The membership problem for constant-sized quantum correlations is undecidable

Honghao Fu[1], Carl A. Miller[1,2], and William Slofstra[3]

[1] *Joint Institute for Quantum Information and Computer Science, University of Maryland, College Park, MD, 20740, USA*

[2] *National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899, USA*

[3] *Institute for Quantum Computing and Department of Pure Mathematics, University of Waterloo, Waterloo, Canada*

January 19, 2021

Abstract

When two spatially separated parties make measurements on an unknown entangled quantum state, what correlations can they achieve? How difficult is it to determine whether a given correlation is a quantum correlation? These questions are central to problems in quantum communication and computation. Previous work has shown that the general membership problem for quantum correlations is computationally undecidable. In the current work we show something stronger: there is a family of constant-sized correlations — that is, correlations for which the number of measurements and number of measurement outcomes are fixed — such that solving the quantum membership problem for this family is computationally impossible. Intuitively, our result means that the undecidability that arises in understanding Bell experiments is innate, and is not dependent on varying the number of measurements in the experiment. This places strong constraints on the types of descriptions that can be given for quantum correlation sets. Our proof is based on a combination of techniques from quantum self-testing and from undecidability results of the third author for linear system nonlocal games.

Contents

1 Introduction

Suppose two spatially separated parties, say Alice and Bob, are each able to perform different measurements on their local system. If Alice can perform n_A different measurements, each with m_A outcomes, and Bob can perform n_B different measurements, each with m_B outcomes, then from the point of view of an outside observer, their 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 measures outcome a and Bob measures outcome b, given that Alice performs measurement x and Bob performs measurement y. The collection P is called a *correlation (matrix)* or *behaviour* [Tsi93].

It is natural to ask which correlations can occur in nature. Suppose measurement x on Alice's system always gives outcome c_x, and measurement y on Bob's system always gives outcome d_y. Then the corresponding correlation is $P(a,b|x,y) = \delta_{a,c_x}\delta_{b,d_y}$, where δ is the Kronecker delta. Correlations of this form are called *deterministic correlations*. The convex hull of the set of deterministic correlations is denoted by $C_c(n_A, n_B, m_A, m_B)$, or C_c when the tuple (n_A, n_B, m_A, m_B) is clear. Correlations in C_c are called *classical correlations*. All deterministic correlations obviously occur in nature, and if Alice and Bob have access to shared randomness, they can also achieve all correlations in C_c. It is a fundamental fact of quantum mechanics, first observed theoretically by John Bell and now verified in many experiments, that Alice and Bob can achieve correlations outside of C_c by using quantum entanglement [Bel64].

Bell's theorem leads to the question of which correlations can be achieved in quantum mechanics. To study this question, Tsirelson introduced the set of quantum correlations [Tsi93]. There are actually several ways to define the set of quantum correlations, depending on whether we assume that all Hilbert spaces are finite-dimensional, and whether we use the tensor-product axiom or commuting-operator axiom for joint systems. This leads to four different choices for the set of quantum correlations: the finite-dimensional quantum correlations C_q, the quantum-spatial correlations C_{qs}, the quantum-approximate correlations C_{qa}, and the commuting-operator correlatons C_{qc}. We use the same convention as for classical correlations, in that C_t refers to $C_t(n_A, n_B, m_A, m_B)$ when the tuple (n_A, n_B, m_A, m_B) is clear. Tsirelson suggested that all four sets should be equal, but we now know that (for some n_A, n_B, m_A, m_B) all four sets are different, and hence give a strictly increasing sequence

$$C_c \subsetneq C_q \subsetneq C_{qs} \subsetneq C_{qa} \subsetneq C_{qc}$$

[Slo19, CS18, JNV+20]. The last inequality $C_{qa} \subsetneq C_{qc}$ is a very exciting consequence of the recent proof [JNV+20] that $\mathsf{MIP}^* = \mathsf{RE}$ by Ji, Natarajan, Vidick, Wright, and Yuen, and following [Fri12, JNP+11], this inequality gives a negative resolution to the Connes embedding problem.

As the convex hull of a finite set, C_c is a polytope in $\mathbb{R}^N$, where $N = n_A n_B m_A m_B$. The sets C_t, $t \in \{q, qs, qa, qc\}$, are also convex subsets of $\mathbb{R}^N$ (in addition, C_{qa} and C_{qc} are closed), but it follows from a result of Tsirelson [Tsi87] that these sets are not polytopes. Following up in [Tsi93], Tsirelson asks whether the sets of quantum correlations might still have nice geometric descriptions, specifically by analytic or even polynomial inequalities. This question is significant for two reasons:

(1) (Practical) The quantum correlation set captures what is possible with quantum entanglement, and thus a description of this set tells us what is theoretically achievable in experiments and quantum technologies.

(2) (Conceptual) A nice description of the set of quantum correlations could improve our conceptual understanding of quantum entanglement, similarly to how the description of C_c as the convex hull of deterministic correlations is central to our understanding of classical correlations.

Due to the significance of this question, describing the set of quantum correlations has been a central question in the field. On the geometric side, Tsirelson's original results show that when $m_A = m_B = 2$, a certain linear slice of the quantum correlation set is the elliptope, a convex set described by quadratic inequalities ([Tsi87], see also [Lan88, WW01, Mas03, Pit08] for subsequent work on the special case that $n_A = n_B = 2$, and [TVC19] for a description as the elliptope). The convex geometry of $C_q(2,2,2,2)$ is studied in detail in [GKW$^+$18]. The geometry of $C_q(2,2,2,2)$ is in general fairly tractable: Jordan's lemma[1] implies that any correlation in $C_q(2,2,2,2)$ can be achieved via measurements on an entangled pair of qubits, and thus $C_q(2,2,2,2)$ can be described by polynomial functions on a finite number of parameters. However, no similar dimension reduction argument is known when the number of measurements or number of measurement outcomes is greater than 2. A result of Russell describes another linear slice, the synchronous correlations, in $C_q(3,3,2,2)$, but again this description does not extend to other numbers of measurements and outcomes [Rus20].

In another line, a number of authors have considered whether it's possible to give a conceptual, rather than geometric, description of the quantum correlation sets. The first result in this line comes from Tsirelson's original definition of quantum correlations, where he observes that quantum correlations belong to the set of nonsignalling correlations, which are those correlations P for which the sums

$$\sum_b P(a,b|x,y) \text{ and } \sum_a P(a,b|x,y)$$

are independent of y and x respectively. This condition captures the fact that, when spatially separated, Alice and Bob cannot communicate with each other. Since the set of nonsignalling correlations is strictly larger than the commuting-operator correlations C_{qc}, the fact that Alice and Bob cannot communicate does not identify the set of quantum correlations among all correlations. But it is natural to ask whether there might not be additional principles which would suffice to identify the set of correlations. Some examples of conditions which further restrict the set of nonsignalling correlations and which are satisfied by quantum correlations can be found in [BBL$^+$06, PPK$^+$09, NW09, FSA$^+$13, SGAN18], but so far these do not give a complete description of the set of quantum correlations.

Based on the apparent difficulty of describing the set of quantum correlations, there has also been a line of work studying the computational complexity of problems related to these sets. The main line of inquiry has been to consider the difficulty of determining the quantum and commuting-operator values of a nonlocal game [CHTW04]. For example, one can consider the problem of determining whether a given nonlocal game has a perfect strategy.

Problem (PerfectStrategy$_t$)**.** *Given a tuple of natural numbers (n_A, n_B, m_A, m_B) and a nonlocal game G with n_A and n_B questions and m_A and m_B answers, does G have a perfect strategy in C_t?*

From the point of view of convex geometry, the quantum (resp. commuting-operator) value of a nonlocal game is the maximum a certain linear functional takes on the set C_{qa} (resp. C_{qc}). (Asking whether such a nonlocal game has a perfect strategy corresponds to asking whether this maximum is equal to 1.) Prior to the year 2020, there was a series

[1] See, e.g., Lemma 3.1 in the supplementary information of [MS12].

of deep works showing that even the approximate version of this optimization problem is indeed very difficult [IV12, RUV13, Ji17, NV18, NV17, FJVY19, NW19]. These results have implications in computational complexity theory, as they imply lower bounds on the complexity class MIP* of multiprover proofs with entangled provers. In the exact (rather than approximate) case, previous results by the third author of the current paper imply that $(\text{PerfectStrategy}_t)$ are undecidable for $t \in \{q, qs, qa, qc\}$ [Slo19, Slo20]. The decision problem for the approximate case is known as the $\text{GappedPerfectStrategy}_t$ problem.

Problem $(\text{GappedPerfectStrategy}_t)$**.** *Given a tuple of natural numbers (n_A, n_B, m_A, m_B) and a nonlocal game G with n_A and n_B questions and m_A and m_B answers, decide whether G has a perfect strategy in C_t, or the quantum value of G is $\leq 1/2$, given that one of the two is the case.*

As mentioned above, recently Ji, Natarajan, Vidick, Wright, and Yuen have shown that $\text{GappedPerfectStrategy}_t$ is also undecidable for $t \in \{q, qs, qa\}$ [JNV+20].

Rather than looking at nonlocal games, a more straightforward way to study the difficulty of describing quantum correlation sets is to look at the membership problem for these sets. Specifically, we can look at the decision problems for $t \in \{q, qs, qa, qc\}$ and subfields $\mathbb{K} \subseteq \mathbb{R}$.

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

The point of restricting to correlations in $\mathbb{K}^{n_A n_B m_A m_B}$ rather than $\mathbb{R}^{n_A n_B m_A m_B}$ is that it is not possible to describe all real numbers in a finite fashion. We are primarily interested in fields, such as $\mathbb{Q}$, where it is practical to work with elements of the field on a computer. For our results we actually need to take a larger field than $\mathbb{Q}$, so in what follows we'll set $\mathbb{K} = \overline{\mathbb{Q}} \cap \mathbb{R}$ unless otherwise noted, where $\overline{\mathbb{Q}}$ is the algebraic closure of the rationals.[2]

The questions $(\text{Membership}_{t,\mathbb{K}})$ are a very general way of studying descriptions of the sets C_t for $t \in \{q, qs, qa, qc\}$, since we don't restrict to any particular form of description, but instead just look at a basic functionality that we would hope to have from any nice description, namely a way of being able to distinguish elements inside the set from those outside. The decision problems $(\text{Membership}_{t,\mathbb{K}})$ are not equivalent to the problems $(\text{PerfectStrategy}_t)$ or $(\text{GappedPerfectStrategy}_t)$, since nonlocal games do not necessarily have unique perfect strategies in C_t. Nonetheless, the two families of decision problems are closely related. Indeed, Coudron and the last author show that the methods used in [Slo20] to show the undecidability of $(\text{PerfectStrategy}_{qc})$ also imply the undecidability of $(\text{Membership}_{qc,\mathbb{K}})$ [CS19]. The methods of [Slo19] can be adapted to show the undecidability of $(\text{Membership}_{t,\mathbb{K}})$ for $t \in \{q, qs, qa\}$ in similar fashion (although some work is needed for the case $t = q$). The undecidability of $(\text{GappedPerfectStrategy}_t)$ can be used (in a blackbox fashion, so without referring to the proof methods) to get the stronger result that $(\text{Membership}_{t,\mathbb{Q}})$ is undecidable for $t \in \{q, qs, qa\}$ [JNV+20].

Taken together, the above undecidability results put very strong restrictions on what descriptions of the quantum correlation sets are possible. For instance, they imply that

[2] Since $\overline{\mathbb{Q}}$ is computable, it is possible to work with $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}} \cap \mathbb{R}$ on a computer, and indeed support for this is included in Mathematica and other computer algebra packages.

there is no Turing machine which takes tuples (n_A, n_B, m_A, m_B) as inputs, and outputs a description of $C_t(n_A, n_B, m_A, m_B)$ in terms of a finite list of polynomial inequalities, since such a Turing machine would allow us to decide $(\text{Membership}_{t,\mathbb{K}})$. Similarly, these results also imply that there can be no finite set of principles, independent of (n_A, n_B, m_A, m_B), such that we can decide whether a correlation satisfies every principle, and such that a correlation satisfies all the principles if and only if it belongs to $C_t(n_A, n_B, m_A, m_B)$.

However, we note that the reasoning in the last two paragraphs depends crucially on the fact that the parameters (n_A, n_B, m_A, m_B) can vary. (The papers [Slo20, Slo19, JNV+20] all involve games with unbounded alphabet size.) What happens to the complexity of $(\text{Membership}_{t,\mathbb{K}})$ when (n_A, n_B, m_A, m_B) are held constant? The above results leave open the possibility that every set $C_t(n_A, n_B, m_A, m_B)$ has a nice description, but that it is just not possible to have a Turing machine which outputs these descriptions as a function of (n_A, n_B, m_A, m_B).

Proving the undecidability of a constant-sized version of $(\text{Membership}_{t,\mathbb{K}})$ would allow us to understand the true sources of complexity in the study of quantum correlations: it would show that the undecidability is not only a consequence of varying the size of the correlation, but is in fact embedded into the shape of a single set $C_t(n_A, n_B, m_A, m_B)$ for some (n_A, n_B, m_A, m_B). In particular, this would rule out any kind of computable description (e.g., by polynomial inequalities) for the shape of that set.

Our main result addresses the constant-sized membership problem for 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 $P \in C_t(n_A, n_B, m_A, m_B)$?*

We show the following.

Theorem 1.1. *(Informal version) There is an integer α_0 such that the decision problem $(\text{Membership}(n_A, n_B, m_A, m_B)_{t,\mathbb{K}})$ is undecidable for $t \in \{qa, qc\}$ and $n_A, n_B, m_A, m_B > \alpha_0$.*

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 us to decide membership in that set.

As mentioned above, in this theorem $\mathbb{K}$ is the intersection $\overline{\mathbb{Q}} \cap \mathbb{R}$. However, the proof of this theorem does not rely on writing down very complicated elements of $\overline{\mathbb{Q}}$. In fact, $\mathbb{K}$ could be replaced with $\mathbb{K}_0 \cap \mathbb{R}$, where $\mathbb{K}_0$ is the subfield of $\overline{\mathbb{Q}}$ generated by roots of unity. In this way, the theorem is similar to the undecidability results for $(\text{Membership}_{t,\mathbb{K}})$ that follow from [Slo19, Slo20, CS19]. However, in those results, if the correlations are defined in terms of observables instead of measurements, then it is possible to take $\mathbb{K} = \mathbb{Q}$. In our case, even if we work with correlations defined in terms of observables, we still need to use roots of unity. We also note that, in the proof of Theorem 1.1, we can actually restrict to synchronous correlations. The formal versions of Theorem 1.1 are given in Corollaries 6.13 and 7.12.

To prove Theorem 1.1, we combine techniques from [Slo19, Slo20] with self-testing methods from [Fu19]. Specifically, [Fu19] shows that it is possible to self-test a maximally entangled state of arbitrary dimension, using constant-sized correlations. This is done by self-testing a relation $T^p = 1$ for a certain word T in the observables used in the correlation, and a chosen prime integer p. The methods used in [Slo19, Slo20] are group-theoretic, and involve reducing from nonlocal games to the word problem for groups. We show that there is a group $G/\langle t^{p(n)} = e\rangle$, where $p(n)$ is the n-th prime of some fixed primitive root, such that deciding if a fixed known element of this group is trivial is equivalent to deciding if a Turing machine halts on input n. Then, intuitively, the corresponding correlation C_n has two parts: the first parts certifies the relations of the group G using techniques from [Slo19, Slo20]; and the second part certifies the relation $t^{p(n)} = e$ using techniques from [Fu19]. The aforementioned techniques ensure that the size of C_n is fixed and independent of n. In the end, we manage to show that deciding if C_n is quantum is equivalent to deciding if n is not a halting input of the Turing machine.

It is interesting to also consider upper bounds on the complexity of the problem $(\text{Membership}(n_A, n_B, m_A, m_B)_{t,\mathbb{K}})$. When $t = qc$, this problem is contained in coRE, and Theorem 1.1 actually shows that this problem is coRE-complete (for large enough n_A, n_B, m_A, m_B). When $t = q$ or $t = qs$, this problem is contained in RE, but when $t = qa$, the best known upper bound on this decision problem is Π_2^0. In this case, Theorem 1.1 only shows that $(\text{Membership}(n_A, n_B, m_A, m_B)_{qa,\mathbb{K}})$ is coRE-hard, so this lower bound is not necessarily tight. Recently, Mousavi, Nezhadi, and Yuen have shown that the three-player version of $(\text{PerfectStrategy}_{qa})$ is Π_2^0-complete [MNY20], and it seems reasonable to conjecture that $(\text{Membership}(n_A, n_B, m_A, m_B)_{qa,\mathbb{K}})$ is also Π_2^0-complete for large enough n_A, n_B, m_A, m_B. We leave this as an open problem.

1.1 Acknowledgements

The authors thank Henry Yuen for helpful conversations about the topics of this paper. CAM thanks Johannes Bausch for a conversation about [BCLPG20] which helped to inspire this project. This paper is partly a contribution of the U. S. National Institute of Standards and Technology, and is not subject to copyright in the United States.

2 Notation and group theory background

We denote the set $\{0, 1, \ldots n-1\}$ by $[n]$. The n-th root of unity is denoted by $\omega_n := e^{i2\pi/n}$. For a Hilbert space $\mathcal{H}$, we denote by $\mathcal{L}(\mathcal{H})$ the set of all linear operators acting on $\mathcal{H}$ and by $\mathcal{U}(\mathcal{H})$ the set of all unitaries acting on $\mathcal{H}$ and the unitary group acting on $\mathcal{H}$.

Next, we introduce some basic notions of group theory, on which the undecidability results heavily rely. For more contexts, please refer to [Rot12].

For a group G, we denote the trivial element of G by e. 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 conjugate of g by h by $h^{-1}gh$. Following the convention of [KMS17], we may also write $h^{-1}gh$ as g^h.

Let S be a set of letters. We denote by $\mathcal{F}(S)$ the *free group generated by S*, which consists of all finite words made from $\{s, s^{-1} | s \in S\}$ such that neither ss^{-1} nor $s^{-1}s$ appears as a substring of a word for any s. The group law is given by concatenation and cancellation. For a more formal treatment, we refer to [Rot12, Pages 343 - 345].

Definition 2.1 (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 $\langle S : R\rangle$ denotes the quotient of $\mathcal{F}(S)$ by the normal subgroup generated by R in $\mathcal{F}(S)$. If the group G is isomorphic to $\langle S : R\rangle$, then we say G has a presentation $\langle S : R\rangle$.*

If a group G is defined by $\langle S : R\rangle$, we write $G = \langle S : R\rangle$. If both sets S and R are finite, then we say the group $G = \langle S : R\rangle$ is *finitely-presented*. The elements of S are the *generators* and the elements of R are the *relations*. A relation $r \in R$ is written as $r = e$ to convey its significance in the quotient group G.

The *free product* of a group G with a group H is denoted by $G * H$. By [Rot12, Theorem 11.53], if the presentation of G is $\langle S_G : R_G\rangle$ and the presentation of H is $\langle S_H : R_H\rangle$, then

$$G * H \cong \langle S_G \cup S_H : R_G \cup R_H\rangle.$$

For simplicity, when the presentation of G is clear from the context, we also write $G * H$ as $\langle G, S_H : R_H\rangle$.

A more general notion of the free product of groups is *the free product of groups with amalgamation*. Let G_1 and G_2 be two groups with subgroups H_1 and H_2 respectively such that there exists an injective homomorphism $\phi : H_1 \to H_2$. Then the free product of G_1 and G_2 with amalgamation is defined by

$$G_1 *_\phi G_2 := \frac{G_1 * G_2}{\langle h_1 = \phi(h_1) \mid \text{for all } h_1 \in H_1\rangle}.$$

Another way to construct new groups from a given group is by Higman-Neumann-Neumann extension (*HNN-extension*) [HNN49]. Let H be a subgroup of G and let $\phi : H \to H$ be an injective homomorphism, then the HNN-extension of G is

$$\overline{G} = \frac{G * \mathcal{F}(\{t\})}{\langle t^{-1}ht = \phi(h) \mid \text{for all } h \in H\rangle}.$$

We also write the HNN-extension of G by $\langle G, t : t^{-1}ht = \phi(h) \mid \text{for all } h \in H\rangle$. By [Rot12, Theorem 11.70], the natural homomorphism induced by the identification of each $g \in G$ in $\overline{G}$ is injective so G is embedded in $\overline{G}$. We shall introduce other important properties of the free product with amalgamation and the HNN-extension later when they are needed.

A *unitary representation* ρ of a group G on the Hilbert space $\mathcal{H}$ is a homomorphism $\rho : G \to \mathcal{U}(\mathcal{H})$. Consider an orthonormal set $\{|g\rangle : g \in G\}$. The *regular representation* of G is defined on the Hilbert space $\text{span}(\{|g\rangle : g \in G\})$, denoted by $\ell^2 G$. The *left regular representation* $L : G \to \mathcal{U}(\ell^2 G)$ maps g to $L(g)$ such that $L(g)|h\rangle = |gh\rangle$ for all $g, h \in G$. The *right regular representation* $R : G \to \mathcal{U}(\ell^2 G)$ maps g to $R(g)$ such that $R(g)|h\rangle = |hg^{-1}\rangle$ for all $g, h \in G$. It is immediate to see that

$$L_g R_{g'}|h\rangle = |ghg'^{-1}\rangle = R_{g'} L_g|h\rangle$$

for all $g, g', h \in G$. That is, $L(g)$ commutes with $R(g')$ for all $g, g' \in G$.

Definition 2.2. *Let n be a positive integer. The **Dihedral group** D_n is*

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

The elements of D_n are $(t_1t_2)^j$ and $t_2(t_1t_2)^j$ for $j \in [n]$. The left and right regular representation of D_n are defined on $L^2 D_n$.

Definition 2.3 (Definition 17 of [Slo19]). *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*

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

A different presentation of $\Gamma(A)$ is given in the proposition below.

Proposition 2.4. *Let $A\boldsymbol{x} = 0$ be an $m \times n$ linear system over $\mathbb{Z}_2$. For $j \in [m]$, define*

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

and a set

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

Define

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

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

The isomorphism between $\Gamma(A)$ and $\Gamma'(A)$ can be chosen to be $\phi : x_k \mapsto g_{i,k}$ for some i such that $k \in I_i$. The rest of the proof is routine, so we omit it.

Definition 2.5 (Definition 31 of [Slo19]). *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 2.6 (Definition 32 of [Slo19]). *Let A be an $m \times n$ 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. Let*

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

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

In the end of the section, we introduce solvable groups and sofic groups. 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 $1 \leq j \leq k$. A more general notion is *soficity*. A group G is *sofic* if, intuitively, any finite subset F of $G \setminus \{e\}$ can be well-approximated by a permutation group S_n for some n. For the formal definition of soficity, we refer to [CLP15, Chapter II.1].

For our proof, we use the following properties of solvable groups and sofic group introduced in [CLP15, Chapter II.3 and II.4].

1. Solvable groups are sofic;
2. 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 ([CLP15, Proposition II.4.1]); and
3. 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 ([CLP15, Propositiin II.4.1]).

3 Quantum correlation

The central object of our study is quantum correlation. We introduce it formally in this section.

3.1 Sets of quantum correlations

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

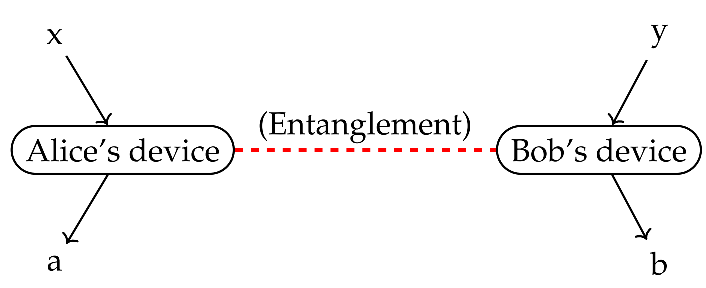


Figure 1: A nonlocal test between Alice and Bob

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 3.1. *A **bipartite correlation** of a nonlocal scenario* $([n_A],[n_B],[m_A],[m_B])$ *is a function* $P:[n_A]\times[n_B]\times[m_A]\times[m_B]\to\mathbb{R}_{\geq 0}:(i,j,k,l)\mapsto P(k,l|i,j)$ *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

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 $P(k,l|i,j)$. Therefore, the *size of a correlation* P of the nonlocal scenario $([n_A],[n_B],[m_A],[m_B])$ is the size of its correlation matrix, which equals $n_An_Bm_Am_B$.

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

Definition 3.2. *For a Hilbert space* $\mathcal{H}$*, a set of self-adjoint matrices in* $\mathcal{L}(\mathcal{H})$*,* $\{P_j \mid j\in[n]\}$*, is a **projective measurement** if* $P_i^2=P_i$ *for all* $i\in[n]$*,* $P_iP_j=0$ *for all* $i\neq j$*, and* $\sum_{j\in[n]}P_j=\mathbb{1}_{\mathcal{H}}$*.*

Definition 3.3. *A **quantum spatial strategy with projective measurements** for a nonlocal scenario* $T=([n_A],[n_B],[m_A],[m_B])$ *is a tuple*

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

where $\mathcal{H}_A$ *and* $\mathcal{H}_B$ *are Hilbert spaces,* $\{\{P_i^{(k)}\mid k\in[m_A]\}\mid i\in[n_A]\}$ *and* $\{\{Q_j^{(l)}\mid l\in[m_B]\}\mid j\in[n_B]\}$ *are two sets of projective measurements on* $\mathcal{H}_A$ *and* $\mathcal{H}_B$ *respectively.*

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, which is the reason why we say the strategy is spatial as in Fig. 1. 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 has conditional probabilities

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

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

Definition 3.4. *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 3.5. *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 3.6. *The set $C_{qa}(n_A, n_B, m_A, m_B)$ is the closure of $C_q(n_A, n_B, m_A, m_B)$ in $\mathbb{R}^{n_A n_B m_A m_B}$.*

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 3.7. *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*

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

where $\mathcal{H}$ is a Hilbert space, and $\{\{P_i^{(k)} \mid k \in [m_A]\} \mid i \in [n_A]\}$ and $\{\{Q_j^{(l)} \mid l \in [m_B]\} \mid j \in [n_B]\}$ are two sets of projective measurements on $\mathcal{H}$ such that $P_i^{(k)} Q_j^{(l)} = Q_j^{(l)} P_i^{(k)}$ 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. With quantum commuting-operator strategies we can define a larger set of quantum correlations.

Definition 3.8. *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 nonlocal scenario $([n_A], [n_B], [m_A], [m_B])$.*

It can be seen that $C_{qs}(n_A, n_B, m_A, m_B) \subseteq C_{qc}(n_A, n_B, m_A, m_B)$. Since $C_{qc}(n_A, n_B, m_A, m_A)$ is its own closure [Fri12, Proposition 3.4], we get that $C_{qa}(n_A, n_B, m_A, m_B) \subseteq C_{qc}(n_A,n_B,m_A,m_B)$.

Definition 3.9 (Synchronous correlation)**.** *A correlation P of a nonlocal scenario $([n_A], [n_B], [m_A], [m_B])$ is synchronous if $n_A = n_B = n$, $m_A = m_B = m$, and*

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

for all $i \in [n]$.

For $t \in \{q, qs, qa, qc\}$ and $n, m > 0$, we can identify a subset of $C_t(n, n, m, m)$, denoted by $C_t^s(n, m)$, which contains all the synchronous correlations in it.

3.2 A correlation associated with a 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.

Definition 3.10. *Let $A\boldsymbol{x} = 0$ be a binary linear system where each row has κ nonzero entries. For each $i \in [m]$, we define* [3]

$$I_i = \{j \in [n] \mid A(i,j) = 1\}$$
$$S_i = \{\boldsymbol{x} \in \mathbb{Z}_2^{I_i} \cong \mathbb{Z}_2^{\kappa} \mid \sum_{j \in I_i} \boldsymbol{x}(j) \equiv 0 \pmod 2\}.$$

A correlation $P : [m] \times [m] \times \mathbb{Z}_2^{\kappa} \times \mathbb{Z}_2^{\kappa}$ is a ***perfect correlation*** *associated with $A\boldsymbol{x} = 0$ if $P(\boldsymbol{x},\boldsymbol{y}|i,j) = 0$ when $\boldsymbol{x} \notin S_i$, or $\boldsymbol{y} \notin S_j$, or there exists $k \in I_i \cap I_j$ such that $\boldsymbol{x}(k) \neq \boldsymbol{y}(k)$.*

Next, we define the correlation induced by a representation of a solution group. For a binary linear system $A\boldsymbol{x} = 0$, let $\rho : \Gamma(A) \to \mathcal{U}(\mathbb{C}^d)$ be a unitary representation of $\Gamma(A)$. Define projectors

$$P_i^{(\boldsymbol{x})} = \prod_{j \in I_i} \left(\frac{\mathbb{1} + (-1)^{\boldsymbol{x}(j)} \rho(x_j)}{2} \right),$$
$$Q_i^{(\boldsymbol{x})} = \prod_{j \in I_i} \left(\frac{\mathbb{1} + (-1)^{\boldsymbol{x}(j)} \rho(x_j)}{2} \right)^{\intercal},$$

for each $i \in [m]$ and $\boldsymbol{x} \in S_i$. Since $\prod_{j \in I_i} \rho(x_j) = \mathbb{1}$, we know $\{P_i^{(\boldsymbol{x})} \mid \boldsymbol{x} \in S_i\}$ and $\{Q_i^{(\boldsymbol{x})} \mid \boldsymbol{x} \in S_i\}$ are projective measurements for each $i \in [m]$. Define

$$|\psi\rangle := \frac{1}{\sqrt{d}} \sum_{j \in [d]} |j\rangle |j\rangle.$$

Then the projective measurement strategy is

$$S_\rho = (|\psi\rangle, \{\{P_i^{(\boldsymbol{x})} \mid \boldsymbol{x} \in S_i\} \mid i \in [m]\}, \{\{Q_i^{(\boldsymbol{x})} \mid \boldsymbol{x} \in S_i\} \mid i \in [m]\}),$$

and the induced quantum correlation $\tilde{P} : [m] \times [m] \times \mathbb{Z}_2^{\kappa} \times \mathbb{Z}_2^{\kappa} \to \mathbb{Q}$ is defined by

$$\tilde{P}(\boldsymbol{x},\boldsymbol{y}|i,j) = \langle \psi | P_i^{(\boldsymbol{x})} \otimes Q_j^{(\boldsymbol{y})} | \psi \rangle$$

for $i, j \in [m]$ and $\boldsymbol{x} \in S_i, \boldsymbol{y} \in S_j$.

Proposition 3.11. *The correlation $\tilde{P}$ defined above is a perfect correlation associated with $A\boldsymbol{x} = 0$.*

Proof. By the definition of $\tilde{P}$, it is easy to see that $\tilde{P}(\boldsymbol{x},\boldsymbol{y}|i,j) = 0$ 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 $\tilde{P}(\boldsymbol{x},\boldsymbol{y}|i,j)$ has the term

$$\frac{\mathbb{1} + \rho(x_{k_0})}{2} \otimes \frac{\mathbb{1} - \rho(x_{k_0})^{\intercal}}{2} |\psi\rangle = \frac{(\mathbb{1} + \rho(x_{k_0}))(\mathbb{1} - \rho(x_{k_0}))}{4} \otimes \mathbb{1} |\psi\rangle = 0.$$

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 $\tilde{P}(\boldsymbol{x},\boldsymbol{y}|i,j) = 0$, which completes the proof. □

[3] 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..

Note that $\tilde{P}$ is also a perfect correlation of the binary linear system game associated with $A\boldsymbol{x} = 0$. For a detailed introduction of binary linear system games, we refer to [Slo19, Section 3].

4 Embedding procedures

In this section, we give an overview of the two embedding procedures: one for embedding general finitely-presentable groups into solution groups, first introduced in [Slo20], and one for embedding extended homogeneous linear-plus-conjugacy groups into solution groups, first introduced in [Slo19]. The two embedding procedures are key steps 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.

4.1 A general embedding procedure

This section is based on [CS19, Section 4].

Theorem 4.1 (Adapted from Theorem 4.1 of [CS19])**.** *Let $G = \langle S : R \rangle$ be a finitely-presented group. Then there is an $m \times n$ linear system $A\boldsymbol{x} = 0$ and a map: $\phi : \mathcal{F}(S) \to \mathcal{F}(\{x_j \mid j \in [n]\})$ such that*

1. *ϕ descends to an injection $G \to \Gamma(A)$;*
2. *Define $N = |S| + \sum_{r \in R} |r|$, then A has exactly three non-zero entries in every row, the dimensions m and n are of order $O(N)$, and A can be constructed from $\langle S : R \rangle$ in time of order $O(poly(N))$.*

Instead of repeating the full proof, we list the key steps, following the proof of [CS19, Theorem 4.1]. For each reduced word $w = s_0^{a_0} s_1^{a_1} \dots s_{k-1}^{a_{k-1}} \in \mathcal{F}(S)$, where $s_j \in S$ and $a_j \in \{1, -1\}$, we write $w^+ = s_0 s_1 \dots s_{k-1}$.

In the first step, define $S' = \{u_s, v_s \mid s \in S\}$, $\phi_1 : \mathcal{F}(S) \to \mathcal{F}(S')$ by $\phi_1(s) = u_s v_s u_s v_s$, and

$$G' = \langle S' : \{u_s^2 = v_s^2 = e \mid s \in S\} \cup R' \rangle,$$

where $R' = \{\phi_1(r)^+ \mid r \in R\}$. It can be checked that G is embedded in G'.

In the second step, we embed G' into G'' and get an embedding of G into G''. The construction of G'', known as the *wagon wheel construction*, takes several steps. For each $r \in R'$ such that r equals $s_0 s_1 \dots s_{l-1}$, we introduce auxiliary variables

$$\{a_{r,j}, b_{r,j}, c_{r,j}, d_{r,j} \mid j \in [l]\},$$

and equations

$$\begin{aligned}
&s_j + a_{r,j} + b_{r,j} = 0, \\
&a_{r,j} + b_{r,j-1} + c_{r,j-1} = 0, \\
&d_{r,j} + d_{r,j-1} + c_{r,j-1} = 0,
\end{aligned}$$

for each $j \in [l]$. Let $A\boldsymbol{x} = 0$ be the binary linear system of all the equations over all $r \in R'$. Then,

$$G'' = \Gamma(A),$$

Define $S'' = \cup_{r \in R'} \{a_{r,j}, b_{r,j}, c_{r,j}, d_{r,j} \mid j \in [|r|]\}$, then the set of generators of G'' is $S' \cup S''$. From the construction of G'' we can see that $\phi_2 : s \mapsto s$ for each $s \in S'$ descends to an injection into G''. Hence, $\phi_2 \circ \phi_1$ descends to an injection from G into G''.

Definition 4.2 (Oblivious solution group). *Let $A\boldsymbol{x} = 0$ be an $m \times n$ binary linear system, and let*

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

where $P = \{g_{i,k} g_{j,k} \mid k \in [n], k \in I_i \cap I_j\}$, be its solution group following Proposition 2.4. Define a set

$$G^* = \{e\} \cup \bigcup_{i \in [m]} \{g_{i,k} \mid k \in I_i\}.$$

Then $\Gamma'(A)$ is oblivious if

$$\langle P \rangle^{G_0 * \ldots * G_{m-1}} \cap [(G^*)^2 \setminus P] = \{e\}.$$

In other words, $\Gamma(A)'$ is oblivious if for any $g \neq h \in G^*$

$$gh = e \text{ in } \Gamma'(A) \iff gh \in P.$$

An important property of this embedding procedure is that the embedded solution group is *oblivious*.

Lemma 4.3 (Adapted from Lemma 4.2 of [CS19]). *Let $A\boldsymbol{x} = 0$ be the $m \times n$ binary linear system from the construction in the proof of Theorem 4.1. Then, the solution group $\Gamma'(A)$ is oblivious.*

The proof follows directly from the proof of [CS19, Lemma 4.2].

4.2 An fa^*-embedding procedure

Before we introduce the fa^*-embedding procedure, we introduce the approximate representations of a group, and certain embeddings of groups.

If $\mathcal{H}$ is finite-dimensional, we say a unitary representation of G, $\phi : G \to \mathcal{U}(\mathcal{H})$ 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 4.4 (Definition 10 of [Slo19]). *A homomorphism $\phi : G \to H$ is a* ***fin-embedding*** *if the induced map: $G^{fin} \to H^{fin}$ is injective, and a* ***fin*-embedding*** *if ϕ is injective and also a fin-embedding.*

Next, we define approximate representations of a group G.

Definition 4.5 (Definition 5 of [Slo19]). *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 $\|\phi(r) - \mathbb{1}\| \le \epsilon$ for all $r \in R$.*

An element $g \in G = \langle S : R \rangle$, whose representative is $w \in \mathcal{F}(S)$, is *nontrivial in approximate representations* of G if for all $\delta > 0$, there is an ϵ-approximate representation $\phi : \mathcal{F}(S) \to \mathcal{U}(\mathcal{H})$ such that $\|\phi(w) - \mathbb{1}\| \ge \delta$. 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 $\epsilon > 0$, there is an ϵ-approximate representation $\phi : \mathcal{F}(S) \to \mathcal{U}(\mathcal{H})$ such that $\phi(w) = \mathbb{1}$. The next proposition allows us to quantify the normalized trace of finitely many elements that are nontrivial in approximate representations.

Proposition 4.6. *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 $0 \le \tilde{\mathrm{Tr}}(\phi(w)) \le \zeta$ for each $w \in W$.*

This proposition is generalized from [Slo19, Lemma 12], which is about the trace of one element that is nontrivial in approximate representations. The proof of the proposition above is very similar to the proof of [Slo19, Lemma 12], where the only difference is to choose the parameter δ to be $\min_{w \in W} \|\phi(w) - \mathbb{1}\|$. The rest of the proof is similar, so we omit it here.

By the definition of the normalized Hilbert-Schmidt norm, the set of elements of G that are trivial in finite-dimensional approximate representations form a normal subgroup of G, denoted by N^{fa}. For a group G, we define

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

Definition 4.7 (Definition 14 of [Slo19]). *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, and a* ***fa*-embedding****, if ϕ 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 4.8 (Lemma 15 of [Slo19]). *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.*

In the last part of this section, we review the procedure to construct an fa^*-embedding of an extended homogeneous linear-plus-conjugacy group (Definition 2.6) into a solution group (Definition 2.3), and discuss its effect when it is applied to a type of groups, called *hyperlinear* groups. We refer to this procedure as the fa^*-embedding procedure. It has two steps. In the first step, an extended homogeneous linear-plus-conjugacy group is embedded into a homogeneous linear-plus-conjugacy group (Definition 2.5). Then, the homogeneous linear-plus-conjugacy group is embedded into a solution group in the second step. These two steps are summarized in the two propositions below.

Proposition 4.9 (Proposition 33 of [Slo19])**.** *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 4.10 (Proposition 27 and Lemma 29 of [Slo19])**.** *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.*

Intuitively, a group is *hyperlinear* if every finite set of its group elements can be well-approximated by the unitary group $\mathcal{U}(\mathcal{H})$ for some finite-dimensional Hilbert space $\mathcal{H}$. For the formal definition, we refer to [Slo19, Section 2.2].

Lemma 4.11 (Lemma 13 of [Slo19])**.** *A finitely-presented group G is* ***hyperlinear*** *if and only if every non-trivial element of G is nontrivial in approximate representations.*

Another important fact is that sofic groups are hyperlinear [CLP15, Chapter II.3].

Consequently, if the extended homogeneous-linear-plus-conjugacy group G is hyperlinear and it is embedded in $\Gamma = \langle S_\Gamma : R_\Gamma \rangle$, there exists a subset $S \subset S_\Gamma$ such that each $s \in S$ is nontrivial in approximate representations of Γ. Then, we can apply Proposition 4.6 to conclude that for any finite subset W of $\mathcal{F}(S)$ and for any $0 < \epsilon, \zeta < 1$, there is an ϵ-approximate representation of Γ such that $0 \leq \tilde{\mathrm{T}}\mathrm{r}(w) \leq \zeta$ for each $w \in W$ that is nontrivial in approximate representations of Γ. We apply this observation in the proof of Theorem 7.8.

5 Minsky machines and Kharlampovich-Myasnikov-Sapir groups

5.1 Minsky machines

A *k-glass Minsky Machine* [Min67], denoted by MM_k, consists of k glasses and an arbitrary amount of coins, where each glass can hold arbitrarily many coins. Intuitively, the two operations of each glass are adding a coin to the glass and removing a coin from a non-empty glass.

The states of MM_k are numbered from 0 to $N-1$ where 0 is the final accept state and 1 is the starting state, so a *configuration of* MM_k is in $[N] \times (\mathbb{Z}_{\geq 0})^{\times k}$ and of the form $(i; n_0, n_1, \ldots n_{k-1})$ 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 $j_0, j_1 \dots j_{l-1}$ where $l < k$, and go to state j. This command is encoded as

$$i; \to j; Add(j_0, j_1 \dots j_{l-1});$$

2. When the state is i, if the glasses numbered $j_0, j_1 \dots j_{l-1}$ where $l < k$ are all nonempty, then remove a coin from each of the glasses numbered $j_0, j_1 \dots j_{l-1}$, and go to state j. This command is encoded as

$$i; n_{j_0} > 0, \dots n_{j_{l-1}} > 0 \to j; Sub(j_0, j_1, \dots j_{l-1});$$

3. When the state is i, if the glasses numbered $j_0, j_1 \dots j_{l-1}$ where $l < k$ are empty, go to state j. This command is encoded as

$$i; n_{j_0} = 0, n_{j_1} = 0, \dots n_{j_{l-1}} = 0 \to j;$$

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

$$i; \to 0.$$

If at any give 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 following theorem. Recall that a subset S of natural numbers is *recursively enumerable* if there is an algorithm such that the algorithm halts on input s if and only if $s \in S$. The relation between Minsky machines and RE sets is summarized in the next Theorem.

Theorem 5.1. *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 $n \in X$.*

This theorem is based on the proof of the point (a) of [KMS17, Theorem 2.7], in which the authors show how to construct a 3-glass Minsky machine that can accept any integer of a recursively enumerable set. Therefore, we omit the proof here. This theorem implies that if $n \notin X$, MM_3 works indefinitely long when the input is n.

5.2 Kharlampovich-Myasnikov-Sapir groups

For a 3-glass Minsky machine, deterministic or non-deterministic, 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 $R(\mathsf{MM}_3)$. For the formal definitions of $S(\mathsf{MM}_3)$ and $R(\mathsf{MM}_3)$ we refer to [KMS17, Section 4.1]. Note that the parameter p in the definition of $G(\mathsf{MM}_3)$ in [KMS17, Section 4.1] is set to be 2 in this paper.

Intuitively, $G(\mathsf{MM}_3)$ can simulate MM_3 in the following sense. For each configuration of MM_3, there is a corresponding word in $\mathcal{F}(S(\mathsf{MM}_3))$. In particular, if we denote the word of the starting configuration of input n by $w(n)$ and the word of the accept configuration by $w(a)$, then $w(n) = w(a)$ in $G(\mathsf{MM}_3)$ if and only if the input n is accepted by MM_3.

The set $S(\mathsf{MM}_3)$ contains involutary generators $x(q_0A_0)$, $x(q_1A_0)$, $x(q_1A_0A_1A_2A_3)$, $x(q_0A_0A_1A_2A_3)$, A_1, A_2 and A_3, and non-involutary generators a_j, a'_j for $j = 1, 2, 3$. In particularly, $[x(t), x(s)] = e$ for any $t, s \in \{q_0A_0, q_1A_0, q_1A_0A_1A_2A_3, q_0A_0A_1A_2A_3\}$ ([KMS17, Relation $(G1)$]).

To formally define $w(a)$ and $w(n)$, we borrow more notations from [KMS17]. The authors of [KMS17] define an operation on the elements of $G(\mathsf{MM}_3)$ denoted by $\circledast$. For every $f \in G(\mathsf{MM}_3)$, they define

$$f \circledast a_j = f^{-1} f^{a_j} (f^{-1})^{a_j^{-1}} f^{a_j'^{-1}},$$

and

$$f \circledast A_j = [f, A_j]$$

for $j = 1, 2, 3$. To simplify the notation, they 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 $t_1 \circledast t_2^{\circledast n}$. Then, for the starting configuration of input n, the group element is

$$w(n) := x(q_1A_0) \circledast a_1^{\circledast n} \circledast A_1 \circledast A_2 \circledast A_3.$$

In particular, $w(0) := x(q_1A_0) \circledast A_1 \circledast A_2 \circledast A_3$. For the accept configuration, the group element is

$$w(a) := x(q_0A_0) \circledast A_1 \circledast A_2 \circledast A_3.$$

Note that by relation $(G5a)$ and $(G1)$ [KMS17, Page 334 - 335], we can conclude that $w(a) = x(q_0A_0A_1A_2A_3)$, $w(0) = x(q_1A_0A_1A_2A_3)$, and $w(a)^2 = w(0)^2 = [w(a), w(0)] = e$.

We adapt the following theorem from [KMS17, Properties 3.1 and 3.2 and Theorem 4.3].

Theorem 5.2. *Let X be a recursively enumerable set and MM_3 be the Minsky machine that accepts n if and only if $n \in X$. Then, the group $G(\mathsf{MM}_3)$ is solvable, and in $G(\mathsf{MM}_3)$, $w(n) = w(a)$ if and only if $n \in X$.*

Note that for any 3-glass Minsky Machine, MM_3, deterministic or non-deterministic, the group $G(\mathsf{MM}_3)$ is always solvable, as proved in [KMS17, Part (a) of Theorem 4.3]. About the presentation of $G(\mathsf{MM}_3)$, we adapt the following lemma from [Slo19, Lemma 42].

Lemma 5.3. *Let $G(\mathsf{MM}_3)$ be the group defined in Theorem 5.2. Then, $G(\mathsf{MM}_3)$ is an extended homogeneous linear-plus-conjugacy group. Furthermore, there is a presentation of $G(\mathsf{MM}_3)$ as an extended homogeneous linear-plus-conjugacy group in which the image of $w(0)w(a)$ is one of the involutary generators x_j.*

5.3 An extension of Kharlampovich-Myasnikov-Sapir group

This section is devoted to proving the following proposition.

Proposition 5.4. *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 $H = \langle S : R \rangle$, which has a generator t and an involutary generator x, such that $H/\langle t^{p(n)} = e \rangle$ is sofic, and

$$x = e \text{ in } H/\langle t^{p(n)} = e \rangle \iff n \in X. \tag{1}$$

The existence of r follows [Mur88]. By being an involutary generator, we mean that $x^2 = e$ in G.

To prove it, we first consider a 3-glass Minsky machine that can recognize a specific recursively enumerable set.

Definition 5.5. *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 $p(n)$. The set $P_{X,r}$ is defined by*

$$P_{X,r} := \{p(n) \mid n \in X\}.$$

Claim 5.6. *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 computable. We show $P_{X,r}$ is recursively enumerable by constructing a Turing machine TM that will accept $p(n)$ if $p(n) \in P_{X,r}$.

Let TM_X be the Turing machine that accepts n if and only if $n \in X$. By the definition of recursively enumerable, when $n \notin X$, TM_X may reject it or work indefinitely long. Given input q, TM first checks if $q \in P$. If q is not in P, it rejects q. If q is in P, TM also computes a positive integer n such that $q = p(n)$. Then TM runs $\mathsf{TM}_X(n)$. Hence, TM can accept each $p \in P_{X,r}$ in a finite amount of time. □

Define $\mathbf{MM}_3$ to be the 3-glass Minsky machine that can recognize $P_{X,r}$. Let $G(\mathbf{MM}_3) = \langle S_G : R_G \rangle$ be the KMS group of $\mathbf{MM}_3$. Then we show that the group G defined below is the group H required in Proposition 5.4,

$$G := \frac{G(\mathbf{MM}_3) * \mathcal{F}(\{t\})}{\langle [t, a_1] = [t, a_1'] = e, t^{-1}x(q_1A_0)t = x(q_1A_0) \circledast a_1 \rangle}. \tag{2}$$

Note that

$$G \cong \langle S_G \cup \{t\} : R_G \cup \{[t, a_1] = [t, a_1'] = e, t^{-1}x(q_1A_0)t = x(q_1A_0) \circledast a_1\} \rangle.$$

The proof of Proposition 5.4 is divided into three claims. The claims involve two new related groups: $G_{p(n)}(\mathbf{MM}_3)$ and $\overline{G_{p(n)}(\mathbf{MM}_3)}$, defined by

$$\begin{aligned} G_{p(n)}(\mathbf{MM}_3) &= \frac{G(\mathbf{MM}_3)}{\langle x(q_1A_0) \circledast a_1^{\circledast p(n)} = x(q_1A_0) \rangle}, \\ \overline{G_{p(n)}(\mathbf{MM}_3)} &= \frac{G}{\langle x(q_1A_0) \circledast a_1^{\circledast p(n)} = x(q_1A_0) \rangle}. \end{aligned}$$

Claim 5.7. $G/\langle t^{p(n)}=e\rangle \cong \overline{G_{p(n)}(\mathbf{MM}_3)}$.

Proof. Notice that the sets of generators of $G/\langle t^{p(n)}=e\rangle$ and $\overline{G_{p(n)}(\mathbf{MM}_3)}$ are the same. The only difference about the relations is that $\overline{G_{p(n)}(\mathbf{MM}_3)}$ has the relation $x(q_1A_0)\circledast a_1^{\circledast p(n)} = x(q_1A_0)$ and $G/\langle t^{p(n)}=e\rangle$ has the relation $t^{p(n)}=e$. We are going to show that these two relations imply each other in the two groups. Then it implies that the two groups are isomorphic.

We first show that $t^{p(n)}=e$ implies that $x(q_1A_0)=x(q_1A_0)\circledast a_1^{\circledast p(n)}$ in $G/\langle t^{p(n)}=e\rangle$. 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 $j\geq 1$. By [KMS17, Lemma 4.1, Relation (G1) and Remark 4.2], we know that $v(j)^2=e$ for all $j\geq 0$. 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

$$x(q_1A_0)=t^{-p(n)}x(q_1A_0)t^{p(n)}=x(q_1A_0)\circledast a_1^{\circledast p(n)}$$

in $G/\langle t^{p(n)}=e\rangle$.

On the other hand, $x(q_1A_0)\circledast a_1^{\circledast p(n)}=x(q_1A_0)$ implies that

$$t^{-p(n)}x(q_1A_0)t^{p(n)}=x(q_1A_0)$$

in $\overline{G_{p(n)}(\mathbf{MM}_3)}$. That is, $t^{p(n)}$ commutes with $x(q_1A_0)$, a_1 and a_1'. Since the only element in the intersection of the centralizers of $x(q_1A_0)$, a_1 and a_1' in G is e ([KMS17, Relations $(G1)$, $(G5c)$ and $(G7)$]), we know that $t^{p(n)}=e$, and the claim follows. Moreover, we can also see that the natural homomorphism $\phi: G/\langle t^{p(n)}=e\rangle\to\overline{G_{p(n)}(\mathbf{MM}_3)}$, is an isomorphism between $G/\langle t^{p(n)}=e\rangle$ and $\overline{G_{p(n)}(\mathbf{MM}_3)}$. □

For the next two claims, we construct a non-deterministic version of $\mathbf{MM}_3$, denoted by $\mathbf{MM}_3^{(p(n))}$. Comparing to $\mathbf{MM}_3$, the machine $\mathbf{MM}_3^{(p(n))}$ has additional states $2',3',\ldots p(n)'$. In addition to the commands of $\mathbf{MM}_3$, the new commands are

$1; Add(1)\to 2'$
$i'; Add(1)\to (i+1)'$ for $2\leq i<p(n)$
$p(n)'; Add(1)\to 1.$

Claim 5.8. *Let $G(\mathsf{MM}_3^{(p(n))})$ be the KMS-group of $\mathsf{MM}_3^{(p(n))}$. Then, $G_{p(n)}(\mathsf{MM}_3) \leq G(\mathsf{MM}_3^{(p(n))})$ and $w(0) = w(a)$ in $G_{p(n)}(\mathsf{MM}_3)$ if and only if $n \in X$.*

Proof. First, we state some observations of $G(\mathsf{MM}_3^{(p(n))})$. Based on [KMS17, Relation $(G8)$], in $G(\mathsf{MM}_3^{(p(n))})$ the relations involving $x(q_1 A_0)$ are

$$x(q_1 A_0) = x(q_{2'} A_0) \circledast a_1$$
$$x(q_{p(n)'} A_0) \circledast a_1 = x(q_1 A_0)$$

and the relations from $G(\mathsf{MM}_3)$ involving $x(q_1 A_0)$. From the relations involving states $2', 3' \dots (p(n)-1)'$, we can further deduce that in $G(\mathsf{MM}_3^{(p(n))})$

$$x(q_1 A_0) \circledast a_1^{\circledast p(n)} = x(q_1 A_0).$$

Therefore, the sets of generators and relations of $G_{p(n)}(\mathsf{MM}_3)$ are subsets of those of $G(\mathsf{MM}_3^{p(n)})$. So the mapping, ϕ, sending $g \in G_{p(n)}(\mathsf{MM}_3)$ to $g \in G(\mathsf{MM}_3^{(p(n))})$ is a homomorphism.

In $G(\mathsf{MM}_3^{(p(n))})$,

$$\begin{aligned} w(0) &= x(q_1 A_0) \circledast A_1 \circledast A_2 \circledast A_3 \\ &= x(q_1 A_0) \circledast a_1^{\circledast p(n)} \circledast A_1 \circledast A_2 \circledast A_3. \end{aligned}$$

On the other hand, $x(q_1 A_0) \circledast a_1^{p(n)} \circledast A_1 \circledast A_2 \circledast A_3 = w(a)$ in $G(\mathsf{MM}_3^{p(n)})$ if and only if $n \in X$. Hence, $w(0) = w(a)$ in $G(\mathsf{MM}_3^{p(n)})$ if and only if $n \in X$. Under the homomorphism ϕ, the preimage of $w(0)w(a)$ in $G_{p(n)}(\mathsf{MM}_3)$ is $w(0)w(a)$. Since $w(0)^2 = w(a)^2 = [w(0), w(a)] = e$, we can see that in $G_{p(n)}(\mathsf{MM}_3)$

$$w(0)w(a) = e \iff n \in X,$$

which completes the proof. □

Claim 5.9. *The group $\overline{G_{p(n)}(\mathsf{MM}_3)}$ is sofic.*

Proof. By Claim 5.8, $G_{p(n)}(\mathsf{MM}_3)$ is a subgroup of $G(\mathsf{MM}_3^{(p(n))})$. Since $G(\mathsf{MM}_3^{(p(n))})$ is solvable by Theorem 5.2, so is $G_{p(n)}(\mathsf{MM}_3)$.

Next, we will first show that $\overline{G_{p(n)}(\mathsf{MM}_3)}$ is an HNN-extension of $G_{p(n)}(\mathsf{MM}_3)$. Consider the subgroup H of $G_{p(n)}(\mathsf{MM}_3)$ generated by $x(q_1 A_0), a_1$ and a_1'. Let T be the normal subgroup generated by $x(q_1 A_0)$ in H, then

$$H = T \rtimes \langle a_1, a_1' \rangle.$$

This is because every $t \in T$ has order 2 but $\langle a_1, a_1' \rangle \cong \mathbb{Z} \times \mathbb{Z}$ ([KMS17, Relation $(G1)$]), which implies that $T \cap \langle a_1, a_1' \rangle = \{e\}$, and that $H / \langle x(q_1 A_0) = e \rangle = \langle a_1, a_1' \rangle$. Hence, every $h \in H$ can be written as $t a_1^n a_1'^m$ for some $t \in T$ and n, m.

We consider the function $\phi : H \to H$ defined by

$$\begin{aligned} \phi(e) &= e \\ \phi(a_1) &= a_1 \\ \phi(a_1') &= a_1' \\ \phi(x(q_1 A_0)) &= x(q_1 A_0) \circledast a_1, \end{aligned}$$

such that $\phi(t a_1^n a_1'^m) = \phi(t)\phi(a_1)^n \phi(a_1')^m$. We first prove ϕ is a homomorphism. From the definition, we can see that $\phi(x(q_1 A_0)^{a_1^n a_1'^m}) = \phi(x(q_1 A_0))^{a_1^n a_1'^m}$ for all n, m, then for all $t \in T$, $\phi(t^{a_1^n a_1'^m}) = \phi(t)^{a_1^n a_1'^m}$. 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 $t_1, t_2 \in T$, 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 injective. 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

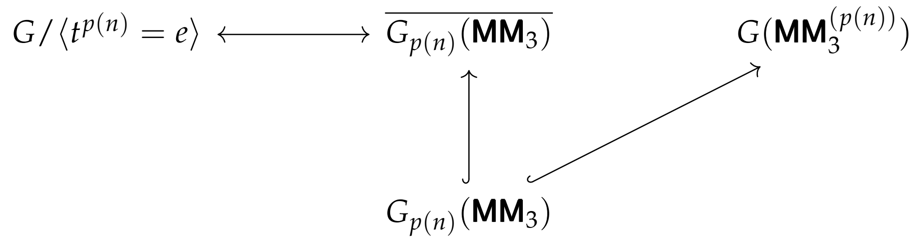
$$\phi^{p(n)}(x(q_1 A_0)) = x(q_1 A_0) \circledast a_1^{\circledast p(n)}.$$

Note that it is equivalent to prove that $t^{-p(n)} x(q_1 A_0) t^{p(n)} = x(q_1 A_0) \circledast a_1^{\circledast p(n)}$, which is proved in the proof of Claim 5.7. Then we know that $\phi^{p(n)}(x(q_1 A_0)) = x(q_1 A_0) \circledast a_1^{\circledast p(n)} = x(q_1 A_0)$, and hence, $\phi^{p(n)} = \mathbb{1}$ in H. The fact that $\phi^{p(n)} = \mathbb{1}$ implies that ϕ is injective. Because ϕ is injective and

$$\overline{G_{p(n)}(\mathbf{MM}_3)} \cong \frac{G_{p(n)}(\mathbf{MM}_3) * \mathcal{F}(\{t\})}{\langle t^{-1} a_1 t = \phi(a_1), t^{-1} a_1' t_1 = \phi(a_1'), t^{-1} x(q_1 A_0) t = \phi(x(q_1 A_0)) \rangle},$$

we can conclude that $\overline{G_{p(n)}(\mathbf{MM}_3)}$ is an HNN-extension of $G_{p(n)}(\mathbf{MM}_3)$. Since an HNN-extension of a solvable group is sofic [CLP15, Proposition II.4.1], $\overline{G_{p(n)}(\mathbf{MM}_3)}$ is sofic. □

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 diagram below.



Proof of Proposition 5.4. It suffices to choose $H = G$, which is defined in eq. (2), $t = t$ and $x = w(0)w(a)$. By the definition of G, $x^2 = e$. Since $G_{p(n)}(\mathsf{MM}_3)$ is embedded in $\overline{G_{p(n)}(\mathsf{MM}_3)}$ (Claim 5.9), we know $w(0)w(a) = e$ in $\overline{G_{p(n)}(\mathsf{MM}_3)}$ if and only if $n \in X$. By Claim 5.7, 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 Claim 5.7 and Claim 5.9, we know $G/\langle t^{p(n)} = e\rangle$ is sofic. □

6 Membership problem of constant-sized commuting-operator correlations

In this section and the next section, we'll let $\mathbb{K}_0$ be the subfield of $\mathbb{C}$ generated by $\mathbb{Q}$ and the roots of unity ω_n for $k, n \in \mathbb{Z}$.

This section is devoted to proving the Membership problem of $C^s_{qc}(N, M)$ over $\mathbb{K}$, which is defined below, is coRE-complete.

Problem (Membership$(N, N, M, M)^s_{\mathbb{K},qc}$). *Given a correlation $P \in \mathbb{K}^{N^2 \times M^2}$ for some constants N and M, decide if $P \in C^s_{qc}(N, M)$.*

We first present how to derive operator relations from correlations of certain forms. Such relations are used in the proofs of Theorems 6.8 and 7.4. The main result of this section is Theorem 6.9. In the proof of Theorem 6.9, we will embed a group of the form $G/\langle t^p = e\rangle$ into $\Gamma/\langle (t_1t_2)^{2p} = e\rangle$ following the general embedding procedure. To construct a correlation that certifies the relations of $\Gamma/\langle (t_1t_2)^{2p} = e\rangle$, we first show that there exists a constant-sized correlation that can certify the relation $(t_1t_2)^{2p} = e$ for any prime p.

6.1 Deriving operator relations from correlations

Quantum correlations can tell us some relations satisfied by the projectors and observables with respect to the shared state. In this section, we list such observations, which include what can be derived from the correlation $\tilde{P}$ associated with $\Gamma(A)$. Such relations are commonly used in the proofs of self-tests. Starting from this section, when we try to derive the operator relations from a correlation, we work in the commuting-operator model. About the notation, we omit the identity operator when it is applied by Alice or Bob. For example, $\langle\psi|P^{(k)}_i \cdot \mathbb{1}_B|\psi\rangle$ is written as $\langle\psi|P^{(k)}_i|\psi\rangle$.

Proposition 6.1. *Let $|\psi\rangle \in \mathcal{H}$ be a quantum state, and $\{P_j \mid j \in [n]\}$ and $\{Q_j \mid j \in [n]\}$ be two commuting projective measurements on $\mathcal{H}$ for some $n \geq 2$. If $\langle\psi|P_jQ_k|\psi\rangle = 0$ for all $j \neq k \in [n]$, then*

$$P_j|\psi\rangle = Q_j|\psi\rangle$$

for each $j \in [n]$.

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

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

From such calculations, we know

$$\|P_j|\psi\rangle\| = \|Q_j|\psi\rangle\| = \sqrt{x_j}.$$

Then we will prove that $P_j|\psi\rangle = Q_j|\psi\rangle$.

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

By the positivity of the vector norm, we know $P_j|\psi\rangle - Q_j|\psi\rangle = 0$, and similarly for other $j \in [n]$. □

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

Proposition 6.2. *Let $|\psi\rangle \in \mathcal{H}$ be a quantum state, $\{P_0^{(k)} \mid k \in [m_A]\}$ and $\{P_1^{(k)} \mid k \in [m_A]\}$ be two projective measurements on $\mathcal{H}$, both of which commute with the projective measurement $\{Q^{(l,l')} \mid l, l' \in [m_A]\}$ on $\mathcal{H}$. If*

$$\langle\psi|P_0^{(k)}Q^{(l,l')}|\psi\rangle = \langle\psi|P_1^{(k')}Q^{(l,l')}|\psi\rangle = 0$$

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

$$P_0^{(k)}P_1^{(k')}|\psi\rangle = P_1^{(k')}P_0^{(k)}|\psi\rangle$$

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

Proof. The condition implies that the strategies

$$\begin{aligned}&(|\psi\rangle, \{P_0^{(k)} \mid k \in [m_A]\}, \{\sum_{l'\in[m_A]} Q^{(k,l')} \mid k \in [m_A]\}),\\ &(|\psi\rangle, \{P_1^{(k')} \mid k' \in [m_A]\}, \{\sum_{l\in[m_A]} Q^{(l,k')} \mid k' \in [m_A]\})\end{aligned}$$

both satisfy the condition of Proposition 6.2, so we can derive that

$$\begin{aligned}P_0^{(k)}|\psi\rangle &= \sum_{l'\in[m_A]} Q^{(k,l')}|\psi\rangle,\\ P_1^{(k')}|\psi\rangle &= \sum_{l\in[m_A]} Q^{(l,k')}|\psi\rangle,\end{aligned}$$

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

$$\begin{aligned} P_0^{(k)} P_1^{(k')}|\psi\rangle &= P_0^{(k)} \sum_{l\in[m_A]} Q^{(l,k')}|\psi\rangle = \sum_{l\in[m_A]} Q^{(l,k')} P_0^{(k)}|\psi\rangle \\ &= \sum_{l\in[m_A]} Q^{(l,k')} \sum_{l'\in[m_A]} Q^{(k,l')}|\psi\rangle = Q^{(k,k')}|\psi\rangle = \sum_{l'\in[m_A]} Q^{(l',k)} \sum_{l\in[m_A]} Q^{(l,k')}|\psi\rangle \\ &= P_1^{(k')} \sum_{l'\in[m_A]} Q^{(l',k)}|\psi\rangle = P_1^{(k')} P_0^{(k)}|\psi\rangle, \end{aligned}$$

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 6.3 (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 $j = m$. Consider the case $j = m + 1$, 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. □

Before we study the implication of $\tilde{P}$, we prove a fact about commuting projectors.

Proposition 6.4. *Let $\{P_i \mid i \in [n]\}$ be a commuting set of projectors on $\mathcal{H}$ and $|\psi\rangle \in \mathcal{H}$. Then, $\prod_{i\in[n]} P_i|\psi\rangle = |\psi\rangle$ if and only if $P_i|\psi\rangle = |\psi\rangle$ for each $i \in [n]$.*

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

$$\begin{aligned}\|P_0|\psi\rangle - \prod_{0<l<n} P_l|\psi\rangle\|^2 =&\langle\psi|P_0|\psi\rangle + \langle\psi|\prod_{0<l<n} P_l|\psi\rangle - 2\langle\psi|\prod_{i\in[n]} P_i|\psi\rangle \\ =&\langle\psi|P_0|\psi\rangle + \langle\psi|\prod_{0<l<n} P_l|\psi\rangle - 2.\end{aligned}$$

Since $\|P_0|\psi\rangle - \prod_{0<l<n} P_l|\psi\rangle\|^2 \geq 0$, $\langle\psi|P_0|\psi\rangle \leq 1$, and $\langle\psi|\prod_{0<l<n} P_l|\psi\rangle \leq 1$, we know

$$P_0|\psi\rangle = |\psi\rangle \qquad\qquad \langle\psi|\prod_{0<l<n} P_l|\psi\rangle = 1.$$

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

Lemma 6.5. *For a binary linear system $A\boldsymbol{x} = 0$, if a commuting-operator strategy*

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

can induce the correlation $\tilde{P}$, then there exist two commuting sets of binary observables $\{M_{i,k} \mid i \in [m], k \in I_i\}$ and $\{N_{i,k} \mid i \in [m], k \in I_i\}$ with respect to $|\psi\rangle$ such that

$$M_{i,k}|\psi\rangle = N_{j,k}|\psi\rangle$$

for all $i, j \in [m]$ and $k \in I_i \cap I_j$,

$$\begin{aligned}M_{i,k}M_{i,l}|\psi\rangle &= M_{i,l}M_{i,k}|\psi\rangle, \\ N_{i,k}N_{i,l}|\psi\rangle &= N_{i,l}N_{i,k}|\psi\rangle,\end{aligned}$$

for all $k, l \in I_i$, and

$$\prod_{l\in I_i} M_{i,l}|\psi\rangle = \prod_{l\in I_i} N_{i,l}|\psi\rangle = |\psi\rangle,$$

for all $i \in [m]$.

Proof. Since $\tilde{P}(\boldsymbol{x}, \boldsymbol{y}|i, j) = 0$ for all $\boldsymbol{y}$, when $\boldsymbol{x} \notin S_i$, we know that $P_i^{(\boldsymbol{x})}|\psi\rangle = 0$ for all $\boldsymbol{x} \notin S_i$. Similarly, $Q_j^{(\boldsymbol{y})}|\psi\rangle = 0$ for all $\boldsymbol{y} \notin S_j$. We define

$$\begin{aligned}M_{i,k} &= \sum_{\boldsymbol{x}\in S_i:\boldsymbol{x}(k)=0} P_i^{(\boldsymbol{x})} - \sum_{\boldsymbol{x}\in S_i:\boldsymbol{x}(k)=1} P_i^{(\boldsymbol{x})} \\ N_{j,l} &= \sum_{\boldsymbol{y}\in S_j:\boldsymbol{y}(l)=0} Q_j^{(\boldsymbol{x})} - \sum_{\boldsymbol{y}\in S_j:\boldsymbol{y}(l)=1} Q_j^{(\boldsymbol{x})},\end{aligned}$$

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 rest of the proof, we fix a question pair (i, j) and assume $I_i \cap I_j = \{k_l \mid l \in [\alpha]\}$. Define $\Pi_{k_l} = \sum_{\boldsymbol{x},\boldsymbol{y}:\boldsymbol{x}(k_l)=\boldsymbol{y}(k_l)} P_i^{(\boldsymbol{x})} Q_j^{(\boldsymbol{y})}$ for each $l \in [\alpha]$. The fact that

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

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 $l \in [\alpha]$.

For the last conclusion, notice that

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

Because $\sum_{\boldsymbol{x}\notin S_i} P_i^{(\boldsymbol{x})} = 0$, we know

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

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

This lemma implies that if a relation $\prod_{l\in[n]} x_{i_l,k_l} = e$ is embedded in $\Gamma(A)$, then we can repeatedly apply Lemma 6.3 to conclude that

$$\prod_{l\in[n]} M_{i_l,k_l}|\psi\rangle = \prod_{l\in[n]} N_{i_l,k_l}|\psi\rangle = |\psi\rangle,$$

which is a key observation used in the proofs of Theorems 6.9 and 7.8.

6.2 The correlation $\mathfrak{C}_{2p}$ for D_{2p}

Recall that, for a prime p, the Dihedral group of order $4p$ is defined by $D_{2p} = \langle t_1, t_2 : t_1^2 = t_2^2 = (t_1t_2)^{2p} = e\rangle$. In this section, we introduce a correlation $\mathfrak{C}_{2p}$ that can certify the relation $(t_1t_2)^{2p} = e$. For this reason, we include symbols t_1 and t_2 in the input set I of $\mathfrak{C}_{2p}$, where

$$I := \{0, 1, 2, t_1, t_2, (0, t_1), (0, t_2)\}.$$

To define $\mathfrak{C}_{2p}$, we present a commuting-operator strategy inducing $\mathfrak{C}_{2p}$, denoted by

$$\tilde{S} = (|\tilde{\psi}\rangle, \{\{\tilde{P}_x^{(a)} \mid x \in I\} \mid a \in [8]\}, \{\{\tilde{Q}_y^{(b)} \mid y \in I\} \mid b \in [8]\}),$$

based on the left and right regular representations of D_{2p}. The definitions of $|\tilde{\psi}\rangle$, $\tilde{P}_x^a$ and $\tilde{Q}_y^b$ are given below.

Recall that the vector space

$$L^2 D_{2p} = \mathrm{span}(\{|(t_1t_2)^j\rangle, |t_2(t_1t_2)^j\rangle \mid j \in [2p]\}),$$

and the left and right regular representations of D_{2p} are $L : D_{2p} \to \mathcal{U}(L^2D_{2p})$ and $R : D_{2p} \to \mathcal{U}(L^2D_{2p})$. We first define $|\tilde{\psi}\rangle := |e\rangle \in L^2D_{2p}$.

Next we define some idempotent elements of $\mathbb{C}[D_{2p}]$.

$$\pi_0^{(0)} = \frac{1}{2p} \sum_{j \in [2p]} (t_1t_2)^j \tag{3}$$

$$\pi_0^{(1)} = \frac{1}{2p} \sum_{j \in [2p]} (-1)^j (t_1t_2)^j \tag{4}$$

$$\pi_0^{(2)} = \frac{1}{p} \sum_{j \in [2p]} \cos(\frac{j\pi}{p})(t_1t_2)^j \tag{5}$$

$$\pi_0^{(3)} = e - \pi_0^{(0)} - \pi_0^{(1)} - \pi_0^{(2)}. \tag{6}$$

$$\pi_1^{(0)} = \frac{1}{2}\pi_0^{(2)} + \frac{1}{2p} \sum_{j \in [2p]} \cos(\frac{(j+1/2)\pi}{p}) t_2(t_1t_2)^j \tag{7}$$

$$\pi_1^{(1)} = \pi_0^{(2)} - \pi_1^{(0)} \tag{8}$$

$$\pi_1^{(2)} = e - \pi_0^{(2)}. \tag{9}$$

$$\pi_2^{(0)} = \frac{1}{2}\pi_0^{(2)} + \frac{1}{2p} \sum_{j \in [2p]} \sin(\frac{(j+1/2)\pi}{p}) t_2(t_1t_2)^j \tag{10}$$

$$\pi_2^{(1)} = \pi_0^{(2)} - \pi_2^{(0)} \tag{11}$$

$$\pi_2^{(2)} = e - \pi_0^{(2)}. \tag{12}$$

Then we define the projectors used by Alice and Bob.

- For the input 0,

$$\tilde{P}_0^{(a)} = \begin{cases} R(\pi_0^{(a)}) & \text{if } a \in [4] \\ 0 & \text{otherwise;} \end{cases}$$

$$\tilde{Q}_0^{(b)} = \begin{cases} L(\pi_0^{(b)}) & \text{if } b \in [4] \\ 0 & \text{otherwise.} \end{cases}$$

- For the inputs $x, y \in \{1,2\}$,

$$\tilde{P}_x^{(a)} = \begin{cases} R(\pi_x^{(a)}) & \text{if } a \in [3] \\ 0 & \text{otherwise;} \end{cases}$$
$$\tilde{Q}_y^{(b)} = \begin{cases} L(\pi_y^{(b)}) & \text{if } b \in [3] \\ 0 & \text{otherwise.} \end{cases}$$

- For the inputs $x, y \in \{t_1, t_2\}$

$$\tilde{P}_x^{(a)} = \begin{cases} \frac{R(e)+(-1)^a R(x)}{2} & \text{if } a \in [2] \\ 0 & \text{otherwise;} \end{cases}$$
$$\tilde{Q}_y^{(b)} = \begin{cases} \frac{L(e)+(-1)^b L(y)}{2} & \text{if } b \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

- For the inputs $(0,x)$ and $(0,y)$ with $x, y \in \{t_1, t_2\}$

$$\tilde{P}_{(0,x)}^{(a_0,a_1)} = \tilde{P}_0^{(a_0)} \tilde{P}_x^{(a_1)} \qquad \text{with } a_0 \in [4], a_1 \in [2],$$
$$\tilde{Q}_{(0,y)}^{(b_0,b_1)} = \tilde{Q}_0^{(b_0)} \tilde{Q}_y^{(b_1)} \qquad \text{with } b_0 \in [4], b_1 \in [2].$$

Note that the fact that $\tilde{P}_0^{(a)}$ commutes with $\tilde{P}_x^{(a)}$ for $x \in \{t_1, t_2\}$ follows from the observation that

$$R(t_1)R((t_1t_2)^j)R(t_1) = R((t_1t_2)^{-j}) \qquad R(t_2)R((t_1t_2)^j)R(t_2) = R((t_1t_2)^{-j})$$

for each $j \in [2p]$. With similar reasoning, we get that $\tilde{Q}_0^{(b)}$ commutes with $\tilde{Q}_y^{(b)}$ for $y \in \{t_1, t_2\}$.

Definition 6.6. *The correlation $\mathfrak{C}_{2p} : I \times I \times [8] \times [8] \to \mathbb{K}_0$, is defined by*

$$\mathfrak{C}_{2p}(a, b|x, y) = \langle \tilde{\psi} | \tilde{P}_x^{(a)} \tilde{Q}_y^{(b)} | \tilde{\psi} \rangle.$$

Since $\mathfrak{C}_{2p}$ is induced by $\tilde{S}$, the next claim is immediate.

Claim 6.7. *The correlation $\mathfrak{C}_{2p}$ is symmetric and in $C_{qc}^s(7,8)$.*

The importance of $\mathfrak{C}_{2p}$ is summarized in the next theorem.

Theorem 6.8. *If a commuting-operator strategy $S = (|\psi\rangle, \{M_x^{(a)}\}, \{N_y^{(b)}\})$ can induce $\mathfrak{C}_{2p}$ 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*

$$U_A U_B |\psi\rangle = |\psi\rangle$$
$$(N_{t_1} N_{t_2})^2 U_B |\psi\rangle = U_B (N_{t_1} N_{t_2})^{2r} |\psi\rangle$$
$$(M_{t_1} M_{t_2})^2 U_A |\psi\rangle = U_A (M_{t_1} M_{t_2})^{2r} |\psi\rangle,$$

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*

$$(M_{t_1} M_{t_2})^{2p} |\psi\rangle = |\psi\rangle.$$

Before we prove Theorem 6.8, we present certain nonzero values of $\mathfrak{C}_{2p}$, which will help the proof.

For question 0.

$$\mathfrak{C}_{2p}(a, b|0, 0) = \begin{cases} \frac{1}{2p} & \text{if } a = b = 0 \text{ or } a = b = 1 \\ \frac{1}{p} & \text{if } a = b = 2 \\ \frac{p-2}{p} & \text{if } a = b = 3 \\ 0 & \text{otherwise.} \end{cases}$$

When Alice's question is from $\{t_1, t_2\}$ and Bob's question is from $\{1, 2\}$, some of the nonzero values of $\mathfrak{C}_{2p}(a, b|x, y)$ are summarized in the following table.

		$y = 1$		$y = 2$	
		$b = 0$	$b = 1$	$b = 0$	$b = 1$
$x = t_1$	$a = 0$	$\frac{\cos^2(\pi/4p)}{2p}$	$\frac{\sin^2(\pi/4p)}{2p}$	$\frac{1-\sin(\pi/2p)}{4p}$	$\frac{1+\sin(\pi/2p)}{4p}$
	$a = 1$	$\frac{\sin^2(\pi/4p)}{2p}$	$\frac{\cos^2(\pi/4p)}{2p}$	$\frac{1+\sin(\pi/2p)}{4p}$	$\frac{1-\sin(\pi/2p)}{4p}$
$x = t_2$	$a = 0$	$\frac{\cos^2(\pi/4p)}{2p}$	$\frac{\sin^2(\pi/4p)}{2p}$	$\frac{1+\sin(\pi/2p)}{4p}$	$\frac{1-\sin(\pi/2p)}{4p}$
	$a = 1$	$\frac{\sin^2(\pi/4p)}{2p}$	$\frac{\cos^2(\pi/4p)}{2p}$	$\frac{1-\sin(\pi/2p)}{4p}$	$\frac{1+\sin(\pi/2p)}{4p}$

Table 1: The correlation for $x \in \{t_1, t_2\}$ and $y \in \{1, 2\}$.

Note that in this case for $a > 1$ or $b > 2$, $\mathfrak{C}_{2p}(a, b|x, y) = 0$.

When $x, y \in \{0, 1, 2\}$, the values of $\mathfrak{C}_{2p}(a, b|x, y)$ for $a, b \in [3]$ are summarized in the following table.

		$x=1$			$x=2$			$x=0$	
		$a=0$	$a=1$	$a=2$	$a=0$	$a=1$	$a=2$	$a=2$	$a\neq 2$
$y=1$	$b=0$	$\frac{1}{2p}$	0	0	$\frac{1}{4p}$	$\frac{1}{4p}$	0	$\frac{1}{2p}$	0
	$b=1$	0	$\frac{1}{2p}$	0	$\frac{1}{4p}$	$\frac{1}{4p}$	0	$\frac{1}{2p}$	0
	$b=2$	0	0	$\frac{p-1}{p}$	0	0	$\frac{p-1}{p}$	0	$\frac{p-1}{p}$
$y=2$	$b=0$	$\frac{1}{4p}$	$\frac{1}{4p}$	0	$\frac{1}{2p}$	0	0	$\frac{1}{2p}$	0
	$b=1$	$\frac{1}{4p}$	$\frac{1}{4p}$	0	0	$\frac{1}{2p}$	0	$\frac{1}{2p}$	0
	$b=2$	0	0	$\frac{p-1}{p}$	0	0	$\frac{p-1}{p}$	0	$\frac{p-1}{p}$
$y=0$	$b=2$	$\frac{1}{2p}$	$\frac{1}{2p}$	0	$\frac{1}{2p}$	$\frac{1}{2p}$	0	$\frac{1}{p}$	0
	$b\neq 2$	0	0	$\frac{p-1}{p}$	0	0	$\frac{p-1}{p}$	0	$\frac{p-1}{p}$

Table 2: The correlation for $x, y \in \{0, 1, 2\}$.

When $x \in \{0, t_1\}$ and $y = (0, t_1)$ some values of $\mathfrak{C}_{2p}(a, b|x, y)$ are given in the table below.

		$y=(0,t_1)$							
		$b=(0,0)$	$b=(0,1)$	$b=(1,0)$	$b=(1,1)$	$b=(2,0)$	$b=(2,1)$	$b=(3,0)$	$b=(3,1)$
$x=0$	$a=0$	$\frac{1}{4p}$	$\frac{1}{4p}$	0	0	0	0	0	0
	$a=1$	0	0	$\frac{1}{4p}$	$\frac{1}{4p}$	0	0	0	0
	$a=2$	0	0	0	0	$\frac{1}{2p}$	$\frac{1}{2p}$	0	0
	$a=3$	0	0	0	0	0	0	$\frac{p-2}{2p}$	$\frac{p-2}{2p}$
$x=t_1$	$a=0$	$\frac{1}{4p}$	0	$\frac{1}{4p}$	0	$\frac{1}{2p}$	0	$\frac{p-2}{2p}$	0
	$a=1$	0	$\frac{1}{4p}$	0	$\frac{1}{4p}$	0	$\frac{1}{2p}$	0	$\frac{p-2}{2p}$

Table 3: The correlation when Alice's questions are 0 and t_1 and Bob's question is $(0, t_1)$.

The correlation $\mathfrak{C}_{2p}(a, b|x, y)$ has similar values when $x \in \{0, t_2\}$ and $y = (0, t_2)$, when $x = (0, t_1)$ and $y \in \{0, t_1\}$, and when $x = (0, t_2)$ and $y \in \{0, t_2\}$.

When $x = (0, t_1)$ and $y = (0, t_2)$, some of the values of $\mathfrak{C}_{2p}(a, b|x, y)$ are summarized in the following table.

		$y=(0,t_2)$							
		$b=(0,0)$	$b=(0,1)$	$b=(1,0)$	$b=(1,1)$	$b=(2,0)$	$b=(2,1)$	$b=(3,0)$	$b=(3,1)$
$x=(0,t_1)$	$a=(0,0)$	$\frac{1}{4p}$	0	0	0	0	0	0	0
	$a=(0,1)$	0	$\frac{1}{4p}$	0	0	0	0	0	0
	$a=(1,0)$	0	0	0	$\frac{1}{4p}$	0	0	0	0
	$a=(1,1)$	0	0	$\frac{1}{4p}$	0	0	0	0	0
	$a=(2,0)$	0	0	0	0	$\frac{\cos^2(\pi/2p)}{2p}$	$\frac{\sin^2(\pi/2p)}{2p}$	0	0
	$a=(2,1)$	0	0	0	0	$\frac{\sin^2(\pi/2p)}{2p}$	$\frac{\cos^2(\pi/2p)}{2p}$	0	0
	$a=(3,0)$	0	0	0	0	0	0	$\frac{p-2}{2p}$	0
	$a=(3,1)$	0	0	0	0	0	0	0	$\frac{p-2}{2p}$

Table 4: The correlation when Alice's question is $(0, t_1)$ and Bob's question is $(0, t_2)$.

Proof of Theorem 6.8. In order to prove this theorem, we need to find a decomposition of $|\psi\rangle$ as

$$|\psi\rangle = \sum_{j=1}^{p-1} (|\psi_j\rangle + |\psi_{-j}\rangle) + |\psi_0\rangle + |\psi_p\rangle + |\psi_{2p}\rangle + |\psi_{3p}\rangle,$$

where $\{|\psi_i\rangle\}$ is an orthogonal set. Intuitively, this decomposition follows the decomposition of the regular representation of t_1t_2 into irreducible representations. The states $|\psi_0\rangle$, $|\psi_p\rangle$, $|\psi_{2p}\rangle$ and $|\psi_{3p}\rangle$ are in each of the 1-dimensional irreducible representations. For $1 \le j \le p-1$, $|\psi_j\rangle$ and $|\psi_{-j}\rangle$ are in the 2-dimensional irreducible representation, in which

$$t_1t_2 \mapsto \begin{pmatrix} \omega_{2p}^{j} & 0 \\ 0 & \omega_{2p}^{-j} \end{pmatrix}$$

Applying Proposition 6.2 to the values given in Table 3, we can get that

$$M_x^{(a_x)} M_0^{(a_0)} |\psi\rangle = N_{(0,a_x)}^{(a_0,a_x)} |\psi\rangle = M_0^{(a_0)} M_x^{(a_x)} |\psi\rangle$$

for $a_0 \in [4]$, $x \in \{t_1, t_2\}$ and $a_x \in [2]$.

Applying Proposition 6.1 to the values given in Table 4, we can get that

$$M_{(0,t_1)}^{(0,a_1)} |\psi\rangle = N_{(0,t_2)}^{(0,a_1)} |\psi\rangle, \tag{13}$$

$$M_{(0,t_1)}^{(1,a_1)} |\psi\rangle = N_{(0,t_2)}^{(1,1-a_1)} |\psi\rangle \tag{14}$$

for each $a_1 \in [2]$, and that

$$M_{t_1}^{(a_1)} M_0^{(0)} |\psi\rangle = N_{(0,t_2)}^{(0,a_1)} |\psi\rangle = M_{t_2}^{(a_1)} M_0^{(0)} |\psi\rangle \tag{15}$$

$$M_{t_1}^{(a_1)} M_0^{(1)} |\psi\rangle = N_{(0,t_2)}^{(1,1-a_1)} |\psi\rangle = M_{t_2}^{(1-a_1)} M_0^{(1)} |\psi\rangle. \tag{16}$$

Then we can define the first two sub-normalized states $|\psi_0\rangle$ and $|\psi_p\rangle$, which are

$$|\psi_0\rangle := M_{t_1}^{(0)} M_0^{(0)} |\psi\rangle, \tag{17}$$

$$|\psi_p\rangle := M_{t_1}^{(1)} M_0^{(0)} |\psi\rangle. \tag{18}$$

Define $M_x := M_x^{(0)} - M_x^{(1)}$ and $N_y := N_y^{(0)} - N_y^{(1)}$ for $x, y = t_1, t_2$. From Table 3 and their definitions, we know that

$$\| |\psi_0\rangle \|^2 = \| |\psi_p\rangle \|^2 = \frac{1}{4p}, \tag{19}$$

$$M_{t_1} |\psi_0\rangle = |\psi_0\rangle, \tag{20}$$

$$M_{t_1} |\psi_p\rangle = -|\psi_p\rangle, \tag{21}$$

and hence $\langle\psi_0|\psi_p\rangle = 0$. By eqs. (15) and (16), we know

$$|\psi_0\rangle = M_{t_2}^{(0)} M_0^{(0)} |\psi\rangle, \tag{22}$$

$$|\psi_p\rangle = M_{t_2}^{(1)} M_0^{(0)} |\psi\rangle. \tag{23}$$

The definition of M_{t_2} implies that

$$M_{t_2}|\psi_0\rangle = |\psi_0\rangle, \tag{24}$$

$$M_{t_2}|\psi_p\rangle = -|\psi_p\rangle. \tag{25}$$

Next, we define another two sub-normalized states $|\psi_{2p}\rangle$ and $|\psi_{3p}\rangle$, which are

$$|\psi_{2p}\rangle := M_{t_1}^{(1)} M_0^{(1)} |\psi\rangle \tag{26}$$

$$|\psi_{3p}\rangle := M_{t_1}^{(0)} M_0^{(1)} |\psi\rangle. \tag{27}$$

Based on Table 3 and the definition of M_{t_1} we can see that

$$\| |\psi_{2p}\rangle \|^2 = \| |\psi_{3p}\rangle \|^2 = \frac{1}{4p}, \tag{28}$$

$$M_{t_1}|\psi_{2p}\rangle = -|\psi_{2p}\rangle \tag{29}$$

$$M_{t_1}|\psi_{3p}\rangle = |\psi_{3p}\rangle, \tag{30}$$

By eqs. (15) and (16), we get that

$$|\psi_{2p}\rangle = M_{t_2}^{(0)} M_0^{(1)} |\psi\rangle \tag{31}$$

$$|\psi_{3p}\rangle = M_{t_2}^{(1)} M_0^{(1)} |\psi\rangle. \tag{32}$$

Hence, by the definition of M_{t_2}, we get that

$$M_{t_2}|\psi_{2p}\rangle = |\psi_{2p}\rangle \tag{33}$$

$$M_{t_2}|\psi_{3p}\rangle = -|\psi_{3p}\rangle, \tag{34}$$

and that

$$\langle\psi_{2p}|\psi_{3p}\rangle = 0. \tag{35}$$

Also, notice that $|\psi_0\rangle, |\psi_p\rangle$ are 1-eigenvectors of $M_{t_1}M_{t_2}$ and $|\psi_{2p}\rangle, |\psi_{3p}\rangle$ are -1-eigenvectors of $M_{t_1}M_{t_2}$, so

$$\langle\psi_0|\psi_{2p}\rangle = \langle\psi_0|\psi_{3p}\rangle = \langle\psi_p|\psi_{2p}\rangle = \langle\psi_p|\psi_{3p}\rangle = 0. \tag{36}$$

We can conclude that $\{|\psi_0\rangle, |\psi_p\rangle, |\psi_{2p}\rangle, |\psi_{3p}\rangle\}$ is an orthogonal set.

Following [Fu19, Proposition 6.10], Tables 1 and 2 give us the correlations induced by the following two strategies

$$S := (\frac{M_0^{(2)}|\psi\rangle}{\|M_0^{(2)}|\psi\rangle\|}, \{\{M_x^{(0)}, M_x^{(1)}\} \mid x = 1,2\}, \{\{N_y^{(0)}, N_y^{(1)}\} \mid y = t_1, t_2\}),$$
$$S' := (\frac{M_0^{(2)}|\psi\rangle}{\|M_0^{(2)}|\psi\rangle\|}, \{\{M_x^{(0)}, M_x^{(1)}\} \mid x = t_1, t_2\}, \{\{N_y^{(0)}, N_y^{(1)}\} \mid y = 1,2\}).$$

Then we can define $M_2 := M_2^{(0)} - M_2^{(1)}$ and

$$|\psi_1\rangle = \frac{1}{2}(M_1^{(0)} - iM_2M_1^{(1)} + iM_2M_1^{(0)} + M_1^{(1)})|\psi\rangle \tag{37}$$
$$|\psi_{-1}\rangle = \frac{1}{2}(M_1^{(0)} + iM_2M_1^{(1)} - iM_2M_1^{(0)} + M_1^{(1)})|\psi\rangle. \tag{38}$$

Following the proofs of [Fu19, Propositions 6.11, 6.12 and 6.13], we can conclude that

$$\||\psi_1\rangle\|^2 = \||\psi_{-1}\rangle\|^2 = \frac{1}{2p} \tag{39}$$
$$M_{t_1}M_{t_2}|\psi_1\rangle = \omega_{2p}|\psi_1\rangle \tag{40}$$
$$N_{t_1}N_{t_2}|\psi_1\rangle = \omega_{2p}^{-1}|\psi_1\rangle \tag{41}$$
$$M_{t_1}M_{t_2}|\psi_{-1}\rangle = \omega_{2p}^{-1}|\psi_{-1}\rangle \tag{42}$$
$$N_{t_1}N_{t_2}|\psi_{-1}\rangle = \omega_{2p}|\psi_{-1}\rangle. \tag{43}$$

Using the unitaries U_A and U_B from the assumption of the theorem, we can define

$$|\psi_j\rangle = (U_AU_B)^{\log_r j}|\psi_1\rangle \qquad |\psi_{-j}\rangle = (U_AU_B)^{\log_r j}|\psi_{-1}\rangle. \tag{44}$$

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 $\||\psi_j\rangle\|^2 = \||\psi_{-j}\rangle\|^2 = 1/2p$. Following the proof of [Fu19, Proposition 6.14], we can get that

$$(M_{t_1}M_{t_2})^2|\psi_j\rangle = \omega_p^j|\psi_j\rangle$$
$$(N_{t_1}N_{t_2})^2|\psi_j\rangle = \omega_p^{-j}|\psi_j\rangle$$
$$(M_{1_1}M_{t_2})^2|\psi_{-j}\rangle = \omega_p^{-j}|\psi_{-j}\rangle$$
$$(N_{t_1}N_{t_2})^2|\psi_{-j}\rangle = \omega_p^j|\psi_{-j}\rangle.$$

It implies that $|\psi_j\rangle$ is an eigenvector of M_1M_2 of eigenvalue ω_{2p}^j or $-\omega_{2p}^j$, and that $|\psi_{-j}\rangle$ is an eigenvector of M_1M_2 of eigenvalue ω_{2p}^{-j} or $-\omega_{2p}^{-j}$ for $1 \le j \le p-1$. By the orthogonality between eigenvectors of different eigenvalues of a unitary, we know that

$$\langle\psi_j|\psi_{-j}\rangle = \langle\psi_j|\psi_k\rangle = \langle\psi_{-j}|\psi_{-k}\rangle = 0 \tag{45}$$

for each $1 \le j \ne k \le p-1$.

Define

$$|\psi'\rangle = \sum_{j=1}^{p-1}(|\psi_j\rangle + |\psi_{-j}\rangle) + |\psi_0\rangle + |\psi_p\rangle + |\psi_{2p}\rangle + |\psi_{3p}\rangle. \tag{46}$$

By the orthogonality relations and the norms of each subnormalized state, we can calculate that $\||\psi'\rangle\| = 1$. Moreover,

$$\begin{aligned}\langle\psi|\psi'\rangle =& \langle\psi|\psi_0\rangle + \langle\psi|\psi_p\rangle + \langle\psi|\psi_{2p}\rangle + \langle\psi|\psi_{3p}\rangle + \sum_{j=1}^{p-1}(\langle\psi|\psi_j\rangle + \langle\psi|\psi_{-j}\rangle)\\ =& \||\psi_0\rangle\|^2 + \||\psi_p\rangle\|^2 + \||\psi_{2p}\rangle\|^2 + \||\psi_{3p}\rangle\|^2 + (p-1)(\langle\psi|\psi_1\rangle + \langle\psi|\psi_{-1}\rangle)\\ =& \frac{1}{p} + (p-1)(\frac{1}{2p} + \frac{1}{2p}) = 1,\end{aligned}$$

where we use $(U_A U_B)|\psi\rangle = |\psi\rangle$ and derivation in the proof of [Fu19, Proposition 6.14]. Therefore, we know $|\psi\rangle = |\psi'\rangle$.

With the decomposition of $|\psi\rangle$, we can conclude that

$$\begin{aligned}&(M_{t_1}M_{t_2})^{2p}|\psi\rangle\\ =&(M_{t_1}M_{t_2})^{2p}(|\psi_0\rangle + |\psi_p\rangle + |\psi_{2p}\rangle + |\psi_{3p}\rangle + \sum_{j=1}^{p-1}(|\psi_j\rangle + |\psi_{-j}\rangle))\\ =&1^{2p}(|\psi_0\rangle + |\psi_p\rangle) + (-1)^{2p}(|\psi_{2p}\rangle + |\psi_{3p}\rangle) + \sum_{j=1}^{p-1}(\omega_{2p}^{2jp}|\psi_j\rangle + \omega_{2p}^{-2jp}|\psi_{-j}\rangle)\\ =&|\psi\rangle,\end{aligned}$$

which completes the proof. □

6.3 Proof of undecidability

Theorem 6.9. *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 that $G = \langle S : R\rangle$ is a finitely presented group, which has a generator t and an involutary generator x such that

$$x = e \text{ in } G/\langle t^{p(n)} = e\rangle \iff n \in X. \tag{47}$$

Then, there exist a constant M_{qc}, which only depends on the presentation $\langle S : R\rangle$ of G and r, and a family of correlations $\{C_n \mid n > 0\} \subset \mathbb{K}_0^{M_{qc}^2 \times 8^2}$ such that $C_n \in C_{qc}^s(M_{qc}, 8)$ if and only if $n \notin X$.

The existence of r follows from [Mur88]. The proof of Theorem 6.9 is broken into several claims.

To construct C_n, we first extend G and embed it into a solution group. Define

$$D := \langle u, t_D : u^{-1} t_D u = t_D^r \rangle$$
$$K := (G * D)/\langle t = t_D \rangle.$$

Note that

$$K/\langle t^{p(n)} = e\rangle \cong \frac{(G/\langle t^{p(n)} = e\rangle) * D}{\langle t = t_D\rangle},$$

which means that $K/\langle t^{p(n)} = e\rangle$ is the free product of $G/\langle t^{p(n)} = e\rangle$ and D with amalgamation. Hence, $G/\langle t^{p(n)} = e\rangle$ is embedded in $K/\langle t^{p(n)} = e\rangle$ and $x = e$ in $K/\langle t^{p(n)} = e\rangle$ if and only if $n \in X$. Because of the relation $t = t_D$, we can write t and t_D as t in $K/\langle t^{p(n)} = e\rangle$ without any confusion.

Claim 6.10. *There exist an oblivious solution group Γ and an injective homomorphism $\phi : K \to \Gamma$ such that $\phi(x) = x$ and $\phi(t) = (t_1t_2)^2$. Moreover, $\Gamma/\langle (t_1t_2)^{2p(n)} = e\rangle$ is oblivious, and in $\Gamma/\langle (t_1t_2)^{2p(n)} = e\rangle$,*

$$x = e \iff n \in X.$$

Proof. To construct the solution group Γ, wherein K is embedded, we follow Theorem 4.1 with a slight modification. The embedding takes two steps.

In the first step, we embed G in G', which is defined below. Define $S' = \{s_1, s_2 \mid s \in S\} \cup \{x\}$, $\phi_1 : \mathcal{F}(S) \to \mathcal{F}(S')$ by $\phi_1(s) = s_1s_2s_1s_2$ for each $s \neq x$ and $\phi_1(x) = x$, and

$$G' = \langle S' : \{s_1^2 = s_2^2 = e \mid s \in S\} \cup R' \cup \{x = x_1x_2x_1x_2\}\rangle,$$

where $R' = \{\phi_1(r)^+ \mid r \in R\}$. In particular, if any $r \in R$ involves x, in $\phi_1(r)^+$, we replace x by $x_1x_2x_1x_2$. Following the steps of Theorem 4.1, we embed D in D', which has generators $t_{D,1}$ and $t_{D,2}$ such that t_D is embedded as $(t_{D,1}t_{D,2})^2$.

In the second step, we follow the wagon wheel construction and construct an $m_0 \times n_0$ binary linear system $A_G\boldsymbol{x} = 0$. Define $I_{G,i} = \{k \in [n_0] \mid A_G(i,k) = 1\}$ for $i \in [m_0]$. Then G' is embedded in

$$\Gamma'(A_G) = \frac{G_0 * G_1 * \ldots * G_{m_0-1}}{\langle P_G\rangle},$$

where

$$G_i = \langle \{g_{i,k} \mid k \in I_{G,i}\} : \{g_{i,k}^2, [g_{i,k}, g_{i,k'}], \prod_{j\in I_{G,i}} g_{i,j} \mid k, k' \in I_{G,i}\}\rangle.$$

We also follow the wagon wheel construction to construct an $m_1 \times n_1$ binary linear system $A_D\boldsymbol{y} = 0$. Define $I_{D,i} = \{k \in [n_1] \mid A_D(i,k) = 1\}$ for $i \in [m_1]$. Then D' is embedded in

$$\Gamma'(A_D) = \frac{H_0 * H_1 * \ldots * H_{m_1-1}}{\langle P_D\rangle},$$

where

$$H_i = \langle \{h_{i,k} \mid k \in I_{D,i}\} : \{h_{i,k}^2, [h_{i,k}, h_{i,k'}], \prod_{j \in I_{D,i}} h_{i,j} \mid k, k' \in I_{G,i}\} \rangle.$$

To define Γ, we need to define the following sets. The sets of the generators of $\Gamma'(A_G)$ and $\Gamma'(A_D)$ are

$$G^{\#} = \bigcup_{i \in [m_0]} \{g_{i,k} \mid k \in I_{G,i}\} \tag{48}$$

$$H^{\#} = \bigcup_{i \in [m_1]} \{h_{i,k} \mid k \in I_{D,i}\}. \tag{49}$$

The set of words related to t and t_D is

$$P_t = \{gh, hg \mid g = t_1 \in G^{\#}, h = t_{D,1} \in H^{\#}\} \cup \{gh, hg \mid g = t_2 \in G^{\#}, h = t_{D,2} \in H^{\#}\}.$$

Then the solution group Γ is

$$\Gamma := \frac{\Gamma'(A_G) * \Gamma'(A_D)}{\langle P_t \rangle}.$$

In other words,

$$\Gamma = \frac{G_0 * G_1 * \ldots * G_{m_0 - 1} * H_0 * \ldots H_{m_1 - 1}}{\langle P_G \cup P_D \cup P_t \rangle}.$$

In the construction of Γ, we effectively combine the two systems $A_G \boldsymbol{x} = 0$ and $A_D \boldsymbol{y} = 0$. For simplicity, we define $m := m_0 + m_1$ and $n := n_0 + n_1$, then the new system is an $m \times n$ binary linear system game $A\boldsymbol{x} = 0$ where

$$A(i,k) = 1 \iff (i < m_0, A_G(i,k) = 1) \text{ or } (i \geq m_0, k \geq n_0, A_D(i - m_0, k - n_0) = 1).$$

To show

$$\Gamma \cong \Gamma'(A),$$

we can rewrite Γ as

$$\Gamma \cong \frac{G_0 * G_1 * \ldots * G_{m_0 - 1} * G_{m_0} * \ldots G_{m-1}}{\langle P_G \cup P_D \cup P_t \rangle},$$

where $G_j \cong H_{j - m_0}$ as we relabel the generator $h_{j-m_0,k}$ as $g_{j,k+n_0}$ for $j \geq m_0$ and the sets P_D and P_t are adjusted accordingly.

Because G and D are embedded in $\Gamma'(A_G)$ and $\Gamma'(A_D)$ respectively and the relation $t = t_D$ is enforced by $\langle P_t \rangle$, we can conclude that K is embedded in Γ and the injective homomorphism is denoted by $\phi : K \to \Gamma$. The homomorphism ϕ induces the natural homomorphism

$$\phi' : K / \langle t^{p(n)} = e \rangle \to \Gamma / \langle (t_1 t_2)^{2p(n)} = e \rangle$$

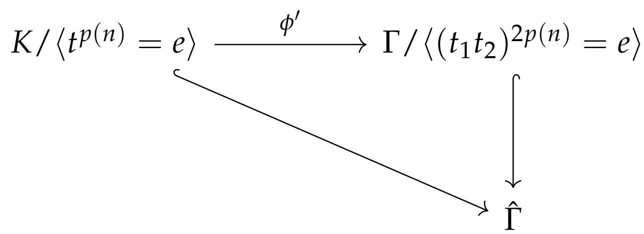
by $\phi'(s) = \phi(s)$. Next we show that ϕ' is also injective.

We can embed $\Gamma/\langle (t_1t_2)^{2p(n)} = e\rangle$ into a solution group denoted by $\hat{\Gamma}$. The only additional step after constructing $A_G\boldsymbol{x} = 0$ and $A_D\boldsymbol{y} = 0$ is to add equations for the relation $(t_1t_2)^{2p(n)} = e$. We can apply the wagon wheel construction to the relation $(t_1t_2)^{2p(n)} = e$ to construct a linear system $A_t\boldsymbol{x} = 0$. Denote the combined linear system of $A_t\boldsymbol{x} = 0$, $A_G\boldsymbol{x} = 0$ and $A_D\boldsymbol{x} = 0$ by $\hat{A}\boldsymbol{x} = 0$. Then

$$\hat{\Gamma} = \Gamma'(\hat{A}) \cong \frac{\Gamma'(A_G) * \Gamma'(A_D) * \Gamma'(A_t)}{\langle P_t' \rangle},$$

where P_t' says all the generators of the three solution groups that equals t_1 are equivalent and all the generators of the three solution groups that equals t_2 are equivalent Following the same steps of embedding K, the group $K/\langle t^{p(n)} = e\rangle$ can also be embedded in $\hat{\Gamma}$.

The commutation diagram is given below.



The two injections in the diagram implies that ϕ' is injective as well. We have shown that $x = e$ in $K/\langle t^{p(n)} = e\rangle \iff n \in X$, so

$$x = e \text{ in } \Gamma/\langle (t_1t_2)^{2p(n)} = e\rangle \iff n \in X.$$

What remains to prove is that $\Gamma/\langle (t_1t_2)^{2p(n)} = e\rangle$ is also oblivious. The first step is to prove that Γ is oblivious. Recall the definitions of $G^\#$ and H^* in eqs. (48) and (49), which are associated with $\Gamma'(A_G)$ and $\Gamma'(A_D)$ respectively. The fact that $\Gamma'(A_G)$ and $\Gamma'(A_D)$ are oblivious implies that for any $g_1, g_2 \in G^\# \cup \{e\}$

$$g_1g_2 = e \in \Gamma'(A_G) \iff g_1 = g_2 = e \text{ or } g_1g_2 \in P_G,$$

and for any $h_1, h_2 \in H^\# \cup \{e\}$

$$h_1h_2 = e \in \Gamma'(A_D) \iff h_1 = h_2 = e \text{ or } h_1h_2 \in P_D,$$

Then, in the free product of the two solution groups with amalgamation, which is Γ, for any $g \in G^\#$ and $h \in H^\#$,

$$gh = e \text{ in } \Gamma \iff g = t_1, h = t_{D,1} \text{ or } g = t_2, h = t_{D,2};$$

otherwise, it is nontrivial by the free product. Define

$$O_\Gamma := \{e\} \sqcup G^\# \sqcup H^\#,$$

then, in Γ, for any $g, h \in O_\Gamma$,

$$gh = e \text{ in } \Gamma \iff g = h = e \text{ or } gh \in P_G \cup P_D \cup P_t.$$

Hence, Γ is oblivious.

By Lemma 4.3 we know $\hat{\Gamma} = \Gamma'(\hat{A})$ is also oblivious. For the new linear system $A_t\boldsymbol{x} = 0$, we denote the set of newly introduced generators by T and denote the set of newly introduced relations by $\hat{P}$. For simplicity, we also write

$$P_\Gamma = P_G \sqcup P_D \sqcup P_t.$$

The fact that $\hat{\Gamma}$ is oblivious implies that for any $g, h \in O_\Gamma \sqcup T$,

$$gh = e \text{ in } \hat{\Gamma} \iff g = h = e \text{ or } gh \in P_\Gamma \sqcup \hat{P}$$

Considering that

$$(P_\Gamma \cup \{(t_1t_2)^{2p(n)}\}) \subset \langle P_\Gamma \sqcup \hat{P} \rangle$$

and that, for any $g, h \in O_\Gamma$, $gh = e$ in $\Gamma / \langle (t_1t_2)^{2p(n)} \rangle$ implies that $gh = e$ in $\hat{\Gamma}$, we know

$$gh = e \text{ in } \Gamma / \langle (t_1t_2)^{2p(n)} = e \rangle \iff g = h = e \text{ or } gh \in P_\Gamma \text{ or } gh = (t_1t_2)^{2p(n)}.$$

So we can conclude that $\Gamma / \langle (t_1t_2)^{2p(n)} = e \rangle$ is also oblivious. □

Next, we construct the correlation C_n. For the linear system $A\boldsymbol{x} = 0$, we define

$$I_i = \{k \in [n] \mid A(i,k) = 1\} \text{ for } i \in [m];$$

and redefine

$$O_\Gamma = \{e\} \cup \bigcup_{i \in [m]} \{g_{i,k} \mid A(i,k) = 1\}.$$

Also, define

$$F := G_0 * \ldots * G_{m-1} * \langle g_m : g_m^4 = e \rangle * \langle g_{m+1} : g_{m+1}^3 = e \rangle * \langle g_{m+2} : g_{m+2}^3 = e \rangle$$

We define $O := O_\Gamma \cup \{g_m, g_{m+1}, g_{m+2}, (g_m, t_1), (g_m, t_2)\}$.

The correlations $C_n : (O \cup [m_1]) \times (O \cup [m_1]) \times [8] \times [8] \to \mathbb{K}_0$ [4] are defined below. Note that the size of C_n is fixed and independent of n. The constant M_{qc} in the statement of Theorem 6.9 equals $|O| + m$.

We first define a function $f : F \to \mathbb{C}$. For $g \in F$,

$$f(g) = \begin{cases} 0 & \text{if } g = x \\ 1 & \text{if } g = e \text{ or } g \in P_G \cup P_D \cup P_t \\ 0 & \text{otherwise.} \end{cases}$$

[4]There is a bijection between $O \cup [m]$ and $[|O| + m]$. For a better presentation of C_n and the following proof, we work with $O \cup [m]$

The definition of C_n

Note that f can be extended to a homomorphism on $\mathbb{C}[F]$ linearly, so we can define C_n based on f. When $i, j \in [m]$,

$$C_n(\boldsymbol{x}, \boldsymbol{y}|i, j) = f((\prod_{k \in I_i} \frac{e + (-1)^{\boldsymbol{x}(k)} g_{i,k}}{2})(\prod_{l \in I_j} \frac{e + (-1)^{\boldsymbol{y}(l)} g_{j,l}}{2})).$$

When $i \in [m], g \in O_\Gamma$,

$$C_n(\boldsymbol{x}, y|i, g) = \begin{cases} f((\prod_{k \in I_i} \frac{e+(-1)^{\boldsymbol{x}(k)} g_{i,k}}{2})(\frac{e+(-1)^y g}{2}) & \text{if } y \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

$$C_n(x, \boldsymbol{y}|g, i) = \begin{cases} f((\frac{e+(-1)^x g}{2})(\prod_{k \in I_i} \frac{e+(-1)^{\boldsymbol{y}(k)} g_{i,k}}{2})) & \text{if } x \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

When $g_1, g_2 \in O_\Gamma$,

$$C_n(x, y|g_1, g_2) = \begin{cases} f((\frac{e+(-1)^x g_1}{2})(\frac{e+(-1)^y g_2}{2}) & \text{if } x, y \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

Recall the definitions of $\pi_x^{(a)}$ in eq. (3) to eq. (12). When $i \in \{m, m+1, m+2\}$ and $h \in O_\Gamma$

$$C_n(x, y|g_i, h) = \begin{cases} f(\pi_{i-m}^{(x)}[\frac{e+(-1)^y h}{2}]) & \text{if } i = m, x \in [4], y \in [2] \\ f(\pi_{i-m}^{(x)}[\frac{e+(-1)^y h}{2}]) & \text{if } i \in \{m+1, m+2\}, x \in [3], y \in [2] \\ 0 & \text{otherwise .} \end{cases}$$

$$C_n(x, y|h, g_i) = \begin{cases} f([\frac{e+(-1)^x h}{2}]\pi_{i-m}^{(y)}) & \text{if } i = m, x \in [2], y \in [4] \\ f([\frac{e+(-1)^x h}{2}]\pi_{i-m}^{(y)}) & \text{if } i \in \{m+1, m+2\}, x \in [2], y \in [3] \\ 0 & \text{otherwise .} \end{cases}$$

When $i \in \{m_1, m_1+1, m_1+2\}$ and $j \in [m]$

$$C_n(x, \boldsymbol{y}|g_i, j) = \begin{cases} f(\pi_{i-m}^{(x)}[\prod_{k \in I_j} \frac{e+(-1)^{\boldsymbol{y}(k)} g_{j,k}}{2}]) & \text{if } i = m, x \in [4] \\ f(\pi_{i-m}^{(x)}[\prod_{k \in I_j} \frac{e+(-1)^{\boldsymbol{y}(k)} g_{j,k}}{2}]) & \text{if } i \in \{m+1, m+2\}, x \in [3] \\ 0 & \text{otherwise,} \end{cases}$$

$$C_n(\boldsymbol{x}, y|j, g_i) = \begin{cases} f([\prod_{k \in I_j} \frac{e+(-1)^{\boldsymbol{x}(k)} g_{j,k}}{2}]\pi_{i-m}^{(y)}) & \text{if } i = m, y \in [4] \\ f([\prod_{k \in I_j} \frac{e+(-1)^{\boldsymbol{x}(k)} g_{j,k}}{2}]\pi_{i-m}^{(y)}) & \text{if } i \in \{m+1, m+2\}, y \in [3], \\ 0 & \text{otherwise.} \end{cases}$$

When $g,h \in I' = \{g_m, g_{m+1}, g_{m+2}, (g_m,t_1),(g_m,t_2)\}$, we define a function $\alpha : I' \to I$ by $\alpha(g_m) = 0, \alpha(g_{m+1}) = 1, \alpha(g_{m+2}) = 2, \alpha((g_m,t_1)) = (0,t_1)$ and $\alpha((g_m,t_2)) = (0,t_2)$. Then,

$$C_n(x,y|g,h) = \mathfrak{C}_{2p(n)}(x,y|\alpha(g),\alpha(h)).$$

When $g \in \{g_m, g_{m+1}, g_{m+2}, (g_m,t_1),(g_m,t_2)\}$ and $h \in \{g \in O_\Gamma \mid g = t_1 \text{ in } \Gamma\}$

$$C_n(x,y|g,h) = \mathfrak{C}_{2p(n)}(x,y|\alpha(g),t_1) \qquad C_n(x,y|h,g) = \mathfrak{C}_{2p(n)}(x,y|t_1,\alpha(g)).$$

When $g \in \{g_m, g_{m+1}, g_{m+2}, (g_m,t_1),(g_m,t_2)\}$ and $h \in \{g \in O_\Gamma \mid g = t_2 \text{ in } \Gamma\}$

$$C_n(x,y|g,h) = \mathfrak{C}_{2p(n)}(x,y|\alpha(g),t_2) \qquad C_n(x,y|h,g) = \mathfrak{C}_{2p(n)}(x,y|t_2,\alpha(g)).$$

Lastly, when $i \in [m]$,

$$C_n(\boldsymbol{x},(y_0,y_1)|i,(g_m,t_1)) = f([\prod_{k\in I_j} \frac{e+(-1)^{\boldsymbol{x}(k)}g_{j,k}}{2}]\pi_0^{(y_0)}\frac{e+(-1)^{y_1}t_1}{2})$$

$$C_n((x_0,x_1),\boldsymbol{y}|(g_m,t_1),i) = f(\pi_0^{(x_0)}\frac{e+(-1)^{x_1}t_1}{2}[\prod_{k\in I_j} \frac{e+(-1)^{\boldsymbol{y}(k)}g_{j,k}}{2}])$$

for $x_0, y_0 \in [4]$ and $x_1, y_1 \in [2]$. The values of $C_n(\boldsymbol{x},(y_0,y_1)|i,(g_{m_1},t_2))$ and $C_n((x_0,x_1),\boldsymbol{y}|(g_{m_1},t_2),i)$ are defined analogously.

When $g \in O_\Gamma$,

$$C_n(x,(y_0,y_1)|g,(g_m,t_1)) = \begin{cases} f(\frac{e+(-1)^x g}{2}\pi_0^{(y_0)}\frac{e+(-1)^{y_1}t_1}{2}) & \text{if } x \in [2] \\ 0 & \text{otherwise;} \end{cases}$$

$$C_n((x_0,x_1),y|(g_m,t_1),g) = \begin{cases} f(\pi_0^{(x_0)}\frac{e+(-1)^{x_1}t_1}{2}\frac{e+(-1)^y g}{2}) & \text{if } y \in [2] \\ 0 & \text{otherwise;} \end{cases}$$

for $x_0, y_0 \in [4]$ and $x_1, y_1 \in [2]$. The values of $C_n(x,(y_0,y_1)|g,(g_{m_1},t_2))$ and $C_n((x_0,x_1),y|(g_{m_1},t_2),g)$ are defined analogously.

Claim 6.11. *For each n, the correlation $C'_n : [m]\times[m]\times[8]\times[8] \to \mathbb{K}_0$ such that $C'_n(\boldsymbol{x},\boldsymbol{y}|i,j) = C_n(\boldsymbol{x},\boldsymbol{y}|i,j)$ for any $(i,j,\boldsymbol{x},\boldsymbol{y}) \in [m]\times[m]\times[8]\times[8]$ is a perfect correlation of $A\boldsymbol{x} = 0$.*

Proof. By the wagon wheel construction, we know that $|I_i| = 3$ and $|I_i \cap I_j| \le 1$ for $i \ne j$ in $\mathsf{LS}(A,0)$. So if $i \ne j$,

$$C_n(\boldsymbol{x},\boldsymbol{y}|i,j) = \begin{cases} \frac{(1+(-1)^{\sum_{k\in I_i}\boldsymbol{x}(k)})(1+(-1)^{\sum_{k\in I_j}\boldsymbol{y}(k)})}{64} & \text{if } I_i \cap I_j = \emptyset \\ \frac{4(-1)^{\boldsymbol{x}(k)+\boldsymbol{y}(k)}+(1+(-1)^{\sum_{l\in I_i}\boldsymbol{x}(l)})(1+(-1)^{\sum_{l\in I_j}\boldsymbol{y}(l)})}{64} & \text{if } I_i \cap I_j = \{k\}, \end{cases}$$

where we have substituted in the definition of f. If $i = j$,

$$C_n(\boldsymbol{x},\boldsymbol{x}|i,i) = \frac{1+(-1)^{\sum_{k\in I_i}\boldsymbol{x}(k)}}{8}.$$

It is easy to see that, when $i = j$

$$\sum_{\boldsymbol{x}\in\mathbb{Z}_2^3} C_n(\boldsymbol{x},\boldsymbol{x}|i,i) = 4\cdot\frac{1}{4} = 1 = \sum_{\boldsymbol{x}\in S_i} C_n(\boldsymbol{x},\boldsymbol{x}|i,i),$$

when $I_i \cap I_j = \emptyset$

$$\sum_{\boldsymbol{x}\in S_i}\sum_{\boldsymbol{y}\in S_j} C_n(\boldsymbol{x},\boldsymbol{y}|i,j) = 16\cdot\frac{1}{16} = 1,$$

and when $I_i \cap I_j = \{k\}$

$$\sum_{\boldsymbol{x}\in S_i,\boldsymbol{y}\in S_j,\boldsymbol{x}(k)=\boldsymbol{y}(k)} C_n(\boldsymbol{x},\boldsymbol{y}|i,j) = 4\cdot 2\cdot\frac{1}{8} = 1,$$

which completes the proof. □

We extend $\alpha : I' \to I$ to $\alpha : I' \cup \{t_1, t_2\} \to I$ by setting $\alpha(t_1) = t_1$ and $\alpha(t_2) = t_2$.

Claim 6.12. *When $x, y \in I' \cup \{t_1, t_2\}$,*

$$C_n(a, b|x, y) = \mathfrak{C}_{2p}(a, b|\alpha(x), \alpha(y))$$

for all n and $a, b \in [8]$.

Proof of Theorem 6.9

Proof. When $n \in X$, assume $C_n \in C^s_{qc}(M_{qc}, 8)$. Then there exists an commuting-operator inducing 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 $x > 1$,

$$M_g^{(x)}|\psi\rangle = N_g^{(x)}|\psi\rangle = 0.$$

Then we can construct the 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

$$M(g)^2|\psi\rangle = (M_g^{(0)} + M_g^{(1)})|\psi\rangle = \sum_{j\in[8]} M_g^{(j)}|\psi\rangle = |\psi\rangle$$
$$N(g)^2|\psi\rangle = (N_g^{(0)} + N_g^{(1)})|\psi\rangle = \sum_{j\in[8]} N_g^{(j)}|\psi\rangle = |\psi\rangle.$$

Moreover, we know that $\langle\psi|M(x)|\psi\rangle = 0$.

Since S can induce a perfect correlation of $A\boldsymbol{x} = 0$ (Claim 6.11), by Lemmas 6.3 and 6.5, we know that, for $g, g' \in O_\Gamma$,

$$\langle\psi|M(g)M(g')|\psi\rangle = 1 \iff gg' \in P_G \cup P_D \cup P_t.$$

Since D is embedded in Γ, assuming $\phi(u) = (u_1u_2)^2$, we know

$$(M(t_1)M(t_2))^2(M(u_1)M(u_2))^2|\psi\rangle = (M(u_1)M(u_2))^2(M(t_1)M(t_2))^{2r}|\psi\rangle$$
$$(N(t_1)N(t_2))^2(N(u_1)N(u_2))^2|\psi\rangle = (N(u_1)N(u_2))^2(N(t_1)N(t_2))^{2r}|\psi\rangle.$$

Define $U_A = (M(u_1)M(u_2))^2$ and $U_B = (N(u_1)N(u_2))^2$, then these two unitaries satisfy the conditions of Theorem 6.8. Considering that S can induce $\mathfrak{C}_{2p(n)}$ as shown in Claim 6.12, we can use Theorem 6.8 to conclude that

$$(M(t_1)M(t_2))^{2p(n)}|\psi\rangle = |\psi\rangle.$$

By [CLS17, Lemma 8], we know that there exists a Hilbert space $\mathcal{H}_0$, such that for $g, g' \in O_\Gamma$,

$$(M(g)|_{\mathcal{H}_0})^2 = \mathbb{1}_{\mathcal{H}_0}$$
$$M(g)|_{\mathcal{H}_0}M(g')|_{\mathcal{H}_0} = \mathbb{1}_{\mathcal{H}_0} \iff gg' \in P_G \cup P_D \cup P_t,$$

where $M(g)|_{\mathcal{H}_0}$ denotes the linear operator for the actions of $M(g)$ restricted to $\mathcal{H}_0$, and that

$$(M(t_1)|_{\mathcal{H}_0}M(t_2)|_{\mathcal{H}_0})^{2p(n)} = \mathbb{1}_{\mathcal{H}_0}.$$

Hence, $\phi : \Gamma/\langle(t_1t_2)^{2p(n)} = e\rangle \to \mathcal{U}(\mathcal{H}_0)$ defined by $\phi(g) = M(g)|_{\mathcal{H}_0}$ is a representation of $\Gamma/\langle(t_1t_2)^{2p(n)} = e\rangle$. However, by Claim 6.10, when $n \in X$, $x = e$ in $\Gamma/\langle(t_1t_2)^{2p(n)} = e\rangle$. By the construction of $\mathcal{H}_0$, we know $M(x)|\psi\rangle \neq |\psi\rangle$, 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 is not in $C^s_{qc}(M_{qc}, 8)$.

When $n \in X$, by Claim 6.10, $x \neq e$ in $\Gamma/\langle(t_1t_2)^{2p(n)} = e\rangle$. We can construct a strategy based on the left and right regular representations of $\Gamma/\langle(t_1t_2)^{2p(n)} = e\rangle$, denoted by L and R respectively.

The shared state is $|e\rangle \in \ell^2\Gamma/\langle(t_1t_2)^{2p(n)} = e\rangle$. The projectors are the following. For question $g \in O_\Gamma$, Alice and Bob's projectors are

$$\tilde{P}_g^{(x)} = \begin{cases} \frac{R(e)+(-1)^x R(g)}{2} & \text{if } x \in [2] \\ 0 & \text{otherwise,} \end{cases}$$
$$\tilde{Q}_g^{(y)} = \begin{cases} \frac{L(e)+(-1)^y L(g)}{2} & \text{if } y \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

For question $i \in [m]$, Alice and Bob's projectors are

$$\tilde{P}_i^{(\boldsymbol{x})} = \prod_{k \in I_i} \frac{R(e) + (-1)^{\boldsymbol{x}(k)} R(g_{i,k})}{2},$$
$$\tilde{Q}_i^{(\boldsymbol{x})} = \prod_{k \in I_i} \frac{L(e) + (-1)^{\boldsymbol{x}(k)} L(g_{i,k})}{2}.$$

For question g_m, Alice and Bob's projectors are

$$\tilde{P}_{g_m}^{(a)} = \begin{cases} R(\pi_0^{(a)}) & \text{if } a \in [4] \\ 0 & \text{otherwise,} \end{cases}$$
$$\tilde{Q}_{g_m}^{(a)} = \begin{cases} L(\pi_0^{(a)}) & \text{if } a \in [4] \\ 0 & \text{otherwise,} \end{cases}$$

where $\pi_0^{(a)}$ are defined in eq. (3) to eq. (6). For questions g_{m+1} and g_{m+2}, Alice and Bob's projectors are

$$\tilde{P}_{g_{m+1}}^{(a)} = R(\pi_1^{(a)}) \qquad \tilde{P}_{g_{m+2}}^{(a)} = R(\pi_2^{(a)})$$
$$\tilde{Q}_{g_{m+1}}^{(a)} = L(\pi_1^{(a)}) \qquad \tilde{Q}_{g_{m+2}}^{(a)} = L(\pi_2^{(a)}),$$

for $a \in [3]$, otherwise, $\tilde{P}_{g_{m+1}}^{(x)} = \tilde{Q}_{g_{m+1}}^{(x)} = \tilde{P}_{g_{m+2}}^{(x)} = \tilde{Q}_{g_{m+2}}^{(x)} = 0$. The elements $\pi_x^{(a)}$ are defined in eq. (7) to eq. (12). For question (g_m, t_1) and (g_m, t_2), Alice and Bob's projectors are

$$\tilde{P}_{(g_m,t_1)}^{(a_0,x_1)} = \tilde{P}_{g_m}^{(a_0)} \tilde{P}_{t_1}^{(a_1)} \qquad \tilde{P}_{(g_m,t_2)}^{(a_0,x_1)} = \tilde{P}_{g_m}^{(a_0)} \tilde{P}_{t_2}^{(a_1)}$$
$$\tilde{Q}_{(g_m,t_1)}^{(b_0,b_1)} = \tilde{Q}_{g_m}^{(b_0)} \tilde{Q}_{t_1}^{(b_1)} \qquad \tilde{Q}_{(g_m,t_2)}^{(b_0,b_1)} = \tilde{Q}_{g_m}^{(b_0)} \tilde{P}_{t_2}^{(b_1)},$$

for $a_0, b_0 \in [4]$ and $a_1, b_1 \in [2]$. So the inducing commuting-operator strategy of C_n is

$$S_{qc} = (|e\rangle, \{\{\tilde{P}_x^{(a)} \mid a \in [8]\} \mid x \in O \cup [m]\}, \{\{\tilde{Q}_y^{(b)} \mid b \in [8]\} \mid y \in O \cup [m]\}).$$

To see that S_{qc} can induce a perfect correlation of the $A\boldsymbol{x} = 0$, we can use the fact that

$$\langle e|R(g_{i,k})L(g_{j,l})|e\rangle = \langle e|g_{j,l}g_{i,k}\rangle = 1 \iff g_{j,l}g_{i,k} \in P_G \cup P_D \cup P_t.$$

To see that S_{qc} can induce the correlation $\mathfrak{C}_{2p(n)}$, we can use the fact that $D_{2p(n)} \leq \Gamma / \langle (t_1 t_2)^{2p(n)} = e \rangle$. □

Corollary 6.13. *There exist constants N_0 and M_0 such that, for any $N \geq N_0$ and $M \geq M_0$, $(Membership(N, N, M, M)^s_{\mathbb{K}_0,qc})$is* coRE*-complete.*

Proof. By Proposition 5.4, the group G defined in eq. (2) satisfies the conditions of Theorem 6.9. Then, there exists a constant N_0 and a set of correlations $\{C_n\} \subset \mathbb{K}_0^{N_0^2 \times 8^2}$ such that $C_n \in C^s_{qc}(N_0, 8)$ if and only if $n \notin X$. So, the membership problem of $C^s_{qc}(N_0, 8)$ over $\mathbb{K}_0$ is coRE-hard.

On the other hand, it is known that Section 7 is in coRE [NPA08]. Hence, (Membership$(N$, N, M, $M)^s_{\mathbb{K}_0,qc}$) is coRE-complete for $N \geq N_0$ and $M \geq 8$. □

7 Membership problem of constant-sized quantum-approximable correlations

This section is devoted to proving the Membership problem of $C_{qa}^{s}(N,M)$ over $\mathbb{K}$, defined below, is coRE-hard.

Problem (Membership$(N,N,M,M)_{\mathbb{K},qa}^{s}$)**.** *Given a correlation $P \in \mathbb{K}^{N^2 \times M^2}$ for some constants N and M, decide if $P \in C_{qa}^{s}(N,M)$.*

We study the hardness of this problem by studying a problem with equivalent hardness.

Problem (Intersection$(N,N,M,M)_{\mathbb{K},qa}^{s}$)**.** *Given a set of correlations $F \subset \mathbb{K}^{N^2 \times M^2}$ such that $|F| = K$ for some constants N, M and K, decide if $F \cap C_{qa}^{s}(N,M) \neq \emptyset$.*

Proposition 7.1. *For fixed constants N and M, $(Intersection(N,N,M,M)_{\mathbb{K},qa}^{s})$ is as hard as $(Membership(N,N,M,M)_{\mathbb{K},qa}^{s})$.*

Proof. If we have a decider D_m for (Membership$(N,N,M,M)_{\mathbb{K},qa}^{s}$), we can use it to construct a decider D_i for (Intersection$(N,N,M,M)_{\mathbb{K},qa}^{s}$) 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 $C_{qa}^{s}(N,M)$. Since there are only a constant-number of members of F, the overhead is constant.

If we have a decider D_i' for (Intersection$(N,N,M,M)_{\mathbb{K},qa}^{s}$), we can use it to construct a decider D_m' for (Membership$(N,N,M,M)_{\mathbb{K},qa}^{s}$) 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. □

The main result of this section is Theorem 7.8. In the proof of Theorem 7.8, we will embed a group of the form $G/\langle t^p = e\rangle$ into $\Gamma/\langle (t_1t_2)^p = e\rangle$ following the fa^*-embedding procedure. 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.

7.1 The correlation $\mathfrak{C}_p$ for D_p

Recall that, for a prime p, the Dihedral group of order $2p$ is defined by $D_p = \langle t_1, t_2 : t_1^2 = t_2^2 = (t_1t_2)^p = e\rangle$. In this section, we introduce a correlation $\mathfrak{C}_p$ that can certify the relation $(t_1t_2)^p = e$. For this reason, we include symbols t_1 and t_2 in the input set I of $\mathfrak{C}_p$, where

$$I := \{0, 1, 2, t_1, t_2, (0, t_1), (0, t_2)\}.$$

The correlation $\mathfrak{C}_p : I \times I \times [6] \times [6] \to \mathbb{K}_0$ is defined by a commuting-operator strategy. Note that $\mathfrak{C}_p$ is different from $\mathfrak{C}_{2p}$ because the structure of the regular representation of t_1t_2 in D_p is different in D_{2p}.

The inducing strategy of $\mathfrak{C}_p$ is denoted by

$$\tilde{S} = (|\tilde{\psi}\rangle, \{\{\tilde{P}_x^{(a)} \mid x \in I\} \mid a \in [6]\}, \{\{\tilde{Q}_y^{(b)} \mid y \in I\} \mid b \in [6]\}).$$

Recall that the vector space

$$L^2 D_p = \text{span}(\{|(t_1 t_2)^j\rangle, |t_2(t_1 t_2)^j\rangle \mid j \in [p]\})$$

The inducing strategy is based on the left and right regular representations of D_p, which are $L : D_p \to \mathcal{U}(L^2 D_p)$ and $R : D_p \to \mathcal{U}(L^2 D_p)$.

We first define $|\tilde{\psi}\rangle := |e\rangle$. Next we define some idempotent elements of $\mathbb{C}[D_p]$.

$$\pi_0^{(0)} = \frac{1}{p} \sum_{j \in [p]} (t_1 t_2)^j \tag{50}$$

$$\pi_0^{(1)} = \frac{2}{p} \sum_{j \in [p]} \cos(\frac{2j\pi}{p})(t_1 t_2)^j \tag{51}$$

$$\pi_0^{(2)} = e - \pi_0^{(0)} - \pi_0^{(1)} \tag{52}$$

$$\pi_1^{(0)} = \frac{1}{2}\pi_0^{(1)} + \frac{1}{p} \sum_{j \in [p]} \cos(\frac{(2j+1)\pi}{p}) t_2 (t_1 t_2)^j \tag{53}$$

$$\pi_1^{(1)} = \pi_0^{(1)} - \pi_1^{(0)} \tag{54}$$

$$\pi_1^{(2)} = e - \pi_0^{(1)} \tag{55}$$

$$\pi_2^{(0)} = \frac{1}{2}\pi_0^{(1)} + \frac{1}{p} \sum_{j \in [p]} \sin(\frac{(2j+1)\pi}{p}) t_2 (t_1 t_2)^j \tag{56}$$

$$\pi_2^{(1)} = \pi_0^{(1)} - \pi_2^{(0)} \tag{57}$$

$$\pi_2^{(2)} = e - \pi_0^{(1)}. \tag{58}$$

Then we define the projectors used by Alice and Bob.

- For the input 0,

$$\tilde{P}_0^{(a)} = \begin{cases} R(\pi_0^{(a)}) & \text{if } a \in [3] \\ 0 & \text{otherwise;} \end{cases}$$

$$\tilde{Q}_0^{(b)} = \begin{cases} L(\pi_0^{(b)}) & \text{if } b \in [3] \\ 0 & \text{otherwise.} \end{cases}$$

- For the inputs $x, y \in \{1, 2\}$,

$$\tilde{P}_x^{(a)} = \begin{cases} R(\pi_x^{(a)}) & \text{if } a \in [3] \\ 0 & \text{otherwise;} \end{cases}$$

$$\tilde{Q}_y^{(b)} = \begin{cases} L(\pi_y^{(b)}) & \text{if } b \in [3] \\ 0 & \text{otherwise.} \end{cases}$$

- For the inputs $x, y \in \{t_1, t_2\}$

$$\tilde{P}_x^{(a)} = \begin{cases} \frac{R(e)+(-1)^a R(x)}{2} & \text{if } a \in [2] \\ 0 & \text{otherwise;} \end{cases}$$
$$\tilde{Q}_y^{(b)} = \begin{cases} \frac{L(e)+(-1)^b L(y)}{2} & \text{if } b \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

- For the inputs $(0, x)$ and $(0, y)$ with $x, y \in \{t_1, t_2\}$

$$\tilde{P}_{(0,x)}^{(a_0,a_1)} = \tilde{P}_0^{(a_0)} \tilde{P}_x^{(a_1)} \qquad \text{with } a_0 \in [3], a_1 \in [2],$$
$$\tilde{Q}_{(0,y)}^{(b_0,b_1)} = \tilde{Q}_0^{(b_0)} \tilde{Q}_y^{(b_1)} \qquad \text{with } b_0 \in [3], b_1 \in [2].$$

Note that the fact that $\tilde{P}_0^{(a)}$ commutes with $\tilde{P}_x^{(a)}$ for $x \in \{t_1, t_2\}$ follows from the observation that

$$R(t_1)R((t_1t_2)^j)R(t_1) = R((t_1t_2)^{-j}) \qquad R(t_2)R((t_1t_2)^j)R(t_2) = R((t_1t_2)^{-j})$$

for each $j \in [p]$. With similar reasoning, we get that $\tilde{Q}_0^{(b)}$ commutes with $\tilde{Q}_y^{(b)}$ for $y \in \{t_1, t_2\}$.

Definition 7.2. *The correlation $\mathfrak{C}_p : I \times I \times [6] \times [6] \to \mathbb{K}_0$, is defined by*

$$\mathfrak{C}_p(a, b|x, y) = \langle \tilde{\psi}|\tilde{P}_x^{(a)} \tilde{Q}_y^{(b)}|\tilde{\psi}\rangle.$$

Since $\mathfrak{C}_p$ is induced by $\tilde{S}$, the next claim is immediate.

Claim 7.3. *The correlation $\mathfrak{C}_p$ is in $C_{qc}^s(7, 6)$.*

The importance of $\mathfrak{C}_p$ is summarized in the following theorem.

Theorem 7.4. *If a commuting-operator strategy $S = (|\psi\rangle, \{M_x^{(a)}\}, \{N_y^{(b)}\})$ can induce $\mathfrak{C}_p$ 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*

$$U_A U_B|\psi\rangle = |\psi\rangle$$
$$(N_{t_1} N_{t_2})U_B|\psi\rangle = U_B(N_{t_1} N_{t_2})^r|\psi\rangle$$
$$(M_{t_1} M_{t_2})U_A|\psi\rangle = U_A(M_{t_1} M_{t_2})^r|\psi\rangle,$$

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

$$(M_{t_1} M_{t_2})^p|\psi\rangle = |\psi\rangle.$$

The proof of this theorem is very similar to that of Theorem 6.8. The basic idea is to find a decomposition of $|\psi\rangle$ as $|\psi\rangle = \sum_{j=0}^{p} |\psi_j\rangle$, 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 $1 \leq j \leq (p-1)/2$. The proof of this theorem can be found in Appendix A.

7.2 Approximation tools

In the next subsection, we need some approximation techniques to construct an approximate strategy of a quantum correlation based on some approximation representation of a group. Therefore, we first present these techniques in this subsection.

We work with the *normalized Hilbert-Schmidt norm* and the *operator norm* of a linear operator. For a matrix $M \in \mathcal{L}(\mathbb{C}^d)$ for some integer $d \geq 1$, its *normalized trace* is $\tilde{\mathrm{Tr}}(M) = \mathrm{Tr}(M)/d$; its *normalized Hilbert-Schmidt norm* is

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

and 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 paper is summarized in the following lemma, for which we omit the proof.

Lemma 7.5. *For $A, B \in \mathcal{L}(\mathbb{C}^d)$,*

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

In the next proposition, we first show that any unitary can be approximated by another unitary of integer order.

Proposition 7.6. *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 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

$$\begin{aligned}
f'(x) &= (1 + \frac{1}{n})\sin(nx) - \sin(x) \\
f''(x) &= (n+1)\cos(nx) - \cos(x).
\end{aligned}$$

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 $f(\pi/n)$,

$$\begin{aligned}
&f(0) = 0, \\
&f(\pi/n) = 2(\frac{1}{n} + \frac{1}{n^2}) - (1 - \cos(\pi/n)) \geq \frac{2n+2}{n^2} - \frac{\pi^2}{2n^2} \geq 0,
\end{aligned}$$

which is because $2n + 2 \geq 6$ and $\pi^2/2 < 5$, and we complete the proof. □

Proposition 7.7. *Let $\{P_i \mid i \in [n]\} \subset \mathcal{L}(\mathbb{C}^d)$ be a set of matrices such that*

$$\|P_i\|_{op} \leq c \qquad \|P_i^2 - P_i\| \leq \epsilon \qquad \|P_iP_j\| \leq \epsilon \qquad \sum_{i \in [n]} P_i = \mathbb{1},$$

for $i, j \in [n]$ and $i \neq j$ and a constant c. 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

$$\|P_i^n - P_i\| \le \sum_{j=1}^{n-1} \|P_i^{j+1} - P_i^j\| \le \sum_{j=1}^{n-1} \|P_i^2 - P_i\| \|P_i^{j-1}\|_{op} \le c^{n-1}\epsilon,$$

for any $i \in [n]$, and for any $(j_0, j_1, \ldots, j_{n-1})$ with $l \in [n-1]$ such that $j_l \neq j_{l+1}$,

$$\|\prod_{k\in[n]} P_{j_k}\| \le \prod_{k\in[l]} \|P_{j_k}\|_{op} \|P_{j_l} P_{j_{l+1}}\| \prod_{l+1<k<n} \|P_{j_k}\|_{op} \le c^{n-2}\epsilon$$

Let $O = \sum_{i\in[n]} \omega_n^i P_i$, then

$$\begin{aligned}
&\|O\|_{op} \le \sum_{i\in[n]} |\omega_n^i| \|P_i\|_{op} \le cn, \\
&\|O^j - \sum_{i\in[n]} \omega_n^{ji} P_i\| \\
=&\| \sum_{i_0,\ldots i_{j-1}\in[n]} \left(\omega_n^{\sum_{k\in[j]} i_k} \prod_{k\in[j]} P_{i_k} \right) - \sum_{i\in[n]} \omega_n^{ji} P_i \| \\
\le&[(n^j - n)c^{n-2} + nc^{n-1}]\epsilon \le n^j c^{n-1}\epsilon,
\end{aligned}$$

and in particular

$$\|O^n - \mathbb{1}\| \le n^n c^{n-1}\epsilon.$$

By the previous proposition, we can construct a unitary $\hat{O}$ such that $\hat{O}^n = \mathbb{1}$ and

$$\|\hat{O} - O\| \le \frac{\sqrt{n+1}}{n} \|O^n - \mathbb{1}\| \le \sqrt{n+1}(cn)^{n-1}\epsilon.$$

Then it can be checked that

$$\|\hat{O}^j - O^j\| \le \sum_{k\in[j-1]} \|\hat{O}\|_{op}^k \|\hat{O} - O\| \|O\|_{op}^{j-k-1} \le (cn)^j \|\hat{O} - O\|.$$

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

$$\begin{aligned}
\|\Pi_i - P_i\| \le& \frac{1}{n} \| \sum_{j\in[n]} \omega_n^{-ij} (\hat{O}^j - O^j) \| + \frac{1}{n} \| \sum_{j\in[n]} \omega_n^{-ij} (O^j - \sum_{k\in[n]} \omega_n^{jk} P_k) \| \\
\le& \frac{1}{n} \sum_{j\in[n]} (cn)^j \|\hat{O} - O\| + \frac{1}{n} \sum_{j\in[n]} n^j c^{n-1}\epsilon \\
\le& (cn)^{2n-1}\epsilon,
\end{aligned}$$

for each $i \in [n]$. □

7.3 Proof of undecidability

Theorem 7.8. *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 a generator t and an involutary generator x such that $G/\langle t^{p(n)} = e\rangle$ is sofic and

$$x = e \text{ in } G/\langle t^{p(n)} = e\rangle \iff n \in X. \tag{59}$$

Then, there exist constants N_{qa} and M_{qa}, which only depend on the presentation of G and r, and a family of sets of correlations $\{F_n \mid n > 0\}$ where $F_n = \{C_{n,i} \mid i \in [N_{qa}]\} \subset \mathbb{K}_0^{M_{qa}^2 \times 8^2}$ such that $F_n \cap C_{qa}^s(M_{qa}, 8) = \emptyset$ if and only if $n \in X$.

The proof of Theorem 7.8 is based on the fa^*-embedding procedure introduced in Propositions 4.9 and 4.10. and we first prove several claims leading to the proof.

To define F_n, we first extend G and embed it into a solution group. Define

$$D := \langle u, t_D : u^{-1} t_D u = t_D^r \rangle$$
$$K := (G * D)/\langle t = t_D \rangle.$$

Claim 7.9. *$K/\langle t^{p(n)} = e\rangle$ 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 $\langle t_1, t_2 : t_1^2 = t_2^2 = e\rangle \cong \mathbb{Z}_2 * \mathbb{Z}_2$, which is solvable because $\mathbb{Z}_2$ is abelian. Next, we show that D is an HNN-extension of $\mathbb{Z}_2 * \mathbb{Z}_2$. Define $\phi : \mathbb{Z}_2 * \mathbb{Z}_2 \to \mathbb{Z}_2 * \mathbb{Z}_2$ by

$$\phi(t_1 t_2) = (t_1 t_2)^r,$$
$$\phi(t_2) = t_2.$$

Then, we can deduce that $\phi(t_1) = \phi(t_1 t_2 t_2) = (t_1 t_2)^{r-1} t_1$. It can be checked that

$$\phi(t_1) = \begin{cases} t_1 t_2 t_1 & \text{if } r = 2 \\ t_1(t_2 t_1 t_2) t_1 & \text{if } r = 3 \\ t_1(t_2(t_1(t_2 t_1 t_2) t_1) t_2) t_1 & \text{if } r = 5, \end{cases}$$

which implies that $\phi(t_1)^2 = \phi(t_2)^2 = e$. So ϕ is an isomorphism of $\mathbb{Z}_2 * \mathbb{Z}_2$. Since $D \cong \langle \mathbb{Z}_2 * \mathbb{Z}_2, u : u^{-1} t_1 u = \phi(t_1), u^{-1} t_2 u = \phi(t_2)\rangle$ is an HNN-extension of $\mathbb{Z}_2 * \mathbb{Z}_2$, by [CLP15, Propositiin II.4.1], we know D is sofic.

Because $G/\langle t^{p(n)} = e\rangle$ is sofic, by [CLP15, Propositiin II.4.1], 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, 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 $n \in X$. □

Next, we can construct a solution group Γ, wherein K is embedded. Applying the fa^*-embedding procedure to the group K, we can construct an $m \times n$ binary linear system $A\boldsymbol{x} = 0$. Then,

$$\Gamma = \Gamma'(A) = \frac{G_0 * G_1 * \ldots * G_{m-1}}{\langle P_\Gamma \rangle},$$

where

$$G_i = \langle \{g_{i,k} \mid k \in I_i\} : \{g_{i,k}^2 = [g_{i,k}, g_{i,l}] = \prod_{k \in I_i} g_{i,k} = e \mid k, l \in I_i\} \rangle,$$
$$P_\Gamma = \{g_{i,k} g_{j,k} \mid i, j \in [m],\ k \in I_i \cap I_j\}.$$

Denote the fa^*-embedding of K into Γ by ϕ, then there exist $i_0, i_1, i_2 \in [m]$ and $k_0 \in I_{i_0}, k_1 \in I_{i_1}, k_2 \in I_{i_2}$ such that

$$\phi(x) = g_{i_0,k_0} \qquad \phi(t) = g_{i_1,k_1} g_{i_2,k_2}.$$

For simplicity, from now on, we write $\phi(x) = x$ and $\phi(t) = t_1 t_2$.

Claim 7.10. *Denote the natural homomorphism mapping $K/\langle t^{p(n)} = e\rangle$ to $\Gamma/\langle \phi(t)^{p(n)} = e\rangle$ induced by ϕ 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. Given an ϵ-representation ρ of K, the fa^*-embedding procedure gives us an ϵ-representation σ of Γ such that ρ is a direct summand of $\sigma \circ \phi$. If ρ is also an ϵ-representation of $K/\langle t^{p(n)} = e\rangle$ meaning that $\|\rho(t)^{p(n)} - \mathbb{1}\| \le \epsilon$, then we know

$$\sigma(\phi'(t)) = (\rho(t) \oplus \rho(t)) \otimes \mathbb{1}_{\mathbb{C}^{k_0}} \oplus (\rho(t) \oplus \overline{\rho(t)}) \oplus \mathcal{I}_{\mathbb{C}^{k_1}}$$

for some constants k_0 and k_1 depending on the presentation of G. Hence, $\|\sigma(\phi'(t))^{p(n)} - \mathbb{1}\| \le \epsilon$ and σ is an ϵ-approximate representation of $\Gamma/\langle \phi(t)^{p(n)} = e\rangle$. By Lemma 4.8, we know ϕ' is an fa^*-embedding and the statement of the claim follows. □

The family of correlations F_n

Define a group

$$F := G_0 * \ldots * G_{m-1} * \langle g_m : g_m^3 = e\rangle * \langle g_{m+1} : g_{m+1}^3 = e\rangle * \langle g_{m+2} : g_{m+2}^3 = e\rangle.$$

and sets: $O_\Gamma^\# = \{g_{i,k} \mid i \in [m], k \in I_i\}$, $O_\Gamma = \{e\} \cup O_\Gamma^\#$,

$$W_2 = O_\Gamma^\# \times O_\Gamma^\#$$
$$W' = \{w \mid w \in W_2 \text{ and } w = e \text{ or } w = x \text{ in } F\} \cup P_\Gamma$$
$$W = O_\Gamma^\# \cup (W_2 \setminus W').$$

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 $f_{\boldsymbol{z}} : F \to \{0,1\}$ for each $\boldsymbol{z} \in \mathbb{Z}_2^{|W|}$.

$$f_{\boldsymbol{z}}(g) = \begin{cases} 1 & \text{if } g = e \text{ or } g \in P_\Gamma \\ 0 & \text{if } g = x \\ \boldsymbol{z}(g) & \text{if } g \in W \\ 0 & \text{otherwise.} \end{cases}$$

Then, as $f_{\boldsymbol{z}}$ can be extended to a function on $\mathbb{C}[F]$ linearly, based on $f_{\boldsymbol{z}}$, we can define $C_{n,\boldsymbol{z}} : (O \cup [m]) \times (O \cup [m]) \times [8] \times [8] \to \mathbb{K}_0$, for $\boldsymbol{z} \in Z$, where

$$O = O_\Gamma \cup \{g_m, g_{m+1}, g_{m+2}, (g_m, t_1), (g_m, t_2)\}.$$

The constant M_{qa} in the statement of Theorem 6.9 equals $|O| + m$. Recall the idempotent elements defined in eq. (50) to eq. (58)

- When $i, j \in [m]$,

$$C_{n,\boldsymbol{z}}(\boldsymbol{x}, \boldsymbol{y}|i,j) = f_{\boldsymbol{z}}((\prod_{k \in I_i} \frac{e + (-1)^{\boldsymbol{x}(k)} g_{i,k}}{2})(\prod_{l \in I_j} \frac{e + (-1)^{\boldsymbol{y}(l)} g_{j,l}}{2})).$$

- When $i \in [m], g \in O_\Gamma$,

$$C_{n,\boldsymbol{z}}(\boldsymbol{x}, y|i,g) = \begin{cases} f_{\boldsymbol{z}}((\prod_{k \in I_i} \frac{e+(-1)^{\boldsymbol{x}(k)} g_{i,k}}{2})(\frac{e+(-1)^y g}{2})) & \text{if } y \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

$$C_{n,\boldsymbol{z}}(x, \boldsymbol{y}|g,i) = \begin{cases} f_{\boldsymbol{z}}((\frac{e+(-1)^x g}{2})(\prod_{k \in I_i} \frac{e+(-1)^{\boldsymbol{y}(k)} g_{i,k}}{2})) & \text{if } x \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

- When $g_1, g_2 \in O_\Gamma$,

$$C_{n,\boldsymbol{z}}(x, y|g_1, g_2) = \begin{cases} f_{\boldsymbol{z}}((\frac{e+(-1)^x g_1}{2})(\frac{e+(-1)^y g_2}{2})) & \text{if } x, y \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

- When $i \in \{m, m+1, m+2\}$ and $h \in O_\Gamma$

$$C_{n,\boldsymbol{z}}(x, y|g_i, h) = \begin{cases} f_{\boldsymbol{z}}(\pi_i^{(x)} \frac{e+(-1)^y h}{2}) & \text{if }, x \in [3], y \in [2] \\ 0 & \text{otherwise .} \end{cases}$$

$$C_{n,\boldsymbol{z}}(x, y|h, g_i) = \begin{cases} f_{\boldsymbol{z}}(\frac{e+(-1)^x h}{2} \pi_i^{(y)}) & \text{if }, x \in [2], y \in [3] \\ 0 & \text{otherwise .} \end{cases}.$$

- When $i \in \{m, m+1, m+2\}$ and $j \in [m]$

$$C_{n,\boldsymbol{z}}(x, \boldsymbol{y}|g_i, j) = \begin{cases} f_{\boldsymbol{z}}(\pi_{i-m}^{(x)}[\prod_{k \in I_j} \frac{e+(-1)^{\boldsymbol{y}(k)} g_{j,k}}{2}]) & \text{if } x \in [3] \\ 0 & \text{otherwise,} \end{cases}$$

$$C_{n,\boldsymbol{z}}(\boldsymbol{x}, y|j, g_i) = \begin{cases} f_{\boldsymbol{z}}([\prod_{k \in I_j} \frac{e+(-1)^{\boldsymbol{x}(k)} g_{j,k}}{2}]\pi_{i-m}^{(y)}) & \text{if } y \in [3] \\ 0 & \text{otherwise .} \end{cases}$$

- When $g, h \in I' := \{g_m, g_{m+1}, g_{m+2}, (g_m, t_1), (g_m, t_2)\}$, Fix a bijection $\alpha : I' \to I$ as $\alpha(g_m) = 0$, $\alpha(g_{m+1}) = 1$, $\alpha(g_{m+2}) = 2$, $\alpha((g_m, t_1)) = (0, t_1)$ and $\alpha((g_m, t_2)) = (0, t_2)$.

$$C_{n,\boldsymbol{z}}(x, y|g, h) = \begin{cases} \mathfrak{C}_{p(n)}(x, y|\alpha(g), \alpha(h)) & \text{if } x, y \in [6] \\ 0 & \text{otherwise.} \end{cases}$$

- When $g \in I' = \{g_m, g_{m+1}, g_{m+2}, (g_m, t_1), (g_m, t_2)\}$ and $h \in \{g \in O_\Gamma \mid g = t_1 \text{ in } \Gamma\}$

$$C_{n,\boldsymbol{z}}(x, y|g, h) = \begin{cases} \mathfrak{C}_{p(n)}(x, y|\alpha(g), t_1) & \text{if } x, y \in [6] \\ 0 & \text{otherwise,} \end{cases}$$

$$C_{n,\boldsymbol{z}}(x, y|h, g) = \begin{cases} \mathfrak{C}_{p(n)}(x, y|t_1, \alpha(g)) & \text{if } x, y \in [6] \\ 0 & \text{otherwise.} \end{cases}$$

- When $g \in I' = \{g_m, g_{m+1}, g_{m+2}, (g_m, t_1), (g_m, t_2)\}$ and $h \in \{g \in O_\Gamma \mid g = t_2 \text{ in } \Gamma\}$

$$C_{n,\boldsymbol{z}}(x, y|g, h) = \begin{cases} \mathfrak{C}_{p(n)}(x, y|\alpha(g), t_2) & \text{if } x, y \in [6] \\ 0 & \text{otherwise,} \end{cases}$$

$$C_{n,\boldsymbol{z}}(x, y|h, g) = \begin{cases} \mathfrak{C}_{p(n)}(x, y|t_2, \alpha(g)) & \text{if } x, y \in [6] \\ 0 & \text{otherwise.} \end{cases}$$

- When $j \in [m]$,

$$C_{n,\boldsymbol{z}}(\boldsymbol{x}, (y_0, y_1)|j, (g_m, t_1)) = \begin{cases} f_{\boldsymbol{z}}([\prod_{k \in I_j} \frac{e+(-1)^{\boldsymbol{x}(k)} g_{j,k}}{2}]\pi_0^{(y_0)} \frac{e+(-1)^{y_1} t_1}{2}) & \text{if } y_0 \in [3] \\ 0 \text{ otherwise,} \end{cases}$$

$$C_{n,\boldsymbol{z}}((x_0, x_1), \boldsymbol{y}|(g_m, t_1), j) = \begin{cases} f_{\boldsymbol{z}}(\pi_0^{(x_0)} \frac{e+(-1)^{x_1} t_1}{2} [\prod_{k \in I_j} \frac{e+(-1)^{\boldsymbol{y}(k)} g_{j,k}}{2}]) & \text{if } x_0 \in [3] \\ 0 \text{ otherwise,} \end{cases}$$

The values of $C_{n,\boldsymbol{z}}(\boldsymbol{x}, (y_0, y_1)|j, (g_m, t_2))$ and $C_{n,\boldsymbol{z}}((x_0, x_1), \boldsymbol{y}|(g_m, t_2), j)$ are defined analogously.

- When $g \in O_\Gamma$,

$$C_{n,\boldsymbol{z}}(x,(y_0,y_1)|g,(g_m,t_1)) = \begin{cases} f_{\boldsymbol{z}}(\frac{e+(-1)^x g}{2}\pi_0^{(y_0)}\frac{e+(-1)^{y_1}t_1}{2}) & \text{if } x \in [2], y_0 \in [3], y_1 \in [2] \\ 0 & \text{otherwise;} \end{cases}$$
$$C_{n,\boldsymbol{z}}((x_0,x_1),y|(g_m,t_1),g) = \begin{cases} f_{\boldsymbol{z}}(\pi_0^{(x_0)}\frac{e+(-1)^{x_1}t_1}{2}\frac{e+(-1)^y g}{2}) & \text{if } x_0 \in [3], x_1 \in [2], y \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

The values of $C_{n,\boldsymbol{z}}(x,(y_0,y_1)|g,(g_m,t_2))$ and $C_{n,\boldsymbol{z}}((x_0,x_1),y|(g_m,t_2),g)$ are defined analogously.

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 $[m] \times [m] \times [8] \times [8]$ is a perfect correlation of $A\boldsymbol{x} = 0$. Define

$$F_n = \{C_{n,\boldsymbol{z}} | C_{n,\boldsymbol{z}} \text{ induces a perfect correlation of } A\boldsymbol{x} = 0\},$$

and $N_{qa} := |F_n| \leq 2^{|W|}$.

Proof of Theorem 7.8. In $\mathbb{Z}_2^{|W|}$, there exists $\hat{\boldsymbol{z}}$ such that

$$\hat{\boldsymbol{z}}(w) = 1 \iff w = e \in \Gamma / \langle \phi(t)^{p(n)} = e \rangle$$

for all $w \in W$. Since $C_{n,\hat{\boldsymbol{z}}}$ induces a perfect correlation of $\mathsf{LS}(A,0)$, $C_{n,\hat{\boldsymbol{z}}} \in F_n$.

When $n \in X$, the proof follows the proof of Theorem 6.9. Assume $C_{n,\boldsymbol{z}} \in F_n \cap C_{qc}^s(M_{qa}, 8)$ for some $\boldsymbol{z} \in Z$. Then there exists an inducing commuting-operator strategy

$$S = (|\psi\rangle, \{\{M_g^{(x)} \mid x \in [8]\} \mid g \in O \cup [m]\}, \{\{N_g^{(x)} \mid x \in [8]\} \mid g \in O \cup [m]\}).$$

Following the same reasoning as in the proof of Theorem 6.9, we can construct the 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 $g \in O_\Gamma$. From the correlation, we know that $\langle\psi|M(x)|\psi\rangle = 0$.

Since D is embedded in Γ, assuming $\phi(u) = (u_1 u_2)$, we know

$$(M(t_1)M(t_2))(M(u_1)M(u_2))|\psi\rangle = (M(u_1)M(u_2))(M(t_1)M(t_2))^r|\psi\rangle$$
$$(N(t_1)N(t_2))(N(u_1)N(u_2))|\psi\rangle = (N(u_1)N(u_2))(N(t_1)N(t_2))^r|\psi\rangle.$$

Define $U_A = M(u_1)M(u_2)$ and $U_B = N(u_1)N(u_2)$, then these two unitaries satisfy the conditions of Theorem 7.4. Since S can induce $\mathfrak{C}_{p(n)}$, we can use Theorem 7.4 to conclude that

$$\langle\psi|(M(t_1)M(t_2))^{p(n)}|\psi\rangle = 1.$$

By [CLS17, Lemma 8], we know that there exists a Hilbert space $\mathcal{H}_0$, such that for $g, g' \in O_\Gamma$,

$$(M(g)|_{\mathcal{H}_0})^2 = \mathbb{1}_{\mathcal{H}_0}$$
$$M(g)|_{\mathcal{H}_0} M(g')|_{\mathcal{H}_0} = \mathbb{1}_{\mathcal{H}_0} \text{ if } gg' \in P_G \cup P_D \cup P_t,$$

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, $\sigma : \Gamma/\langle (t_1t_2)^{p(n)} = e\rangle \to \mathcal{U}(\mathcal{H}_0)$ induced by $\sigma(g) = M(g)|_{\mathcal{H}_0}$ for each $g \in O_\Gamma$ is a representation of $\Gamma/\langle (t_1t_2)^{p(n)} = e\rangle$. However, by Claim 7.10, when $n \in X$, $x = e$ in $\Gamma/\langle (t_1t_2)^{p(n)} = e\rangle$. By the correlation, we know $M(x)|\psi\rangle \neq |\psi\rangle$, so $\sigma(x) = M(x)|_{\mathcal{H}_0} \neq \mathbb{1}_{\mathcal{H}_0}$, which contradicts the fact that σ is a homomorphism. Hence, $C_{n,\boldsymbol{z}}$ is not in $C^s_{qc}(M_{qa}, 8)$ and not in $C^s_{qa}(M_{qa}, 8)$.

When $n \notin X$, we give a series of finite-dimensional quantum strategies inducing quantum correlations approaching $C_{n,\hat{\boldsymbol{z}}}$. The construction of the quantum strategies depends on the fa^*-embedding procedures summarized in Propositions 4.9 and 4.10.

Before we apply Propositions 4.9 and 4.10, we define

$$A_1 = \{ghk \mid g \in O_\Gamma, h \in D_p, k \in \{e, t_1, t_2\}\}$$
$$A = \{w \in W \cup A_1 \mid w \neq e \text{ in } \Gamma/\langle (t_1t_2)^{p(n)} = e\rangle\}.$$

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 4.9 and 4.10 and [Slo19, Lemma 25], for any $\epsilon, \zeta > 0$, there is an ϵ-approximate representation $\rho : \Gamma/\langle (t_1t_2)^{p(n)} = e\rangle \to \mathcal{U}(\mathbb{C}^d)$ such that, for each $w \in A$,

$$0 \leq \tilde{\operatorname{Tr}}(\rho(w)) \leq \zeta,$$

and for any $g \in O^{\#}_\Gamma$, $\rho(g)^2 = \mathbb{1}$. Moreover, for any $r \in P_\Gamma$,

$$|\tilde{\operatorname{Tr}}(\rho(r)) - 1| \leq \|\rho(r) - \rho(e)\| \leq \epsilon.$$

By [Slo19, Lemma 24], there are representations $\rho_i : G_i \to \mathcal{U}(\mathbb{C}^d)$ such that

$$\|\rho_i(g_{i,k}) - \rho(g_{i,k})\| \leq 15\epsilon \text{ for } k \in I_i.$$

Then we can define Alice and Bob's projectors based on ρ and ρ_i.

- For question $g_{i,k} \in O^{\#}_\Gamma$, Alice and Bob's projectors are

$$\tilde{P}^{(a)}_{g_{i,k}} = \begin{cases} \frac{\mathbb{1}+(-1)^a\rho(g_{i,k})}{2} & \text{if } a \in [2] \\ 0 & \text{otherwise;} \end{cases}$$
$$\tilde{Q}^{(b)}_{g_{i,k}} = \begin{cases} \left(\frac{\mathbb{1}+(-1)^b\rho(g_{i,k})}{2}\right)^{\mathsf{T}} & \text{if } b \in [2] \\ 0 & \text{otherwise.} \end{cases}$$

- For question $i \in [m]$, Alice and Bob's projectors are

$$\tilde{P}^{(\boldsymbol{a})}_i = \prod_{k \in I_i} \frac{\mathbb{1} + (-1)^{\boldsymbol{a}(k)}\rho_i(g_{i,k})}{2},$$
$$\tilde{Q}^{(\boldsymbol{b})}_i = \left[\prod_{k \in I_i} \frac{\mathbb{1} + (-1)^{\boldsymbol{b}(k)}\rho_i(g_{i,k})}{2}\right]^{\mathsf{T}}.$$

- For questions g_m, g_{m+1}, g_{m+2}, recall eq. (50) to eq. (58), we define $\{\tilde{P}^{(a)}_{g_m} \mid a \in [3]\}$, $\{\tilde{P}^{(a)}_{g_{m+1}} \mid a \in [3]\}$ and $\{\tilde{P}^{(a)}_{g_{m+2}} \mid a \in [3]\}$ to be the projective measurements obtained by applying Proposition 7.7 to $\{\rho(\pi_0^{(a)}) \mid a \in [3]\}$, $\{\rho(\pi_1^{(a)}) \mid a \in [3]\}$ and $\{\rho(\pi_2^{(a)}) \mid a \in [3]\}$ respectively. Bob's projectors are $\tilde{Q}^{(b)}_y = (\tilde{P}^{(b)}_y)^\intercal$ for $b \in [3]$ and $y \in \{g_m, g_{m+1}, g_{m+2}\}$. For answers $a, b > 2$, $\tilde{P}^{(a)}_x = \tilde{Q}^{(b)}_y = 0$.

- For questions (g_m, t_1) and (g_m, t_2), we define $\{\tilde{P}^{(a_0,a_1)}_{(g_m,t_1)} \mid a_0 \in [3], a_1 \in [2]\}$ and $\{\tilde{P}^{(a_0,a_1)}_{(g_m,t_2)} \mid a_0 \in [3], a_1 \in [2]\}$ by

$$\tilde{P}^{(a_0,a_1)}_{(g_m,t_1)} = \tilde{P}^{(a_0)}_{g_m} \tilde{P}^{(a_1)}_{t_1}$$
$$\tilde{P}^{(a_0,a_1)}_{(g_m,t_2)} = \tilde{P}^{(a_0)}_{g_m} \tilde{P}^{(a_1)}_{t_2},$$

  respectively. Bob's projectors are defined analogously. Note that by Proposition 7.7 $\tilde{P}^{(a_0)}_{g_m}$ 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.

Note that Proposition 7.7 is applicable because of the following claim.

Claim 7.11. *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 $a \in [3]$.*

Proof. Recall eq. (50) to eq. (58). Let $|\psi\rangle$ be an eigenvector of $\rho(t_1 t_2)$ such that $\rho(t_1 t_2)|\psi\rangle = e^{i\theta}|\psi\rangle$.

$$\|\rho(\pi_0^{(0)})|\psi\rangle\| = \frac{1}{p(n)} \| \sum_{j\in[p(n)]} \rho(t_1 t_2)^j |\psi\rangle\| \leq \frac{1}{p(n)} \sum_{j\in[p(n)]} \|e^{ij\theta}|\psi\rangle\| \leq 1.$$
$$\|\rho(\pi_0^{(1)})|\psi\rangle\| \leq \frac{2}{p(n)} \sum_{j\in[p(n)]} |\cos(\frac{2j\pi}{p(n)})| \|e^{ij\theta}|\psi\rangle\| \leq 2.$$
$$\|\rho(\pi_0^{(1)})|\psi\rangle\| \leq \||\psi\rangle\| + \|\rho(\pi_0^{(0)})|\psi\rangle\| + \|\rho(\pi_0^{(1)})|\psi\rangle\| \leq 4.$$

Recall that

$$\pi_1^{(0)} = \pi_0^{(1)}/2 + \frac{1}{p(n)} \sum_{j\in[p(n)]} \cos(\frac{(2j+1)\pi}{p(n)}) t_2 (t_1 t_2)^j,$$
$$\pi_2^{(0)} = \pi_0^{(1)}/2 + \frac{1}{p(n)} \sum_{j\in[p(n)]} \sin(\frac{(2j+1)\pi}{p(n)}) t_2 (t_1 t_2)^j.$$

Then, with similar reasoning,

$$\begin{aligned}
\|\rho(\pi_1^{(0)})|\psi\rangle\| \leq& 2\\
\|\rho(\pi_1^{(1)})|\psi\rangle\| \leq& 2\\
\|\rho(\pi_1^{(2)})|\psi\rangle\| \leq& \||\psi\rangle\| + \|\rho(\pi_0^{(1)})|\psi\rangle\| \leq 3,\\
\|\rho(\pi_2^{(0)})|\psi\rangle\| \leq& 2\\
\|\rho(\pi_2^{(1)})|\psi\rangle\| \leq& 2\\
\|\rho(\pi_2^{(2)})|\psi\rangle\| \leq& \||\psi\rangle\| + \|\rho(\pi_0^{(1)})|\psi\rangle\| \leq 3,
\end{aligned}$$

which completes the proof. □

In summary, the strategy we construct is

$$S_{\epsilon,\zeta} = (|\mathsf{EPR}_d\rangle, \{\{\tilde{P}_x^{(a)} \mid a \in [8]\}x \in O\}, \{\{\tilde{Q}_y^{(b)} \mid b \in [8]\}y \in O\}).$$

To see that $\{S_{\epsilon,\zeta}\}$ can approach $C_{n,\hat{\boldsymbol{z}}}$, we pick certain entries of $C_{n,\hat{\boldsymbol{z}}}$ as examples to illustrate the argument. For any $g_{i,k}, g_{j,l} \in O_\Gamma$,

$$\langle \mathsf{EPR}_d|\rho(g_{i,k}) \otimes \rho(g_{j,l})^\intercal|\mathsf{EPR}_d\rangle = \tilde{\operatorname{Tr}}(\rho(g_{i,k}g_{j,l}))$$

We can check that if $g_{i,k}g_{j,l} = e$ in $\Gamma/\langle (t_1t_2)^{p(n)} = e\rangle$, $|\tilde{\operatorname{Tr}}(\rho(g_{i,k}g_{j,l})) - 1| \leq \epsilon$, and otherwise, $0 \leq \tilde{\operatorname{Tr}}(\rho(g_{i,k}g_{j,l})) \leq \zeta$. In particular, we know

$$|\langle \mathsf{EPR}_d|\rho(x)|\mathsf{EPR}_d\rangle - \sum_{y\in[2]} [C_{n,\hat{\boldsymbol{z}}}(x, g, 0, y) - C_{n,\hat{\boldsymbol{z}}}(x, g, 1, y)]| \leq \zeta.$$

When the questions are $i, j \in [m]$, first notice that

$$\langle \mathsf{EPR}_d|\tilde{P}_i^{(\boldsymbol{x})} \otimes \tilde{Q}_j^{(\boldsymbol{y})}|\psi\rangle = \tilde{\operatorname{Tr}}\left(\prod_{k\in I_i} \frac{\mathbb{1} + (-1)^{\boldsymbol{x}(k)}\rho_j(g_{i,k})}{2} \prod_{l\in I_j} \frac{\mathbb{1} + (-1)^{\boldsymbol{y}(l)}\rho_i(g_{j,l})}{2}\right).$$

If we write

$$\Pi_{i,j}^{(\boldsymbol{x},\boldsymbol{y})} = (\prod_{k\in I_i} \frac{\mathbb{1} + (-1)^{\boldsymbol{x}(k)}\rho(g_{i,k})}{2})(\prod_{l\in I_j} \frac{\mathbb{1} + (-1)^{\boldsymbol{y}(l)}\rho(g_{j,l})}{2}),$$

then

$$\begin{aligned}
&|C_{n,\hat{\boldsymbol{z}}}(i, j, \boldsymbol{x}, by) - \langle \mathsf{EPR}_d|\tilde{P}_i^{(\boldsymbol{x})} \otimes \tilde{Q}_j^{(\boldsymbol{y})}|\psi\rangle|\\
\leq& |f_{\hat{\boldsymbol{z}}}(i, j, \boldsymbol{x}, \boldsymbol{y}) - \tilde{\operatorname{Tr}}(\Pi_{i,j}^{(\boldsymbol{x},\boldsymbol{y})})| + |\tilde{\operatorname{Tr}}\left(\tilde{P}_i^{(\boldsymbol{x})}(\tilde{Q}_j^{(\boldsymbol{y})})^\intercal - \Pi_{i,j}^{(\boldsymbol{x},\boldsymbol{y})}\right)|\\
\leq& \epsilon + \zeta + 15\epsilon.
\end{aligned}$$

Lastly, when the questions are g_{m+1} and t_1,

$$\begin{aligned}
&|\langle \mathsf{EPR}_d|\tilde{P}^{(0)}_{g_{m+1}} \otimes \tilde{Q}^{(0)}_{t_1} - \rho(\pi_1^{(0)}) \otimes (\frac{\mathbb{1}+\rho(t_1)}{2})^{\mathsf{T}}|\mathsf{EPR}_d\rangle| \\
=&|\tilde{\mathrm{Tr}}\left[(\tilde{P}^{(0)}_{g_{m+1}} - \rho(\pi_1^{(0)}))\frac{\mathbb{1}+\rho(t_1)}{2}\right]| \\
\leq&\|\frac{\mathbb{1}+\rho(t_1)}{2}\|_{op}\|\tilde{P}^{(0)}_{g_{m+1}} - \rho(\pi_1^{(0)})\| \\
\leq&12^5\epsilon.
\end{aligned}$$

We can also bound $\tilde{\mathrm{Tr}}[\rho(\pi_1^{(0)})\frac{\mathbb{1}+\rho(t_1)}{2}]$ from $C_{n,\hat{\boldsymbol{z}}}(g_m, t_1, 0, 0)$,

$$\begin{aligned}
&|\tilde{\mathrm{Tr}}\left[\rho(\pi_1^{(0)})\frac{\mathbb{1}+\rho(t_1)}{2}\right] - C_{n,\hat{\boldsymbol{z}}}(g_m, t_1, 0, 0)| \\
=&|\tilde{\mathrm{Tr}}\left[\rho(\pi_1^{(0)})\frac{\mathbb{1}+\rho(t_1)}{2}\right] - \frac{\cos^2(\pi/2p(n))}{p(n)}| \\
\leq&\frac{1}{2p(n)}\Big[|\tilde{\mathrm{Tr}}(\rho((t_1t_2))^0 - \mathbb{1}| + \sum_{0<j<p(n)} \cos(2j\pi/p(n))|\tilde{\mathrm{Tr}}(\rho(t_1t_2)^j)| \\
&+ \sum_{j\in[p(n)]} \cos(2j\pi/p(n))|\tilde{\mathrm{Tr}}(\rho((t_1t_2)^j t_1))| + \cos((2j+1)\pi/p(n))|\tilde{\mathrm{Tr}}(\rho(t_2(t_1t_2)^j))| \\
&+ \cos(\pi/p(n))|\tilde{\mathrm{Tr}}(\rho((t_1t_2))^p(n) - \mathbb{1}| + \sum_{j\in[p(n)-1]} \cos((2j+1)\pi/p(n))|\tilde{\mathrm{Tr}}(\rho(t_2(t_1t_2)^j))|\Big] \\
\leq&\frac{1}{2p(n)}(\cos(\pi/p(n))\epsilon + 2p(n)\zeta).
\end{aligned}$$

Overall,

$$\begin{aligned}
&|\langle \mathsf{EPR}_d|\tilde{P}^{(0)}_{g_{m+1}} \otimes \tilde{Q}^{(0)}_{t_1}|\mathsf{EPR}_d\rangle - C_{n,\hat{\boldsymbol{z}}}(g_m, t_1, 0, 0)| \\
\leq&|\langle \mathsf{EPR}_d|\tilde{P}^{(0)}_{g_{m+1}} \otimes \tilde{Q}^{(0)}_{t_1} - \rho(\pi_1^{(0)}) \otimes (\frac{\mathbb{1}+\rho(t_1)}{2})^{\mathsf{T}}|\mathsf{EPR}_d\rangle| \\
&+|\tilde{\mathrm{Tr}}\left[\rho(\pi_1^{(0)})\frac{\mathbb{1}+\rho(t_1)}{2}\right] - C_{n,\hat{\boldsymbol{z}}}(g_m, t_1, 0, 0)| \\
\leq&(12^5+1)\epsilon + \zeta.
\end{aligned}$$

In summary,

$$\lim_{\zeta,\epsilon\to 0^+} \langle \mathsf{EPR}_d|\tilde{P}^{(a)}_x \otimes \tilde{Q}^{(b)}_y|\mathsf{EPR}_d\rangle = C_{n,\hat{\boldsymbol{z}}}(x, y, a, b).$$

and $F_n \cap C^s_{qa}(M_{qa}, 8) = \{C_{n,\hat{\boldsymbol{z}}}\}$. □

Corollary 7.12. *There exist constants N_1 and M_1 such that, for constants $N \geq N_1$ and $M \geq M_1$, $(Membership(N, N, M, M)^s_{\mathbb{K}_0,qa})$ is* coRE*-hard.*

Proof. By [Slo19, Lemma 42], the group G defined in eq. (2) is an extended homogeneous linear-plus-conjugacy group that has a presentation where the image of $w(0)w(a)$ is an involutary generator. Then, by Proposition 5.4, the group G also satisfies the conditions of Theorem 7.8. Therefore, there exist constants N_1 and K and a family of sets of correlations $\{F_n\}$ where $F_n \subset \mathbb{K}_0^{N_1^2 \times 8^2}$ and $|F_n| = K$, such that $F_n \cap C_{qa}^s(N_1, 8) \neq \emptyset$ if and only if $n \notin X$. Hence, the problem of deciding if $F_n \cap C_{qa}^s(N_1, 8) \neq \emptyset$ is coRE-complete, and $(\text{Intersection}(N, N, M, M)^s_{\mathbb{K}_0, qa})$ is coRE-hard for $N \geq N_1$ and $M \geq 8$. By Proposition 7.1, $(\text{Membership}(N, N, M, M)^s_{\mathbb{K}_0, qa})$ for $N \geq N_1$ and $M \geq 8$ is also coRE-hard. □

References

[BBL⁺06] G. Brassard, H. Buhrman, N. Linden, A. A. Methot, A. Tapp, and F. Unger. A limit on nonlocality in any world in which communication complexity is not trivial. *Phys. Rev. Lett.*, 96(250401), 2006. URL: https://link.aps.org/doi/10.1103/PhysRevLett.96.250401, doi:10.1103/PhysRevLett.96.250401.

[BCLPG20] Johannes Bausch, Toby S Cubitt, Angelo Lucia, and David Perez-Garcia. Undecidability of the spectral gap in one dimension. *Physical Review X*, 10(3):031038, 2020. URL: https://link.aps.org/doi/10.1103/PhysRevX.10.031038, doi:10.1103/PhysRevX.10.031038.

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

[CHTW04] 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. doi:10.1109/CCC.2004.1313847.

[CLP15] Valerio Capraro, Martino Lupini, and Vladimir Pestov. *Introduction to sofic and hyperlinear groups and Connes' embedding conjecture*, volume 2136. Springer, 2015. doi:10.1007/978-3-319-19333-5.

[CLS17] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017. doi:10.1063/1.4973422.

[CS18] Andrea Coladangelo and Jalex Stark. Unconditional separation of finite and infinite-dimensional quantum correlations. *arXiv preprint arXiv:1804.05116*, 2018.

[CS19] 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.

[FJVY19] Joseph Fitzsimons, Zhengfeng Ji, Thomas Vidick, and Henry Yuen. Quantum proof systems for iterated exponential time, and beyond. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 473–480. ACM, 2019. doi:10.1145/3313276.3316343.

[Fri12] Tobias Fritz. Tsirelson's problem and kirchberg's conjecture. *Reviews in Mathematical Physics*, 24(05):1250012, 2012. doi:10.1142/S0129055X12500122.

[FSA$^+$13] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acin. Local orthogonality as a multipartite principle for quantum correlations. *Nature Communications*, 4(2263), 2013. doi:10.1038/ncomms3263.

[Fu19] Honghao Fu. Constant-sized correlations are sufficient to robustly self-test maximally entangled states with unbounded dimension. *arXiv preprint arXiv:1911.01494*, 2019.

[GKW$^+$18] Koon Tong Goh, Jedrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani. Geometry of the set of quantum correlations. *Phys. Rev. A*, 97:022104, Feb 2018. URL: https://link.aps.org/doi/10.1103/PhysRevA.97.022104, doi:10.1103/PhysRevA.97.022104.

[HNN49] Graham Higmann, Bernhard Neumann, and Hanna Neumann. Embedding theorems for groups. *Journal of the London Mathematical Society*, 1(4):247–254, 1949. doi:10.1112/jlms/s1-24.4.247.

[IV12] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for nexp sound against entangled provers. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 243–252. IEEE, 2012. doi:10.1109/FOCS.2012.11.

[Ji17] Zhengfeng Ji. Compression of quantum multi-prover interactive proofs. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 289–302, 2017. doi:10.1145/3055399.3055441.

[JNP$^+$11] M. Junge, M. Navascués, C. Palazuelos, D. Pérez-García, V. B. Scholz, and R. F. Werner. Connes' embedding problem and Tsirelson's problem. *Journal of Mathematical Physics*, 52(1):012102, 2011. doi:10.1063/1.3514538.

[JNV$^+$20] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. $MIP^* = RE$. *arXiv preprint arXiv:2001.04383*, 2020.

[KMS17] Olga Kharlampovich, Alexei Myasnikov, and Mark Sapir. Algorithmically complex residually finite groups. *Bulletin of Mathematical Sciences*, 7(2):309–352, 2017. doi:10.1007/s13373-017-0103-z.

[Lan88] L. J. Landau. Empirical two-point correlation functions. *Foundations of Physics*, 18:449–460, 1988. doi:10.1007/BF00732549.

[Mas03] Ll. Masanes. Necessary and sufficient condition for quantum-generated correlations. 2003. arXiv:quant-ph/0309137.

[Min67] Marvin Lee Minsky. *Computation: Finite and Infinite Machines*. Prentice-Hall Englewood Cliffs, 1967. doi:10.5555/1095587.

[MNY20] Hamoon Mousavi, Seyed Sajjad Nezhadi, and Henry Yuen. On the complexity of zero gap MIP. *arXiv preprint arXiv:2002.10490*, 2020.

[MS12] Carl A. Miller and Yaoyun Shi. Optimal robust quantum self-testing by binary nonlocal XOR games. arXiv:1207.1819, 2012.

[Mur88] M. Ram Murty. Artin's conjecture for primitive roots. *The Mathematical Intelligencer*, 10(4):59–67, 1988. doi:10.1007/BF03023749.

[NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008. doi:10.1088/1367-2630/10/7/073013.

[NV17] Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1003–1015. ACM, 2017. doi:10.1145/3055399.3055468.

[NV18] Anand Natarajan and Thomas Vidick. Low-degree testing for quantum states, and a quantum entangled games PCP for QMA. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 731–742. IEEE, 2018. doi:10.1109/FOCS.2018.00075.

[NW09] M. Navascues and H. Wunderlich. A glance beyond the quantum model. *Proc. Royal Soc. A*, 466:881–890, 2009. doi:10.1098/rspa.2009.0453.

[NW19] 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. doi:10.1109/FOCS.2019.00039.

[Pit08] I. Pitowsky. Geometry of quantum correlations. *Physical Review A*, 77:062109, 2008. URL: https://link.aps.org/doi/10.1103/PhysRevA.97.022104, doi:10.1103/PhysRevA.97.022104.

[PPK$^+$09] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski. Information causality as a physical principle. *Nature*, 461:1101–1104, 2009. doi:10.1038/nature08400.

[Rot12] Joseph J Rotman. *An introduction to the theory of groups*, volume 148. Springer Science & Business Media, 2012. doi:/10.1007/978-1-4612-4176-8.

[Rus20] Travis B. Russell. Geometry of the set of synchronous quantum correlations. *Journal of Mathematical Physics*, 61:052201, 2020. doi:10.1063/1.5115010.

[RUV13] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456, 2013. doi:10.1038/nature12035.

[SGAN18] Ana Belén Sainz, Yelena Guryanova, Antonio Acín, and Miguel Navascués. Almost-quantum correlations violate the no-restriction hypothesis. *Phys. Rev. Lett.*, 120:200402, May 2018. URL: https://link.aps.org/doi/10.1103/PhysRevLett.120.200402, doi:10.1103/PhysRevLett.120.200402.

[Slo19] William Slofstra. The set of quantum correlations is not closed. In *Forum of Mathematics, Pi*, volume 7. Cambridge University Press, 2019. doi:10.1017/fmp.2018.3.

[Slo20] William Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. *Journal of the American Mathematical Society*, 33(1):1–56, 2020. doi:10.1090/jams/929.

[Tsi87] B.S. Tsirelson. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36(4):557–570, 1987. doi:10.1007/BF01663472.

[Tsi93] B.S. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8:329–345, 1993.

[TVC19] Le Phuc Thinh, Antonios Varvitsiotis, and Yu Cai. Geometric structure of quantum correlators via semidefinite programming. *Phys. Rev. A*, 99:052108, May 2019. URL: https://link.aps.org/doi/10.1103/PhysRevA.99.052108, doi:10.1103/PhysRevA.99.052108.

[WW01] R. F. Werner and M. M. Wolf. All-multipartite bell-correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, 64:032112, Aug 2001. URL: https://link.aps.org/doi/10.1103/PhysRevA.64.032112, doi:10.1103/PhysRevA.64.032112.

A Proof of Theorem 7.4

Before we prove Theorem 7.4, we present certain nonzero values of $\mathfrak{C}_p$, which will help the proof. For question 0.

$$\mathfrak{C}_p(a,b|0,0) = \begin{cases} \frac{1}{p} & \text{if } a=b=0 \\ \frac{2}{p} & \text{if } a=b=1 \\ \frac{p-3}{p} & \text{if } a=b=2 \\ 0 & \text{otherwise.} \end{cases}$$

When $x \in \{t_1, t_2\}$ and $y \in \{1,2\}$, some of the values of $\mathfrak{C}_p(a,b|x,y)$ 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 5: The correlation for $x \in \{t_1, t_2\}$ and $y \in \{1,2\}$.

When $x, y \in \{0,1,2\}$, some of the values of $\mathfrak{C}(a,b|x,y)$ 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 6: The correlation 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 7: The correlation for the commutation test for Alice's questions 0 and t_1.

When $x=(0,t_1)$ and $y=(0,t_2)$, for $a,b\in[2]$,

$$\mathfrak{C}_p((0,a),(0,b)|(0,t_1),(0,t_2)) = \begin{cases} 1/p & \text{if } a=b=0 \\ 1/p & \text{if } a=b=1 \\ 0 & \text{otherwise.} \end{cases} \tag{60}$$

Proof of Theorem 7.4. 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 $\{|\psi_j\rangle\}$ is an orthogonal set and each $|\psi_j\rangle$ is an eigenvector of $M_{t_1}M_{t_2}$ with an eigenvalue ω_p^j.

Applying Proposition 6.2 to the values given in Table 7, 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 6.1 to given in eq. (60), we can get that

$$M_{(0,t_1)}^{(0,a_1)}|\psi\rangle = N_{(0,t_2)}^{(0,a_1)}|\psi\rangle \tag{61}$$

for each $a_1\in[2]$. Then, we can further deduce that

$$M_{t_1}^{(a_1)}M_0^{(0)}|\psi\rangle = N_{(0,t_2)}^{(0,a_1)}|\psi\rangle = M_{t_2}^{a_1}M_0^{(0)}|\psi\rangle \tag{62}$$

Define $M_x := M_x^{(0)} - M_x^{(1)}$ and $N_y := N_y^{(0)} - N_y^{(1)}$ for $x,y=t_1,t_2$, and

$$|\psi_0\rangle = M_{t_1}^{(0)}M_0^{(0)}|\psi\rangle, \tag{63}$$

$$|\psi_p\rangle = M_{t_1}^{(1)}M_0^{(0)}|\psi\rangle. \tag{64}$$

Then we know from the correlation in Table 6 and the definitions of $|\psi_0\rangle$ and $|\psi_p\rangle$ that

$$\||\psi_0\rangle\|^2 = \||\psi_p\rangle\|^2 = \frac{1}{2p}, \tag{65}$$

$$M_{t_1}|\psi_0\rangle = |\psi_0\rangle \tag{66}$$

$$M_{t_1}|\psi_p\rangle = -|\psi_p\rangle, \tag{67}$$

and hence $\langle\psi_0|\psi_p\rangle = 0$. By eq. (62), we know

$$|\psi_0\rangle = M_2^0 M_0^0 |\psi\rangle, \tag{68}$$
$$|\psi_p\rangle = M_2^1 M_0^0 |\psi\rangle. \tag{69}$$

The definition of M_2 implies that

$$M_2|\psi_0\rangle = |\psi_0\rangle, \tag{70}$$
$$M_2|\psi_p\rangle = -|\psi_p\rangle. \tag{71}$$

Following [Fu19, Proposition 6.10], we can extract the correlations induced by the following two strategies from Tables 5 and 6

$$S = \left(\frac{M_0^{(1)}|\psi\rangle}{\|M_0^{(1)}|\psi\rangle\|}, \{\{M_x^{(0)}, M_x^{(1)}\} \mid x = 1,2\}, \{\{N_y^{(0)}, N_y^{(1)}\} \mid y = t_1, t_2\}\right)$$
$$S' = \left(\frac{M_0^{(1)}|\psi\rangle}{\|M_0^{(1)}|\psi\rangle\|}, \{\{M_x^{(0)}, M_x^{(1)}\} \mid x = t_1, t_2\}, \{\{N_y^{(0)}, N_y^{(1)}\} \mid y = 1,2\}\right)$$

Then we can define $M_2 := M_2^{(0)} - M_2^{(1)}$ and

$$|\psi_1\rangle = \frac{1}{2}(M_1^{(0)} - iM_2M_1^{(1)} + iM_2M_1^{(0)} + M_1^{(1)})|\psi\rangle. \tag{72}$$

Following the proofs of [Fu19, Propositions 6.11, 6.12 and 6.13], we can conclude that

$$\||\psi_1\rangle\|^2 = \frac{1}{p} \tag{73}$$
$$M_{t_1}M_{t_2}|\psi_1\rangle = \omega_p|\psi_1\rangle \tag{74}$$
$$N_{t_1}N_{t_2}|\psi_1\rangle = \omega_p^{-1}|\psi_1\rangle. \tag{75}$$

Recall the conditions satisfied by U_A and U_B from the statement of the theorem. Define

$$|\psi_j\rangle = (U_AU_B)^{\log_r j}|\psi_1\rangle. \tag{76}$$

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 [Fu19, Proposition 6.14], 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

$$\langle\psi_j|\psi_k\rangle = 0 \tag{77}$$

for each $1 \le j \ne k \le p-1$.

Define

$$|\psi'\rangle = |\psi_0\rangle + |\psi_p\rangle + \sum_{j=1}^{p-1} |\psi_j\rangle. \tag{78}$$

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 $(U_A U_B)|\psi\rangle = |\psi\rangle$ and derivation in the proof of [Fu19, Proposition 6.14]. This implies that $|\psi\rangle = |\psi'\rangle$.

Finally, 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. □