Approximate traces on groups and the quantum complexity class $\mathrm{MIP}^{co,s}$

Trazas aproximadas sobre grupos y la comunidad cuántica de la clase $\mathrm{MIP}^{co,s}$

Isaac Goldbring[1,a,✉], Bradd Hart[2]

[1]University of California, Irvine, California

[2]McMaster University, Hamilton ON, Canada

Abstract. An open question in quantum complexity theory is whether or not the class MIP^{co}, consisting of languages that can be efficiently verified using interacting provers sharing quantum resources according to the quantum commuting model, coincides with the class $coRE$ of languages with recursively enumerable complement. We introduce the notion of a qc-modulus, which encodes approximations to quantum commuting correlations, and show that the existence of a computable qc-modulus gives a negative answer to a natural variant of the aforementioned question.

Key words and phrases. traces on groups, quantum complexity theory.

2020 Mathematics Subject Classification. 68Q12, 43A35.

Resumen. Una pregunta abierta en teoria de complejidad cuantica es si la clase MIP^{co}, conformada por aquellos lenguajes que pueden ser verificados usando verificadores interactivos que comparten recursos cuánticos según el modelo de computación cuántica, coincide con la clase $coRE$ de lenguajes con complemento recursivamente enumerable. Introducimos el concepto de módulo qc, que codifica aproximaciones a correlaciones de conmutación cuántica y probamos que la existencia de un módulo qc computable da una respuesta negativa a una variante natural de la pregunta.

Palabras y frases clave. trazas de grupos, teoria de complejidad cuántica.

1. Introduction

The complexity class MIP* consists of those languages that can be decided by a classical verifier interacting with multiple all-powerful quantum provers sharing entanglement; in the next section we give an equivalent definition via values of nonlocal games.

The following landmark result in quantum complexity theory appears in [3]:

Theorem 1.1. MIP* = RE. *In other words, the languages that belong to the complexity class* MIP* *are precisely the recursively enumerable languages - those languages L for which there is an algorithm that enumerates L.*

In particular, MIP* contains undecidable problems (such as the halting problem).

The class MIP^{co} consists of languages that can be efficiently verified using interacting provers sharing quantum resources according to the so-called quantum commuting model (hence the *co*). Again, we give an equivalent definition of this class via nonlocal games in the next section. In [3], it was pointed out that every element of the class MIP^{co} is co-recursively enumerable, that is, the complement of a recursively enumerable set. Denoting by coRE the complexity class of langauges that are co-recursively enumerable, the authors of [3] ask whether or not the aforementioned inclusion is actually an equality:

Question 1. Does MIP^{co} = coRE?

The class MIP^{co} has been extensively studied through the lense of nonlocal games; see for example [1] where they look at the ability to approximate the value of nonlocal games under the quantum commuting model. Variants of MIP^{co} where the strategies are allowed to slightly interact have also been studied, for example by Ozawa ([4]). We take a different tack here focusing on the trace space of particular C*-algebras. These spaces are compact in the weak* topology and our key computability assumption essentially asks how effective this compactness is.

In this note, we define variants of MIP* and MIP^{co}, MIP^{*,s} and MIP^{co,s} using *synchronous* nonlocal games. As was noted in [2] and [3], MIP* = MIP^{*,s}. Our main result is that MIP^{co,s} is not equal to coRE provided we can computability approximate quantum commuting correlations in a certain sense. In fact, under this assumption, all languages that belong to MIP^{co,s} are actually decidable.[1]

In section 2, we introduce the basic definitions we will need and resuls about nonlocal games. In section 3, we give the necessary background on traces on

---

[1]After an initial posting of this paper, Junqiao Lin has claimed that Question 1 indeed has a positive solution. If this proof is correct, then our main result shows that one cannot computably approximate quantum commuting correlations in the sense provided by Theorem 5.3 below.

groups. Section 4 contains the material on approximate traces and finally in section 5, the main technical ingredient, the qc-modulus, is introduced and the main theorem is proved.

The authors would like to thank Alec Fox, Thomas Vidick, and Henry Yuen for helpful conversations around this work.

2. Preliminaries: Nonlocal games

Throughout this note, n and m denote natural numbers that are at least 2 and $[n]$ denotes the set $\{1, \ldots, n\}$ (and likewise for $[m]$).

We recall the following definitions from quantum information theory and quantum complexity theory.

Definition 2.1. (1) The set $C_q(n, m)$ of **quantum correlations** consists of the correlations of the form $p(i, j|v, w) = \langle A_i^v \otimes B_j^w \xi, \xi \rangle$ for $v, w \in [n]$ and $i, j \in [m]$, where H is a finite-dimensional Hilbert space, $\xi \in H \otimes H$ is a unit vector, and for every $v, w \in [n]$, $(A_i^v : i \in [m])$ and $(B_j^w : j \in [m])$ are positive operator-valued measures (POVMs) on H.

(2) We set $C_{qa}(n, m)$ to be the closure in $[0, 1]^{n^2 m^2}$ of $C_q(n, m)$.

(3) The set $C_{qc}(n, m)$ of **quantum commuting correlations** consists of the correlations of the form $p(i, j|v, w) = \langle A_i^v B_j^w \xi, \xi \rangle$ for $v, w \in [n]$ and $i, j \in [m]$, where H is a separable Hilbert space, $\xi \in H$ is a unit vector, and for every $v, w \in [n]$, $(A_i^v : i \in [m])$ and $(B_j^w : j \in [m])$ are POVMs on H for which $A_i^v B_j^w = B_j^w A_i^v$ for all $v, w \in [n]$ and $i, j \in [m]$.

Note that $C_q(n, m) \subseteq C_{qc}(n, m)$; since it is know that the latter set is closed, we in fact have that $C_{qa}(n, m) \subseteq C_{qc}(n, m)$. Tsirelson's problem in quantum information theory asks if these latter two sets in fact coincide; a negative resolution to this problem follows from the main result of [3].

Definition 2.2. (1) A **nonlocal game with n questions and m answers** is a pair $\mathfrak{G} = (\mu, D)$, where μ is a probability distribution on $[n] \times [n]$ and

$$D : [n] \times [n] \times [m] \times [m] \to \{0, 1\}$$

is a function.

(2) Given a nonlocal game $\mathfrak{G}$ as in the previous item and $p \in [0, 1]^{n^2 m^2}$, we define the **value of $\mathfrak{G}$ at p** to be

$$\mathrm{val}(\mathfrak{G}, p) := \sum_{v, w \in [n]} \mu(v, w) \sum_{i, j \in [m]} D(v, w, i, j) p(i, j|v, w).$$

Definition 2.3. Given a nonlocal game $\mathfrak{G}$ with n questions and m answers, we define:

(1) the **entangled value of** $\mathfrak{G}$ to be

$$\text{val}^*(\mathfrak{G}) := \sup_{p \in C_{qa}(n,m)} \text{val}(\mathfrak{G}, p);$$

(2) the **quantum commuting value of** $\mathfrak{G}$ to be

$$\text{val}^{co}(\mathfrak{G}) := \sup_{p \in C_{qc}(n,m)} \text{val}(\mathfrak{G}, p).$$

The following, which we present as a definition, is equivalent to the definition give in terms of provers and quantum entanglement [3].

Definition 2.4. A language L (in the sense of complexity theory) belongs to the class MIP* if there is an effective mapping $z \mapsto \mathfrak{G}_z$ from strings to nonlocal games such that:

- if $z \in L$, then $\text{val}^*(\mathfrak{G}_z) \geq \frac{2}{3}$

- if $z \notin L$, then $\text{val}^*(\mathfrak{G}_z) \leq \frac{1}{3}$.

The complexity class MIP^{co} can be defined in an analogous fashion, using val^{co} instead of val^*.

We recall the following definitions:

Definition 2.5. (1) Given $p \in [0,1]^{n^2 m^2}$, we say that p is **synchronous** if $p(i,j|v,v) = 0$ for all $v \in [n]$ and all *distinct* $i, j \in [m]$.

(2) We let $C_{qa}^s(n,m)$ and $C_{qc}^s(n,m)$ denote the synchronous elements of $C_{qa}(n,m)$ and $C_{qc}(n,m)$ respectively.

(3) Given a nonlocal game $\mathfrak{G}$, we let s-val$^*(\mathfrak{G})$ and s-val$^{co}(\mathfrak{G})$ denote the corresponding **synchronous values** of $\mathfrak{G}$, which are defined analogously to $\text{val}^*(\mathfrak{G})$ and $\text{val}^{co}(\mathfrak{G})$, except that we only take the supremum over $C_{qa}^s(n,m)$ and $C_{qc}^s(n,m)$ respectively.

(4) We define the complexity class MIP^{*,s} and MIP^{co,s} analogously to MIP* and MIP^{co}, this time using the appropriate synchronous values of the games in the definition.

The main result of [3] actually shows that MIP^{*,s} coincides with RE and thus a reasonable variant of Question 1 above is whether or not MIP^{co,s} coincides with coRE.

We will see later in Proposition 4.5 that synchronous commuting correlations satisfy a certain "stability" property, namely that correlations that are almost quantum commuting correlations (in a certain technical sense) are near

actual quantum commuting correlations. The main result of this note (Theorem 5.3 below) will show that if this stability relation can be realized "effectively," then all languages in $\mathrm{MIP}^{co,s}$ are in RE, and are thus decidable. Since there are elements of coRE that are undecidable (such as the complement of the halting problem), we would obtain a negative solution to the synchronous version of Question 1 above. Said in the opposite direction: if it turns out that $\mathrm{MIP}^{co,s} = $ coRE, then there is no effective version of stability for almost quantum commuting correlations.

3. Preliminaries: traces on groups and group C*-algebras

Fix a countable group G and let $\mathbb{C}G$ denote the corresponding group ring. We recall the following terminology:

Definition 3.1. A function $\tau : G \to \mathbb{C}$ is called:

(1) **of positive type** if for all $\sum_\lambda a_\lambda u_\lambda \in \mathbb{C}G$, we have $\sum_{\lambda,\gamma} \overline{a_\lambda} a_\gamma \tau(\lambda^{-1}\gamma) \geq 0$

(2) a **class function** if τ is constant on conjugacy classes.

The following terminology is not standard, but convenient for our purposes. In what follows, $\mathbb{D}$ denotes the unit disc in the complex plane.

Definition 3.2. A function $\tau : G \to \mathbb{D}$ is called a **trace** on G if it is a class function of positive type.

Here is the reason for the abuse in terminology. Below, $C^*(G)$ denotes the universal C*-algebra of the group G.

Fact 3.3. Given a trace τ on $C^*(G)$, its restriction to G is a trace on G (in the sense of Definition 3.2). Moreover, the map $\tau \mapsto \tau|G$ is a bijection between traces on $C^*(G)$ and traces on G.

In the sequel, we will freely abuse notation and use τ to denote both the trace on the group G as well as the corresponding trace on $C^*(G)$.

Note that in the definition of being positive type, we can restrict attention to elements of the subring $\mathbb{Q}(i)G$ without changing the notion. Assuming then that some countable enumeration $G = (g_0, g_1, g_2, \ldots)$ of G has been given, there is thus an effectively enumerable countable list (R_l) of requirements that characterize when a function $\tau : G \to \mathbb{D}$ is a trace on G. Note really that this list of requirements is independent of the group G in question and just depends on some fixed effective coding of $\mathbb{Q}(i)$.

We now consider "relaxations" of these requirements:

Definition 3.4. Fix $k, l \in \mathbb{N}$ with $k \geq 1$.

(1) If R_l is the requirement $\sum_{\lambda,\gamma} \overline{a_\lambda} a_\gamma \tau(\lambda^{-1}\gamma) \geq 0$, then we define the relaxed requirement R_l^k to be that $\sum_{\lambda,\gamma} \overline{a_\lambda} a_\gamma \tau(\lambda^{-1}\gamma)$ is within $\frac{1}{k}$ of the positive real axis.

(2) If R_l is the requirement $\tau(\gamma^{-1}\lambda\gamma) = \tau(\lambda)$, then we define the relaxed requirement R_l^k to be $|\tau(\gamma^{-1}\lambda\gamma) - \tau(\lambda)| < \frac{1}{k}$.

We say that $\tau : G \to \mathbb{D}$ is a k-**approximate trace on** G if the relaxed requirements $R_1^k, \ldots, R_k^k$ hold.

The following lemma is obvious:

Lemma 3.5. *For each $k \in \mathbb{N}$, there is $\delta > 0$ such that, for all functions $\tau, \tau' : G \to \mathbb{D}$, if τ is a trace on G and $\|\tau - \tau'\|_\infty < \delta$, then τ' is a k-approximate trace on G. Moreover, δ depends only on k and not on G and this dependence is computable from k.*

4. The groups $\mathbb{F}(n,m)$

Below, for $n, m \geq 2$, we let $\mathbb{F}(n,m)$ denote the group freely generated by n elements of order m. In the C*-algebra $C^*(\mathbb{F}(n,m))$, for each $v \in [n]$, we let $e_{v,1}^{n,m}, \ldots, e_{v,m}^{n,m}$ denote the projections onto the eigenspaces corresponding to the eigenvalue ξ_m^i of the unitary operator corresponding to the vth generator $u_v^{n,m}$ of $\mathbb{F}(n,m)$, where ξ_m denotes a primitive m^{th} root of unity. We then have that $(u_v^{n,m})^j = \sum_{i=1}^m \xi_m^{ji} e_{v,i}^{n,m}$ for each $v \in [n]$ and $j \in [m]$.

Definition 4.1. Given $p \in [0,1]^{n^2 m^2}$, we say that a trace τ on $\mathbb{F}(n,m)$ is **adapted to** p if $p(i,j|v,w) = \tau(e_{v,i}^{n,m} e_{w,j}^{n,m})$ for all $v, w \in [n]$ and all $i, j \in [m]$.

Here is the key fact relating traces on $\mathbb{F}(n,m)$ and quantum commuting correlations:

Fact 4.2. ([5]) For $p \in [0,1]^{n^2 m^2}$, we have $p \in C_{qc}^s(n,m)$ if and only if there is a trace τ on $\mathbb{F}(n,m)$ that is adapted to p.

Proof. In [5], they show that $p \in C_{qc}^s(n,m)$ if and only if there is a tracial C*-algebra (A, τ) and a generating family of projections $p_{v,i}$ such that $\sum_{i=1}^m p_{v,i} = 1$ for each $v = 1, \ldots, n$ and such that $p(i,j|v,w) = \tau(p_{v,i}p_{w,j})$. However, letting $\pi : C^*(\mathbb{F}(n,m)) \to A$ be the surjective *-homomorphism determined by sending $e_{v,i}$ to $p_{v,i}$ and defining τ' on $C^*(\mathbb{F}(n,m))$ by $\tau'(x) := \tau(\pi(x))$, we obtain the equivalence with the above statement. $\checkmark$

Lemma 4.3. *There is a computable function $s : \mathbb{N}^7 \to \bigcup_{n,m \geq 2} \mathbb{Q}(i)\mathbb{F}(n,m)$ so that, for each $n, m \geq 2$, each $v, w \in [n]$, each $i, j \in [m]$, and each $k \geq 1$, we have that $s(v,w,i,j,k,n,m) \in \mathbb{Q}(i)\mathbb{F}(n,m)$ and $\|e_{v,i}^{n,m} e_{w,j}^{n,m} - s(v,w,i,j,k,n,m)\| < \frac{1}{k}$, where the norm is the norm on the universal representation of $\mathbb{C}\mathbb{F}(n,m)$, that is, the norm on $C^*(\mathbb{F}(n,m))$.*

Proof. The theorem follows from the fact that the relation $(u_v^{n,m})^j = \sum_{i=1}^{m} \xi_m^{ji} e_{v,i}^{n,m}$ mentioned above can be effectively inverted to express each $e_{v,i}^{n,m}$ as a polynomial in the generator $u_v^{n,m}$ with coefficients in the computable field $\mathbb{Q}(\xi_m)$. Moreover, this procedure is uniform in n and m.   ☑

In order to match notation, in what follows we will rewrite $s(v, w, i, j, k, n, m)$ as $s_{v,w,i,j,k}^{n,m}$. Also, given a function $\tau : \mathbb{F}(n, m) \to \mathbb{D}$, we extend it to a function $\tau : \mathbb{Q}(i)\mathbb{F}(n, m) \to \mathbb{C}$ by linearity.

Definition 4.4. Fix $n, m \geq 2$, $p \in [0, 1]^{n^2 m^2}$, and $k \geq 1$. We say that a function (not necessarily a trace) $\tau : \mathbb{F}(n, m) \to \mathbb{D}$ is k-**adpated to** p if

$$|p(i, j|v, w) - \tau(s_{v,w,i,j,k}^{n,m})| < \frac{1}{k}$$

for all $v, w \in [n]$ and all $i, j \in [m]$.

Here is the "stability" property satisfied by synchornous quantum commuting correlations:

Proposition 4.5. *Given $m, n \geq 2$ and $\epsilon > 0$, there is $k \geq 1$ such that, for all $p \in [0, 1]^{n^2 m^2}$, if there is a k-approximate trace τ on $\mathbb{F}(n, m)$ that is k-adpated to p, then there is $p' \in C_{qc}^s(n, m)$ with $\|p - p'\|_\infty < \epsilon$.*

Proof. Suppose that the lemma is false for some m, n, ϵ, that is, for each $k \geq 1$, there is $p_k \in [0, 1]^{n^2 m^2}$ for which there is a k-approximate trace τ_k on $\mathbb{F}(n, m)$ that is k-adapted to p_k and yet $\|p_k - p\|_\infty \geq \epsilon$ for all $p \in C_{qc}^s(n, m)$. Let p be a subsequential limit of p_k. Since τ_k is pointwise bounded, by passing to a subsequence if necessary, we may suppose that τ_k converges pointwise to a function $\tau : \mathbb{F}(n, m) \to \mathbb{D}$. Note then that τ is an actual trace on $\mathbb{F}(n, m)$ that is adapted to p, whence $p \in C_{qc}^s(n, m)$. Since $\|p - p_k\|_\infty < \epsilon$ for some k, this is a contradiction.   ☑

5. The main theorem

Definition 5.1. We say that $T : \mathbb{N}^2 \to \mathbb{N}$ is a **qc-modulus** if it satisfies the conclusion of Proposition 4.5 for $\epsilon = \frac{1}{12}$, that is, for all $n, m \geq 2$ and all $p \in [0, 1]^{n^2 m^2}$, if there is a $T(n, m)$-approximate trace τ on $\mathbb{F}(n, m)$ that is $T(n, m)$-adapted to p, then there is $p' \in C_{qc}^s(n, m)$ with $\|p - p'\|_\infty < \frac{1}{12}$.

We let $X_k^{n,m}$ denote those $p \in ([0, 1] \cap \mathbb{Q})^{n^2 m^2}$ for which there is a k-approximate trace $\tau : \mathbb{F}(n, m) \to \mathbb{Q}(i)$ that is k-adapted to p.

The following lemma is clear:

Lemma 5.2. *Each $X_k^{n,m}$ is recursively enumerable, uniformly in k, n, and m.*

Here is the main result of this note:

Theorem 5.3. *If there is a computable qc-modulus $T : \mathbb{N}^2 \to \mathbb{N}$, then every language in $\mathrm{MIP}^{co,s}$ is in RE (and thus decidable).*

Proof. Fix a computable qc-modulus T and suppose that $L \in \mathrm{MIP}^{co,s}$. Let $z \mapsto \mathfrak{G}_z$ be an efficient mapping from strings to nonlocal games such that:

- if $z \in L$, then s-val$^{co}(\mathfrak{G}_z) \geq \frac{2}{3}$

- if $z \notin L$, then s-val$^{co}(\mathfrak{G}_z) \leq \frac{1}{3}$.

Here is the algorithm for enumerating L. Given a string z, first determine the dimensions n and m for $\mathfrak{G}_z$. Set $k := T(n, m)$ and let (p_l) be a computable enumeration of $X_k^{n,m}$. The algorithm then simply starts computing $\mathrm{val}(\mathfrak{G}_z, p_l)$ for each l; if for some l we see that $\mathrm{val}(\mathfrak{G}_z, p_l) > \frac{1}{2}$, then we declare that $z \in L$.

Soundness of the algorithm: suppose that $\mathrm{val}(\mathfrak{G}_z, p_l) > \frac{1}{2}$. By the choice of k, there is $p \in C_{qc}^s(n, m)$ such that $\|p_l - p\|_\infty < \frac{1}{12}$. It follows that $\mathrm{val}^{co,s}(\mathfrak{G}_z) \geq \mathrm{val}(\mathfrak{G}_z, p) > \frac{1}{2} - \frac{1}{12} > \frac{1}{3}$, which tells us that $z \in L$.

Completeness of the algorithm: suppose that $z \in L$ and take $p \in C_{qc}^s(n, m)$ such that $\mathrm{val}(\mathfrak{G}_z, p) \geq \frac{2}{3}$. Let τ_p be a trace on $\mathbb{F}(n, m)$ that is adapted to p, whence $|p(i, j|v, w) - \tau_p(s_{v,w,i,j,k}^{n,m})| \leq \|e_{v,i}^{n,m} e_{w,j}^{n,m} - s_{v,w,i,j,k}^{n,m}\| < \frac{1}{k}$ for all $v, w \in [n]$ and all $i, j \in [m]$. Fix $\eta > 0$ small enough and let $p' \in ([0,1] \cap \mathbb{Q}m)^{n^2 m^2}$ and $\tau' : \mathbb{F}(n, m) \to \mathbb{D} \cap \mathbb{Q}(i)$ be such that $\|p - p'\|_\infty, \|\tau_p - \tau'\|_\infty < \eta$. By Lemma 3.5, if η is small enough, then τ' is a k-approximate trace on $\mathbb{F}(n, m)$. Note also that

$$|p'(i, j|v, w) - \tau'(s_{v,w,i,j,k}^{n,m})| < 2\eta + \|e_{v_i}^{n,m} e_{w,j}^{n,m} - s_{v,w,i,j,k}^{n,m}\| < \frac{1}{k}$$

as long as η is small enough. (Note that the conditions on η are effective in terms of k and thus in terms of n and m.) It follows that τ' is k-adapted to p', whence there is l such that $p' = p_l$. As long as $\eta < \frac{1}{12}$, we have that $\mathrm{val}(\mathfrak{G}_z, p_l) \geq \frac{2}{3} - \frac{1}{12} > \frac{1}{2}$. Consequently, the algorithm will tell us that $z \in L$. ☑

We note that it remains a possibility that $\mathrm{MIP}^{co,s}$ is properly contained in co-RE and yet there is no computable qc-modulus.

References

[1] M. Coudron and W. Slofstra, *Complexity lower bounds for computing the approximately-commuting operator value of non-local games to high precision*, CCC '19: Proceedings of the 34th Computational Complexity Conference (2019), 1–20.

[2] I. Goldbring and B. Hart, *The universal theory of the hyperfinite ii_1 factor is not computable*, preprint. arXiv 2004.02299.

[3] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, *The universal theory of the hyperfinite ii_1 factor is not computable*, MIP* = RE, preprint, arxiv 2001.04383.

[4] N. Ozawa, *Tsirelson's problem and asymptotically commuting unitary matrices*, J. Math. Phys. **54** (2013).

[5] V. Paulsen, S. Severini, D. Stahlke, I. Todorov, and A. Winter, *Estimating quantum chromatic numbers*, Journal of Functional Analysis **270** (2016), 2180–2222.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA, IRVINE,
340 ROWLAND HALL (BLDG.# 400), IRVINE,
CA 92697-3875
e-mail: isaac@math.uci.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS
MCMASTER UNIVERSITY, 1280 MAIN ST.,
HAMILTON ON, CANADA L8S 4K1
e-mail: hartb@mcmaster.ca