focus on the case that $a \in [3]$ and $b \in [2]$.

Recall eq. (7.2), and we know

$$
\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(\sigma(g_m,0)\sigma(g,b)^-)) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g_m,0)\sigma(g,b)^-)| \\
=&\frac{1}{2p(n)}|\widetilde{\mathrm{Tr}}(\sum_{j\in[p(n)]}\rho((t_1t_2)^j)\rho(e+(-1)^b g)) - f_{n,\hat{\boldsymbol{z}}}(\sum_{j\in[p(n)]}(t_1t_2)^j(e+(-1)^b g))| \\
\leq&\frac{1}{2p(n)}\sum_{j\in[p(n)]}\Big[|\widetilde{\mathrm{Tr}}(\rho((t_1t_2)^j)) - f_{n,\hat{\boldsymbol{z}}}((t_1t_2)^j)| + |\widetilde{\mathrm{Tr}}(\rho((t_1t_2)^j g)) - f_{n,\hat{\boldsymbol{z}}}((t_1t_2)^j g)|\Big] \\
\leq&\frac{1}{2p(n)}2(\epsilon+\zeta)\cdot p(n) \\
\leq&\epsilon+\zeta.
\end{aligned}
$$

Recall eq. (7.3), and we know

$$
\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(\sigma(g_m,1)\sigma(g,b)^-)) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g_m,1)\sigma(g,b)^-)| \\
=&\frac{1}{p(n)}|\widetilde{\mathrm{Tr}}(\sum_{j\in[p(n)]}\cos(\frac{2j\pi}{p(n)})\rho((t_1t_2)^j)\rho(e+(-1)^b g)) \\
&\qquad - f_{n,\hat{\boldsymbol{z}}}(\sum_{j\in[p(n)]}\cos(\frac{2j\pi}{p(n)})(t_1t_2)^j(e+(-1)^b g))| \\
\leq&\frac{1}{p(n)}\sum_{j\in[p(n)]}\Big[|\widetilde{\mathrm{Tr}}(\rho((t_1t_2)^j)) - f_{n,\hat{\boldsymbol{z}}}((t_1t_2)^j)| + |\widetilde{\mathrm{Tr}}(\rho((t_1t_2)^j g)) - f_{n,\hat{\boldsymbol{z}}}((t_1t_2)^j g)|\Big] \\
\leq&\frac{1}{p(n)}2(\epsilon+\zeta)\cdot p(n) \\
\leq&2(\epsilon+\zeta),
\end{aligned}
$$

where we use $|\cos(\frac{2j\pi}{p(n)}|) \leq 1$. Recall eq. (7.4), and we know

$$
\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(\sigma(g_m,2)\sigma(g,b)^-)) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g_m,2)\sigma(g,b)^-)| \\
=&|\widetilde{\mathrm{Tr}}((\rho(e) - \rho(\sigma(g_m,0)) - \rho(\sigma(g_m,1)))\rho(\sigma(g,b)^-)) \\
&\qquad - f_{n,\hat{\boldsymbol{z}}}((e - \sigma(g_m,0) - \sigma(g_m,1))\sigma(g,b)^-)| \\
\leq&|\widetilde{\mathrm{Tr}}(\rho(\sigma(g,b)^-)) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g,b)^-)| \\
&\quad + |\widetilde{\mathrm{Tr}}(\rho(\rho(\sigma(g_m,0))\rho(\sigma(g,b)^-) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g_m,0)\sigma(g,b)^-)| \\
&\qquad + |\widetilde{\mathrm{Tr}}(\rho(\rho(\sigma(g_m,1))\rho(\sigma(g,b)^-) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g_m,1)\sigma(g,b)^-)| \\
\leq&\frac{1}{2}(\epsilon+\zeta) + (\epsilon+\zeta) + 2(\epsilon+\zeta) \\
\leq&4(\epsilon+\zeta).
\end{aligned}
$$

Recall eq. (7.5), and we know

$$
\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(\sigma(g_{m+1},0)\sigma(g,b)^-)) - f_{n,\hat{\boldsymbol{z}}}(\sigma(g_{m+1},0)\sigma(g,b)^-)| \\
\leq&\frac{1}{2p(n)}\sum_{j\in[p(n)]}\Big[|\cos(\frac{2j\pi}{p(n)})||\widetilde{\mathrm{Tr}}(\rho((t_1t_2)^j)) - f_{n,\hat{\boldsymbol{z}}}((t_1t_2)^j)| \\
&\qquad + |\cos(\frac{2j\pi}{p(n)})||\widetilde{\mathrm{Tr}}(\rho((t_1t_2)^j g)) - f_{n,\hat{\boldsymbol{z}}}((t_1t_2)^j g)| \\
&\qquad\quad + |\cos(\frac{(2j+1)\pi}{p(n)})||\rho(t_2(t_1t_2)^j) - f_{n,\hat{\boldsymbol{z}}}(t_2(t_1t_2)^j)| \\
&\qquad\qquad + |\cos(\frac{(2j+1)\pi}{p(n)})||\rho(t_2(t_1t_2)^j g) - f_{n,\hat{\boldsymbol{z}}}(t_2(t_1t_2)^j g)|\Big] \\
\leq&\frac{1}{2p(n)}p(n)\cdot 4(\epsilon+\zeta) \\
\leq&2(\epsilon+\zeta).
\end{aligned}
$$

With similar reasoning we can get that

$$|\widetilde{\mathrm{Tr}}(\rho(\sigma(g_{m+1},1)\sigma(g,b)^{-})) - f_{n,\hat{\mathbf{z}}}(\sigma(g_{m+1},1)\sigma(g,b)^{-})| \leq 2(\epsilon+\zeta),$$
$$|\widetilde{\mathrm{Tr}}(\rho(\sigma(g_{m+2},0)\sigma(g,b)^{-})) - f_{n,\hat{\mathbf{z}}}(\sigma(g_{m+2},0)\sigma(g,b)^{-})| \leq 2(\epsilon+\zeta),$$
$$|\widetilde{\mathrm{Tr}}(\rho(\sigma(g_{m+2},1)\sigma(g,b)^{-})) - f_{n,\hat{\mathbf{z}}}(\sigma(g_{m+2},1)\sigma(g,b)^{-})| \leq 2(\epsilon+\zeta),$$

Lastly, recall eqs. (7.7) and (7.10), and we know

$$\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(\sigma(g_{m+1},2)\sigma(g,b)^{-})) - f_{n,\hat{\mathbf{z}}}(\sigma(g_{m+1},2)\sigma(g,b)^{-})|\\
=&|\widetilde{\mathrm{Tr}}(\rho(\sigma(g_{m+2},2)\sigma(g,b)^{-})) - f_{n,\hat{\mathbf{z}}}(\sigma(g_{m+2},2)\sigma(g,b)^{-})|\\
\leq&|\widetilde{\mathrm{Tr}}(\rho(\sigma(g,b)^{-})) - f_{n,\hat{\mathbf{z}}}(\sigma(g,b)^{-})|\\
&+|\widetilde{\mathrm{Tr}}(\rho(\rho(\sigma(g_m,1))\rho(\sigma(g,b)^{-})) - f_{n,\hat{\mathbf{z}}}(\sigma(g_m,1)\sigma(g,b)^{-})|\\
\leq&\frac{1}{2}(\epsilon+\zeta)+2(\epsilon+\zeta)\\
\leq&3(\epsilon+\zeta).
\end{aligned}$$

Next, we prove eq. (7.22), and eq. (7.23) follows analogously. First of all, when $x, y = g_m$, $g \in O_\Gamma \cup \{e\}$ and $a = b = 0$,

$$\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,0)\sigma(g_m,0)^{-})) - f_{n,\hat{\mathbf{z}}}(\rho(g\sigma(g_m,0)\sigma(g_m,0)^{-}))|\\
\leq&\frac{1}{p(n)^2}\sum_{j,k\in[p(n)]}|\widetilde{\mathrm{Tr}}(\rho(g(t_1t_2)^{j-k})) - f_{n,\hat{\mathbf{z}}}(g(t_1t_2)^{j-k})|\\
\leq&\frac{1}{p(n)^2}p(n)^2\cdot(\epsilon+\zeta)\\
=&\epsilon+\zeta.
\end{aligned}$$

Next, when $x, y = g_m$, $g \in O_\Gamma \cup \{e\}$ and $a = 0, b = 1$,

$$\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m, 0)\sigma(g_m, 1)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m, 0)\sigma(g_m, 1)^-)| \\
\leq& \frac{2}{p(n)^2} \sum_{j,k\in[p(n)]} |\cos(\frac{2k\pi}{p(n)})||\widetilde{\mathrm{Tr}}(\rho(g(t_1t_2)^{j-k})) - f_{n,\hat{\mathbf{z}}}(g(t_1t_2)^{j-k})| \\
\leq& \frac{2}{p(n)^2} p(n)^2 \cdot (\epsilon + \zeta) \\
=& 2(\epsilon + \zeta).
\end{aligned}$$

With similar reasoning, we can get that

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m, 1)\sigma(g_m, 1)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m, 1)\sigma(g_m, 1)^-)| \leq 4(\epsilon + \zeta).$$

Next, when $x, y = g_m$, $g \in O_\Gamma \cup \{e\}$ and $a = 2, b = 0$,

$$\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m, 2)\sigma(g_m, 0)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m, 2)\sigma(g_m, 0)^-)| \\
\leq& |\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m, 0)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m, 0)^-)| \\
&\quad + |\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m, 0)\sigma(g_m, 0)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m, 0)\sigma(g_m, 0)^-)| \\
&\qquad + |\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m, 1)\sigma(g_m, 0)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m, 1)\sigma(g_m, 0)^-)| \\
\leq& 4(\epsilon + \zeta).
\end{aligned}$$

With similar reasoning, we can get that

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,2)\sigma(g_m,1)^-)) - f_{n,\hat{\boldsymbol{z}}}(g\sigma(g_m,2)\sigma(g_m,1)^-)| \leq 8(\epsilon+\zeta),$$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,2)\sigma(g_m,2)^-)) - f_{n,\hat{\boldsymbol{z}}}(g\sigma(g_m,2)\sigma(g_m,2)^-)| \leq 15(\epsilon+\zeta).$$

When $x = g_m$, $y = g_{m+1}$, $g \in O_\Gamma \cup \{e\}$ and $a = 0, b = 0$, we can get that

$$\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,0)\sigma(g_{m+1},0)^-)) - f_{n,\hat{\boldsymbol{z}}}(g\sigma(g_m,0)\sigma(g_{m+1},0)^-)| \\
\leq & \frac{1}{p(n)^2}\sum_{j,k\in[p(n)]}\Big[|\cos(\frac{2k\pi}{p(n)})||\widetilde{\mathrm{Tr}}(\rho(g(t_1t_2)^{j-k})) - f_{n,\hat{\boldsymbol{z}}}((t_1t_2)^{j-k})| \\
&\qquad + |\cos(\frac{(2k+1)\pi}{p(n)})||\widetilde{\mathrm{Tr}}(\rho(g(t_1t_2)^{j-k}t_2)) - f_{n,\hat{\boldsymbol{z}}}(g(t_1t_2)^{j-k}t_2)| \\
\leq & 2(\epsilon+\zeta).
\end{aligned}$$

With similar reasoning we can get that for $h = g_{m+1}, g_{m+2}$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,0)\sigma(h,1)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m,0)\sigma(h,1)^-)| \leq 2(\epsilon+\zeta),$$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,0)\sigma(h,2)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m,0)\sigma(h,2)^-)| \leq 3(\epsilon+\zeta),$$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,1)\sigma(h,0)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m,1)\sigma(h,0)^-)| \leq 4(\epsilon+\zeta),$$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,1)\sigma(h,1)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m,1)\sigma(h,1)^-)| \leq 4(\epsilon+\zeta),$$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,1)\sigma(h,2)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m,1)\sigma(h,2)^-)| \leq 6(\epsilon+\zeta),$$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,2)\sigma(h,0)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m,2)\sigma(h,0)^-)| \leq 8(\epsilon+\zeta),$$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,2)\sigma(h,1)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m,2)\sigma(h,1)^-)| \leq 8(\epsilon+\zeta),$$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_m,2)\sigma(h,2)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_m,2)\sigma(h,2)^-)| \leq 9(\epsilon+\zeta).$$

The last case is when $x, y = g_{m+1}, g_{m+2}$. We use $a = b = 0$ as an example.

$$\begin{aligned}
&|\widetilde{\mathrm{Tr}}(\rho(g\sigma(g_{m+1},0)\sigma(g_{m+1},0)^-)) - f_{n,\hat{\mathbf{z}}}(g\sigma(g_{m+1},0)\sigma(g_{m+1},0)^-)| \\
\leq &\frac{1}{p(n)^2} \sum_{j,k\in[p(n)]} |\cos(\frac{2j\pi}{p(n)})\cos(\frac{2k\pi}{p(n)})||\widetilde{\mathrm{Tr}}(\rho(g(t_1t_2)^{j-k})) - f_{n,\hat{\mathbf{z}}}(g(t_1t_2)^{j-k})| \\
&+ |\cos(\frac{2j\pi}{p(n)})\cos(\frac{(2k+1)\pi}{p(n)})||\widetilde{\mathrm{Tr}}(\rho(g(t_1t_2)^{j-k}t_2)) - f_{n,\hat{\mathbf{z}}}(g(t_1t_2)^{j-k}t_2)| \\
&+ |\cos(\frac{(2j+1)\pi}{p(n)})\cos(\frac{2k\pi}{p(n)})||\widetilde{\mathrm{Tr}}(\rho(gt_2(t_1t_2)^{j-k})) - f_{n,\hat{\mathbf{z}}}(gt_2(t_1t_2)^{j-k})| \\
&+ |\cos(\frac{(2j+1)\pi}{p(n)})\cos(\frac{(2k+1)\pi}{p(n)})||\widetilde{\mathrm{Tr}}(\rho(gt_2(t_1t_2)^{j-k}t_2)) - f_{n,\hat{\mathbf{z}}}(gt_2(t_1t_2)^{j-k}t_2)| \\
\leq &4(\epsilon+\zeta).
\end{aligned}$$

With similar reasoning, we can get that when $x, y = g_{m+1}, g_{m+2}$ and $a, b = 0, 1$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(x,a)\sigma(y,b)^{-})) - f_{n,\hat{\mathbf{z}}}(g\sigma(x,a)\sigma(y,b)^{-})| \leq 4(\epsilon + \zeta);$$

when one answer is 2 and the other answer is from $0, 1$,

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(x,2)\sigma(y,b)^{-})) - f_{n,\hat{\mathbf{z}}}(g\sigma(x,2)\sigma(y,b)^{-})| \leq 6(\epsilon + \zeta),$$

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(x,a)\sigma(y,2)^{-})) - f_{n,\hat{\mathbf{z}}}(g\sigma(x,a)\sigma(y,2)^{-})| \leq 6(\epsilon + \zeta);$$

and when both answers are 2

$$|\widetilde{\mathrm{Tr}}(\rho(g\sigma(x,2)\sigma(y,2)^{-})) - f_{n,\hat{\mathbf{z}}}(g\sigma(x,2)\sigma(y,2)^{-})| \leq 8(\epsilon + \zeta).$$

$\square$

Bibliography

[1] Uriel Feige and László Lovász. Two-prover one-round proof systems: Their power and their problems (extended abstract). In *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, STOC '92, pages 733–744, New York, NY, USA, 1992. Association for Computing Machinery.

[2] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[3] Roger Colback. *Quantum and relativistic protocols for secure multi-party computation*. PhD thesis, Trinity College, University of Cambridge, Cambridge, UK, 2006.

[4] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.*, pages 236–249, June 2004.

[5] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3):195–200, 1964.

[6] Andrea Coladangelo and Jalex Stark. An inherently infinite-dimensional quantum correlation. *Nature Communications*, 11(1):3335, 2020.

[7] William Slofstra. The set of quantum correlations is not closed. In *Forum of Mathematics, Pi*, volume 7. Cambridge University Press, 2019.

[8] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. $MIP^* = RE$. *arXiv preprint arXiv:2001.04383*, 2020.

[9] Tobias Fritz. Tsirelson's problem and kirchberg's conjecture. *Reviews in Mathematical Physics*, 24(05):1250012, 2012.

[10] Honghao Fu, Carl A Miller, and William Slofstra. The membership problem for constant-sized quantum correlations is undecidable. *arXiv preprint arXiv:2101.11087*, 2021.

[11] Matthew Coudron and William Slofstra. Complexity lower bounds for computing the approximately-commuting operator value of non-local games to high precision. *arXiv preprint arXiv:1905.11635*, 2019.

[12] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 503–509. IEEE, 1998.

[13] 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.

[14] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456, 2013.

[15] 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 *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 247–277. Springer, 2019.

[16] Honghao Fu and Carl A Miller. Local randomness: Examples and application. *Physical Review A*, 97(3):032324, 2018.

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

[18] Anand Natarajan and John Wright. $NEEXP$ is Contained in MIP^*. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 510–518. IEEE, 2019.

[19] 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(5):052111, 2015.

[20] 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*, pages 1003–1015. ACM, 2017.

[21] 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. IEEE, 2018.

[22] Tzyh Haur Yang and Miguel Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Physical Review A*, 87(5):050102, 2013.

[23] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. *communications*, 8:15485, 2017.

[24] Shubhayan Sarkar, Debashis Saha, Jędrzej Kaniewski, and Remigiusz Augusiak. Self-testing quantum systems of arbitrary local dimension with minimal number of measurements. *arXiv preprint arXiv:1909.12722*, 2019.

[25] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(27):3373–3376, 1990.

[26] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93(6):062121, 2016.

[27] M. Ram Murty. Artin's conjecture for primitive roots. *The Mathematical Intelligencer*, 10(4):59–67, 1988.

[28] Honghao Fu. Constant-sized correlations are sufficient to robustly self-test maximally entangled states with unbounded dimension. *arXiv preprint arXiv:1911.01494*, 2019.

[29] Joseph J Rotman. *An Introduction to the Theory of Groups*, volume 148. Springer Science & Business Media, 2012.

[30] Marvin Lee Minsky. *Computation: Finite and Infinite Machines*. Prentice-Hall Englewood Cliffs, 1967.

[31] Olga Kharlampovich, Alexei Myasnikov, and Mark Sapir. Algorithmically complex residually finite groups. *Bulletin of Mathematical Sciences*, 7(2):309–352, 2017.

[32] Jonathan Dimock. *Quantum Mechanics and Quantum Field Theory: A Mathematical Primer*. Cambridge University Press, 2011.

[33] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[34] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[35] Graham Higmann, Bernhard Neumann, and Hanna Neumann. Embedding theorems for groups. *Journal of the London Mathematical Society*, 1(4):247–254, 1949.

[36] Roger C Lyndon and Paul E Schupp. *Combinatorial Group Theory*. Springer, 2001.

[37] Valerio Capraro, Martino Lupini, and Vladimir Pestov. *Introduction to Sofic and Hyperlinear Groups and Connes' Embedding Conjecture*, volume 2136. Springer, 2015.

[38] Jędrzej Kaniewski. Self-testing of binary observables based on commutation. *Physical Review A*, 95(6):062323, 2017.

[39] J.M. Howie. *Fundamentals of Semigroup Theory*. LMS monographs. Clarendon Press, 1995.

[40] Gilbert Baumslag. Subgroups of finitely presented metabelian groups. *Journal of the Australian Mathematical Society*, 16(1):98–110, 1973.

[41] Vladimir N. Remeslennikov. Infinite solvable and finitely approximable groups. *Mathematical notes of the Academy of Sciences of the USSR*, 17(5):489–492, 1975.

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

[43] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017.

[44] Urmila Mahadev. Classical verification of quantum computations. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 259–267, 2018.

[45] Tony Metger and Thomas Vidick. Self-testing of a single quantum device under computational assumptions. *arXiv preprint arXiv:2001.09161*, 2020.

[46] Laura Mančinska, Jitendra Prakash, and Christopher Schafhauser. Constant-sized robust self-tests for states and measurements of unbounded dimension. *arXiv preprint arXiv:2103.01729*, 2021.

[47] Hamoon Mousavi, Seyed Sajjad Nezhadi, and Henry Yuen. On the Complexity of Zero Gap MIP^*. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli, editors, *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 87:1–87:12, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.